WhiteHat SECURITY

Moving to the Cloud?

Take Your Application Security Solution with You

September 2010

A WhiteHat Security Whitepaper

3003 Bunker Hill Lane, Suite 220 | Santa Clara, CA 95054-1144 | **www.whitehatsec.com**

Introduction

Cloud computing is quickly becoming a fundamental part of information technology. Nearly every enterprise is in some stage of evaluating or deploying cloud solutions. Even as business managers turn to the cloud to reduce costs, streamline staff, and increase efficiencies, they remain wary about the security of their applications and the data they protect. While software-as-a-service has gained in popularity among security solutions, many companies express concern with turning over responsibility for their application security to an unknown entity, and rightly so.

Who is responsible for application security in the new world of cloud computing? Increasingly, we see third-party application providers, who are not necessarily security vendors, being asked to verify the thoroughness and effectiveness of their security strategies. Nevertheless, the enterprise ultimately still bears most of the responsibility for assessing application security regardless of where the application resides. The fact of the matter is, cloud computing or not, application security is a critical component of any operational IT strategy.

Businesses are run on the Internet, and as cloud computing expands that means that a host of new data is being exposed publicly. History and experience tell us that well over 80% of all websites have at least one serious software flaw, or vulnerability, that exposes an organization to loss of sensitive corporate or customer data, significant brand and reputation damage, and in some cases, huge financial repercussions.

Recent incidents on popular websites like YouTube, Twitter and iTunes; hosting vendors like Go Daddy; and the Apple iPad have exposed millions of records, often taking advantage of garden-variety cross-site scripting (XSS) vulnerabilities. The 2009 Heartland Payment Systems breach was accomplished via a SQL Injection vulnerability. Thus far, the financial cost to Heartland is $60 million and counting. The soft costs are more difficult to determine.

Cloud computing will require more focused effort from enterprises that have been less consistent with application security. Those with a strong application security program in place will find that little has changed. Across the board, however, the move will provide an opportunity to prioritize security on what is commonly acknowledged as the most exposed part of their business, Web applications, and often the most seriously underfunded. The following issues must be understood in order to align business goals and security needs as the enterprise transitions to cloud computing.

1. Web Applications are the Primary Attack Target - Securing your Applications Must be a Priority

Most experts agree, and the recent Ponemon Group survey, “The State of Application Security” confirms, that websites are the target of choice for attacks. Why? With more than 200 million websites in production today, it makes sense that attackers of all types would make them their target. No matter the skill level, there is something for everyone on the Web, from random, opportunistic attackers to very focused criminals focused on data from a specific organization.

Their methods can range from Mass SQL Injection Worms planting malware designed to exploit unpatched Web browsers, to using XSS to create authentic-looking phishing sites and steal unsuspecting users’ cookies and session IDs. And, in one of the most recognized cases, an attacker used SQL injection to steal credit and debit card numbers that were then used to steal more than $1 million from ATMs in various countries.

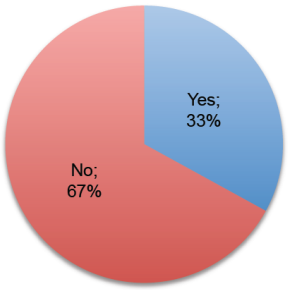
And yet, most organizations believe that application security is underfunded, with only 18% of IT security budgets allocated to address the threat posed by insecure Web applications, while 43 percent of IT security budgets were allocated to network and host security.

While businesses are fighting yesterday's wars, hackers have already moved on. Even more puzzling, application security is not a strategic corporate initiative at more than 70 percent of organizations. And these same security practitioners do not believe they have sufficient resources specifically budgeted to Web application security to address the risk. As more applications move to the cloud, this imbalance must change. IT and the business must work together to prioritize the most critical security risk.

Table 1: IT security budget allocated by layer

Application security	18%
Data security	30%
Host security	9%
Infrastructure/network security	43%

Pie Chart 1: Q. In your opinion, is the level of your website security budget sufficient?



2. Internal Applications are Now External Applications

As organizations embrace cloud computing, many applications, such as human resources, accounting, email and many others, are now accessible online. What was once safely housed behind firewalls, VPNs and other network security devices now resides on the Internet, where corporate network security solutions cannot protect them. Security teams experienced in securing Web applications will not find the transition troubling. However inexperienced development and security teams will have to negotiate a mindshift when practicing cloud security.

The best way to address the problem is have an accurate inventory of your applications, cloud, Web, or wherever they reside. Then, the business owners must assign value to those applications and prioritize the risk associated with them. Finally, security must determine a methodology by which they can assess the security posture of those applications on an ongoing basis in an operational environment. The risk is amplified now that the applications are on a public network. And, the ultimate responsibility resides with the customer.

3. The Network Layer has Become Abstracted

Prior to cloud computing, organizations felt a certain confidence level about the security of applications that resided behind the firewall. To a certain extent, they were justified in their beliefs. Now, we see that network layer, which had been made nearly impenetrable over the past 10 years, becoming abstracted by the advent of cloud computing. Where once there was confidence, there is now confusion among security teams as to where to focus their resources. The short answer is: Keep your eye on the application because it is the only thing you have control over.

Additionally, one of the hot topics in cloud security is the right to test. There's a disconnect between the security team, the business, and the cloud computing provider.

Legally, customers have to ask for the right to test their cloud provider's infrastructure systems. If they do so without permission, they may be violating the law. The customer is left vulnerable in many ways. First, the security team has lost visibility into the network security infrastructure. If the cloud provider makes a change

to its infrastructure, it naturally changes the risk profile of the customer's application. However, the customer is most likely not informed of these changes and therefore unaware of the ultimate impact. It is the customer's responsibility to demand periodic security reports from its cloud vendor and thoroughly understand how their valuable data is being protected.

4. Security Team Loses Visibility with Cloud Computing: No IPS/IDS

One of the main concerns of security professionals anticipating an organizational switch to cloud computing is loss of visibility into attacks in progress, particularly with software-as-a-service (SaaS) offerings. With the enterprise applications hosted by the cloud service provider, the alarm bells that the security team could rely on to alert them of attack, typically Intrusion Prevention or Intrusion Detection Systems, are now in the hands of the vendor. For some, this loss of visibility can translate into loss of control. In order to retain a measure of control, it is critical to understand the security measures that are in place at your cloud vendor and also to require that vendor to provide periodic security updates.

5. Change in Infrastructure is a Great Time to make Policy Changes/New Security Controls

Any time there is a change from one infrastructure to another, it presents businesses with an impetus to review its security policies and procedures. In fact, a move to cloud computing can be an excellent opportunity to institute new security policies and controls across the board. A credible case can be made to review budgets and allocate more funds to application security. Where previously application security was a second-tier spending priority, it now rises to the top when SaaS comes into play.

This is a great time to pull business, security and development teams together to develop a strategy.

6. Cloud Security Brings App Security more in line with Business Goals - Decision Making Based on Business Value and Appropriate Risk.

For many organizations, application security is an afterthought. The corporate focus is on revenue, and often that means frequently pushing new code. Even with a rigid development and QA process, there will be differences between QA websites and the actual production applications. This was not as critical when the applications resided behind the firewall, but now the business unit managers must take into account the value of the data stored in an application residing in the cloud.

Ideally, the security team and the business managers would inventory their cloud (and existing Web) application deployments. Once an accurate asset inventory is obtained, the business managers should evaluate every application and prioritize the security measures based on business value and create a risk profile. Once these

measurements have occurred, an accurate application vulnerability assessment should be performed on all applications. Only then can the team assign value and implement an appropriate solution for the risk level. For example, a brochureware website will not need the level of security as an e-commerce application.

Once an organization has accurate and actionable vulnerability data about all its websites, it can then create a mitigation plan. Having the correct foundation in place simplifies everything. Urgent issues can be "virtually patched" with a Web application firewall; less serious issues can be sent to the development queue for later remediation. Instead of facing the undesirable choice between shutting a website down or leaving it exposed, organizations armed with the right data can be proactive about security, reduce risk and maintain business continuity.

Conclusion

Ultimately, website security in the cloud is no different than website security in your own environment. Every enterprise needs to create a website risk management plan that will protect their valuable corporate and customer data from attackers. If your organization has not prioritized website security previously, then now is the time to make it a priority. Attackers understand what many organizations do not – that Web applications are the easiest and most profitable target. And, cloud applications are accessed via the browser which means the website security is the only preventive measure that will help fight attacks.

At the same time, enterprises need to hold cloud vendors responsible for a certain level of network security while remaining accountable for their own data security. Ask vendors what type of security measures they employ, how frequently they assess their security and more. As a customer, you have a right to know before you hand over your most valuable assets. And, vendors know that a lack of security can mean lost business.

There may be some hurdles to jump during the transition from internal to cloud applications. But, by following these recommendations, an organization can avoid pitfalls:

Recommendations

1. *You can't secure what you don't know you own - Inventory your applications to gain visibility into what data is at risk and where attackers can exploit the money or data transacted.*
2 *Assign a champion - Designate someone who can own and drive data security and is strongly empowered to direct numerous teams for support. Without accountability, security and compliance will suffer.*
•3 *Don't wait for developers to take charge of security - Deploy shielding technologies to mitigate the risk of vulnerable applications.*
4 *Shift budget from infrastructure to application security – With the proper resource allocation, corporate risk can be dramatically reduced.*

WhiteHat Sentinel Simplifies Cloud Application Security

For enterprises that take application security seriously, WhiteHat Sentinel is the solution of choice to gain visibility into corporate security posture, prioritize workflow to adapt to changing threats, and confidently

mitigate issues. With the WhiteHat Sentinel website risk management platform, the security team can maintain control of information security while offering the business the flexibility to explore cloud computing or other options.

WhiteHat Sentinel is the Best Solution Because:

Cloud applications demand assessment in an operational environment

WhiteHat Sentinel is built to assess websites for vulnerabilities in an operational environment. Attacks originate externally. Therefore, it is vital to assess applications from the point-of-view of the hacker. WhiteHat Sentinel performs complete, ongoing assessments safely, without business interruption. WhiteHat Sentinel is the only real-time solution for vulnerability assessment.

WhiteHat Security is a Trusted Leader in Website Vulnerability Management

WhiteHat Security is a recognized expert in website security. As the first SaaS-based solution for website risk management, WhiteHat has been providing operational website vulnerability assessment with WhiteHat Sentinel since its inception. Hundreds of companies, including many of the Fortune 1000, trust WhiteHat Security to help them identify, prioritize and mitigate website vulnerabilities.

Due to WhiteHat Security's experience as a SaaS provider, the company has a unique view into the state of website security across industry verticals. With more than 2,000 websites under management, WhiteHat Security is often at the forefront of identifying new attack vectors and using that knowledge to help customers prevent exposure.

Accuracy, Visibility and Control to Secure Cloud Applications

Only WhiteHat Sentinel was built from the ground up as a SaaS solution, perfectly suited for assessing remote applications. And, WhiteHat Sentinel is backed by a security engineering team that verifies each and every vulnerability identified by Sentinel, ensuring that customers receive only accurate, actionable data. With this data, security teams get unparalleled visibility into their security posture on a continuous basis and actively reduce risk to the business.

Additionally, Sentinel, via its open XML API and highly accurate results, is able to return control to the security team by offering mitigation options with industry-leading Web application firewalls. An integration of a WAF with WhiteHat Sentinel detects and defends website vulnerabilities much more efficiently, and resolves the disconnect between compliance intentions and actual security. With virtual patching, the entire industry is brought to a new level of website protection, with extreme accuracy and efficiency – delivering rapid identification and immediate mitigation of vulnerabilities, without waiting for development resources.

The WhiteHat Sentinel Service – Website Risk Management

WhiteHat Sentinel is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the flexibility, simplicity and manageability that organizations need to take control of website security and prevent Web attacks. WhiteHat Sentinel is built on a Software-as-a-Service (SaaS) platform designed from the ground up to scale massively, support the largest enterprises and offer the most compelling business efficiencies, lowering your overall cost of ownership.

Cost-effective Website Vulnerability Management – As organizations struggle to maintain a strong security posture with shrinking resources, WhiteHat Sentinel has become the solution of choice for total website security at any budget level. The entire Sentinel product family is subscription-based. So, no matter how often you run your application assessments, whether it's once a week or once a month, your costs remain the same.

Accurate – WhiteHat Sentinel delivers the most accurate and customized website vulnerability information available – rated by both threat and severity ratings – via its unique assessment methodology. Built on the most comprehensive knowledge base in Web application security, WhiteHat Sentinel verifies all vulnerabilities, virtually eliminating false positives. So, even with limited resources, the remediation process will be sped up by seeing only real, actionable vulnerabilities, saving both time and money, dramatically limiting exposure to attacks.

Timely – WhiteHat Sentinel was specifically designed to excel in rapidly-changing threat environments and dramatically narrow the window of risk by providing assessments on your schedule. Whether it's a quarterly compliance audit, new product roll-out, or weekly business-as-usual site updates, WhiteHat Sentinel can begin assessing your websites at the touch of a button.

Complete – WhiteHat Sentinel was built to assess hundreds, even thousands of the largest and most complex websites simultaneously. This scalability of both the methodology and the technology enables WhiteHat to streamline the process of website security. WhiteHat Sentinel was built specifically to run in both QA/development and production environments to ensure maximum coverage with no performance impact. And, WhiteHat Sentinel exceeds PCI 6.6 and 11.3.2 requirements for Web application scanning.

Simplified Management – WhiteHat Sentinel is turnkey – no hardware or scanning software to install requiring time-intensive configuration and management. WhiteHat Sentinel provides a comprehensive assessment, plus prioritization recommendations based on threat and severity levels, to better arm security professionals with the knowledge needed to secure an organization's data. WhiteHat Sentinel also provides a Web services API to directly integrate Sentinel vulnerability data with industry-standard bug tracking systems, or SIMs or other systems allowing you to work within your existing framework. With WhiteHat, you focus on the most important aspect of website security – fixing vulnerabilities and limiting risk.

About WhiteHat Security, Inc.
Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of website vulnerability management services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company's flagship service, is the only solution that incorporates expert analysis and industry-leading technology to provide unparalleled coverage to protect critical data from attacks. For more information about WhiteHat Security, please visit www.whitehatsec.com.

WhiteHat Security, Inc. | 3003 Bunker Hill Lane, Suite 220 | Santa Clara, CA 95054-1144 | **www.whitehatsec.com**

090210