Minimize Risk with IBM Application Security Solutions Application Security podcast

Event ID: 106198

Brooke Campanelli: Hello, and welcome to our Minimize Risk with IBM Application Security Solutions podcast. My name is [Brooke Campanelli], and I will be your IBM host today. Before we get started, we have a few general announcements. This presentation is available for download in podcast format. Should you experience any technical difficulties, please visit the podcast help guide located below your presentation window.

Please welcome our guests today, Paul Kaspian and Rick Weinberg who will talk about application security, the most common attacks and risks and how IBM can help. Paul, it's all yours.

Paul Kaspian: Thanks, Brooke. Today more than ever, organizations depend on the Internet to collect and deliver information, exposing companies to an increasing range and frequency of threats. In an effort to quickly bring new applications and services online, many new web applications have been developed and deployed with a minimal attention given to the security risk that they may introduce. Unfortunately, this has resulted in a large number of websites that have become surprisingly vulnerable to hackers.

So how large is this problem? Research has estimated that today up to 90% of externally accessible applications are web enabled, and that 2/3 of them have exploitable vulnerabilities. This has resulted in a new data breach occurring almost daily, putting the number of Americans who have been informed that they have suffered a security breach at approximately 100 million. Securing the applications used to collect sensitive data has understandably become a top priority for many information security professionals. Many organizations are adopting the Application Security solutions from IBM to address these threats and to strengthen their overall security posture.

Now IBM offers both software and services to secure applications by authenticating and authorizing only valid users and protecting web applications from hackers by identifying exploitable vulnerabilities. So obviously, the corporate website is one of the largest externally facing set of applications and is responsible for the most important interactions between a customer and an organization. Many organizations use web applications to collect valuable personal information like credit card numbers, bank account information, as well as confidential information such as medical records, and unfortunately, hackers also understand the value of this information and how to exploit these applications to gain access to it.

Industry analysts have estimated that 75% of attacks are now targeting web applications that interact with these types of information coupled with the increasing adoption of Web 2.0 technology, more and more companies are encouraging their customers to use the web as a first point of contact making it that much more critical that websites and their related applications are secure. Beyond these core security concerns, it's no secret that missed web security vulnerabilities have led to other damaging events such as regulatory non-compliance, fines, lawsuits, brand damage, consumer confidence erosion, and online channel decline. All we need to open a newspaper to understand the additional risks associated with these types of threats.

So that brings us to a key question, why aren't many of these vulnerabilities being addressed? Simply put, security teams are under intense pressure, and many cannot keep up with the volume of applications they need to test for a growing number of vulnerabilities. Currently, many security and development teams are catching issues late in the development cycle resulting in high cost to fix the issues, or even worse, not catching issues until they're already in production. The continuous cycle of developing, updating and auditing applications, combined with trying to keep up with the latest threats is a constant battle.

One of the key challenges is that there's often no one responsible for directly addressing application security. While developing an application, developers are often focused on the functionality rather than security. They're under tight deadlines, they lack security training and expertise, which means they don't realize they're introducing security defects that can be used to exploit the application for malicious purposes. Also, quality assurance professionals test the application for functionality bugs and performance but also don't typically understand security issues. So for example, if a web form doesn't restrict hazardous characters, characters used to issue commands instead of simply submitting data, attacks such as sequel injection can be carried out to gain access to back end databases and the sensitive information that they store.

Organizations need to adopt a process and implement technology to monitor for, identify and remediate these threats in a timely and cost effective way. IBM's Application Security solutions allow companies to preemptively and actively protect applications from external and internal threats, increasing efficiency, supporting compliance and improving an organization's overall security posture. We provide preemptive network security, application security and access management solutions that help protect vital customer data and information assets from external and internal threats.

A critical piece of an organization's overall security posture is implementing a solution to successfully address the application level threats mentioned earlier. Traditionally, vulnerability analysis and vulnerability management has been focused at the network or operating system level which means many IT organizations are not properly addressing the application layer. For those that are concerned with web application vulnerabilities, many spend a large amount of time and resources manually scanning the web applications.

IBM offers software and services to help manage and automate the application security lifecycle, including IBM Rational AppScan. This solution scans applications, identifies vulnerabilities including cross-site scripting and sequel injection and generates detailed fix recommendations to ease remediation. IBM Rational also recognizes the only way to get ahead of this growing threat is by building the application securely from the ground up. As such we offer security tools designed for non-security professionals, such as developers and QA managers, to simplify this complicated task, and we provide integrated web based training on everything from secure coding techniques, how to configure, run and customize AppScan.

Using AppScan, organizations can perform security audits and defect testing throughout the application lifecycle. Production applications are an obvious first place to implement regular audits and analysis to determine security and compliance risks to an organization. At the same time, one must not forget that the application development lifecycle is the breeding ground for the defects

that cause the risks. Performing security testing during the software application development lifecycle at key points during the various stages, from development to QA to staging, will reduce costs and significant reduce your online risk.

Now I'd like to hand the presentation over to Rick.

Rick Weinberg: Thanks, Paul. As organizations enhance their security posture by leveraging AppScan to address their web application vulnerabilities, there's another problem that should be addressed, securing user access to web applications. A few of the most pressing vulnerabilities out there today, cross-site scripting and cross-site request forgery, are successful because they attempt to bypass access controls to the web application.

One step in easing the remediation of these vulnerabilities is to deploy a web access management solution, like IBM Tivoli Access Manager for E-Business, to centrally secure and control access to web applications. Organizations want to ensure they provide access to those users who they have entitled. Tivoli Access Manager is used to define access control lists to web applications so that only the authenticated and authorized users can gain access to the web applications. The value of Tivoli Access Manager becomes more pronounced for organizations that have a large number of heterogeneous applications, as they leverage different authentication and authorization formats. Tivoli Access Manager offers out of the box integration with a number of leading third party applications to enable flexible user authentication and centralized authorization.

Together, AppScan and Tivoli Access Manager compliment each other. AppScan ensures that the web application Tivoli Access Manager is granting access to are scanned and tested for vulnerabilities.

In summary, the consequences of a security breach are great, increased regulatory scrutiny, fines, lawsuits, brand damage, consumer confidence erosion and online channel decline. IBM's Application Security solutions allow companies to preemptively and actively protect applications from the external and internal threat, increasing efficiencies, supporting compliance and improving the organization's overall security posture. With the explosion of web enabled applications, a new reality has emerged. Organizations should not neglect the important step of securing their web applications, the users that access them and the data they collect. It only takes a single breach to ruin a reputation. Back to you, Brooke.

Brooke Campanelli: We thank you for listening to our, Minimize Risk with IBM Application Security Solutions podcast. To learn more about IBM's Application Security offerings, please go to www.ibm.com, and do a search on application security to find links to an application security webcast, an application security solution sheet and a complimentary security health scan in order to provide you with some immediate insight. In addition, if you're interested in learning more about IBM Application Security offerings and related topics through events such as these, please subscribe to our RSS feed and you'll automatically be notified when new events become available. Finally, if you would like to be contacted by an IBM representative regarding any of the information you've heard today, please click on the Contact Me button below your presentation window, an a representative will be in touch with you soon.

Well this concludes our presentation. We hope you have enjoyed your time with us, and we look forward to hearing from you soon.