Welcome to this IBM Rational podcast. I'm Angelique Matheny. The title of this podcast is "**The critical challenge of application security and compliance"** and joining me is David Grant - David is director of marketing, security solutions for IBM Rational and brings 12 years of software industry marketing and strategy experience and expertise.

In this podcast you will hear how the IBM Rational AppScan software suite with a focus on AppScan Enterprise is used across an organization's software development lifecycle to increase visibility and control – helping address the critical challenge of application security.

HI Dave, welcome to the podcast.

We've got a lot to cover today, so let's get started.

1. **Dave, let's start with this. Can you define application security and why it is evolving to be the top threat area? What about the increased adoption of Web 2.0 technology? Has that made the web more difficult to secure?**
   - IT security at the highest level can be broken into 3 categories: host security, network security, and application security. Most companies have invested in securing their hosts and networks while leaving many applications open to vulnerabilities. Application security issues arise when applications are susceptible to 'unintended functionality' that has been coded into the application by accident (or by design) that can be exploited by malicious individuals.
   - Application security and specifically website security has become one of the largest threats in the industry. The reason is that most applications are vulnerable and hackers know this. Applications are an excellent source of sensitive information for these malicious individuals.
   - 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 costs to fix the issues, or even worse, not catching issues until they are 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.
   - Web 2.0 will increase the amount of interaction between clients and therefore will introduce new avenues for hacking as well.

2. **Dave, how large is this problem and where do you see this going? Is it getting better or worse?**
   - Unfortunately this problem is very large. Estimates from industry analysts and from vendors such as rational indicate that anywhere from 75%-90% of applications are vulnerable today.
   - According to an IBM ISS report in 2008 over 50% of all security vulnerabilities are from applications.
   - This problem is getting worse. Simply put, users demand and expect more robust Web applications and functionality. The more code and functionality that goes into Web applications, the more vulnerability you'll most likely find in them.

3. **Typically, how do companies deal with application security?**

- Unfortunately many organizations have a false sense of security in this area as they feel like investments made in other IT security areas such as network security and firewalls address this area.
- Outsource to consulting organizations to conduct ethical hacking attempts on there applications. This is great and an important step in any application security program but unfortunately it is cost prohibitive to do this for all applications and for all changes to applications. Also, this does not address the root cause of the problem: building security into application development.
- In house manual efforts, organizations hire security auditors to perform security checks as a last step in the development lifecycle. This has the same issues as the previous example.
- Automated testing software like rational AppScan. These products automate the process of testing applications for security and compliance issues.

4. **So why are organizations typically falling short on addressing application security?**
    - Most companies have not invested in this area – we have been so busy building and deploying applications that we ignored security. Many organizations are also under the false impression that if their network is locked down and they have a firewall, their applications are secure.
    - Security teams often cannot keep up with the volume of applications they need to test. Currently, they are either catching issues late in the development cycle or not at all. The continuous cycle of developing, updating and auditing applications combined with trying to keep up with the latest patches is a constant battle against hackers.
    - Application development teams have very little if any security expertise so they are building and deploying applications that are leaving organizations very vulnerable. One of the key challenges is that there is often no one responsible for directly addressing application security. While developing an application, developers are often focused on the functionality rather than security. They are under tight deadlines and lack security training and expertise, which mean they don't realize they are introducing security defects that can be used to exploit the application for malicious purposes. Quality assurance professionals test the application for functionality bugs and performance but also don't typically understand security issues.

Root causes:

- Software developers were never trained on security issues or mandated to adhere to security requirements
- Existing defenses do not address application level threats
- Security teams are focused on other issues (network, desktops, etc.) and are overwhelmed
- No defined policy, accountability or process to deal with this issue

5. **Dave, what regulations are affected by web application security? I know the Payment Card Industry is affected. How does the Payment Card Industry compliance help with this?**
    - There are a number of regulations that mandate IT security and as outlined application security is one of the top IT security threats today so there are many regulatory implications. Some that specifically come to mind are: GLBA, HIPAA, US State Breach Notification Acts, FISMA, Safe Harbor, & of course PCI.
    - PCI: As of June 30th, section 6.6 of the Payment Card Industry (PCI) Data Security Standards (DSS's) became mandatory for all companies that are required to be PCI compliant. Section 6.6 is really a direct response to the application security threat and

is an attempt to better protect credit card information from being compromised by a hacker via an insecure web application.
- Section 6.6 was clarified and provides several options for fulfilling the requirement that range from doing a manual review of each application's source code to properly utilizing an automated web application vulnerability scanning tool.

6. **What's needed to counter application security risks and how can IBM help?**
   - One of the most effective solutions is to fix weaknesses before the application is launched. While it sounds like a common sense suggestion, most applications are not built with security in mind. IBM is unique in that we provide solutions for providing application risk assessments, SDLC testing integration, and deployment mgmt.
     i. **As a first step: a proper assessment of your custom web applications**. An IBM Internet Security Systems (ISS) application security assessment is a review of your custom or commercial Web applications to determine security weaknesses that can lead to compromise. Our security experts can thoroughly assess your applications, from both technical and nontechnical perspectives, to uncover security weaknesses and demonstrate the consequences of an attacker taking advantage of those weaknesses. Our consultants attempt to defeat access control mechanisms that are in place to gain access to unauthorized data and/or to access the applications supporting network infrastructure. The result is a detailed report of findings and specific recommendations for remediating any vulnerabilities found.
     ii. **Embed application security from design to production with Rational AppScan.** To help your organization adhere to Web application best practices, develop more secure applications and better manage your business infrastructure, IBM offers a broad portfolio of security solutions that can help you manage application security throughout the application's life cycle. These solutions can identify and quickly address vulnerabilities. Taking a preemptive approach to application security is just one of several modular entry points into IBM security solutions, which can assist you in establishing effective risk management strategies to manage and secure business information and technology assets, anticipating vulnerabilities and risks, and maintaining timely access to information. Rational AppScan can help your organization embed application security from design to production. Prior to deployment, applications are tested for unknown vulnerabilities. Because this solution helps both developers and IT operations staff, it gives you the flexibility to address application security in the ways that make the most sense for your enterprise.
     iii. Rounding out the IBM Web Application Security solution, **Tivoli Access Manager** gives users role-based access to the resources they need and single sign-on (SSO) capabilities to help optimize productivity - and minimize the administrative burden on IT staff that can support high-value initiatives and **Tivoli Compliance Insight Manager** tracks user activities on sensitive or regulated IT assets producing understandable, customizable reports and a compliance dashboard designed to meet regulatory requirements, enable privileged user monitoring and auditing (PUMA), provide for audit of sensitive data disclosure activity across heterogeneous databases, and facilitate rapid action to remediate suspicious or exceptional behavior.

7. **And Rational? - how does Rational fit into an end-to-end Security plan? What benefits does it bring to the table?**
   - Rational acquired a company called Watchfire in 2007. Watchfire was the market leader in application security and compliance. The product called AppScan automates the process of testing applications for security and compliance issues.
   - Most companies treat application security as an after thought and will test applications just before they are deployed or after they are deployed (if they ever test them!). To truly solve the problem of application security you need to build security

into the development process instead of waiting until the end. This is where Rational AppScan fits in. AppScan is an automated application security testing solution that ensures applications are not vulnerable. It scans an application and provides reports and recommendations to the user on how to fix the issue. AppScan can be integrated into all major steps of the software development lifecycle from coding to build to QA through to deployment ensuring the most complete coverage for security issues. Rational's ability to do this is very valuable and unique.

- The benefit to testing earlier are twofold:
    i. Cost – testing for issues earlier in the software cycle is much more cost effective then finding issues just before or in production. Depending on the statistic you see it can range from $25/defect in development to $16,000/defect in production.
    ii. Reduce Exposure – spreading application testing throughout the cycle to more people involved will ensure greater coverage of your applications.

8. Can you describe the Rational AppScan portfolio for addressing application security and compliance across the SDL or software development lifecycle?

- Rational's portfolio is unique in the industry in 2 major ways.
    i. First, the AppScan product line is the only solution that has tailored products for every step of the lifecycle from development all the way through to production.
    ii. Secondly, Rational is a leader in software delivery solutions which enables us to truly integrate security and compliance testing into the environment.
- Development – AppScan Developer Edition & Build Edition. These products test code for security defects and integrate within the development environments such as IDE's (RAD, Eclipse) and Build Automation servers (BuildForge).
- Testers/QA – AppScan Tester Edition. This product is used by testers to test for security and compliance within test environments such as Rational Clearquest. This offering lets Testers reuse test scripts and setup tickets for development
- Security Specialists – AppScan Standard Edition & AppScan Enterprise are used by IT specialists to ensure applications that are built are secure and compliant.
- Deployment & Production Monitoring – AppScan Enterprise and AppScan Ondemand (SaaS offering) are used to monitor applications in production.

9. What is AppScan Enterprise (ASE) and what makes it unique?

- ASE is the only solution on the market that is web-based
    - Easier and more cost effective to deploy across an organization
    - ASE's QuickScan gives developers black box scanning capability from a simple, self-service web portal.
- ASE is the only solution built upon a true enterprise architecture
    - Due to the architecture with web based testing engines and a database backend you can test an unlimited amount of applications efficiently
- ASE provides superior enterprise visibility through metrics and dashboards
    - High level dashboards enable organizations to see application security and compliance posture across the organization regardless of number of applications and geographic locations.
- ASE offers security administrators the most granular access controls
    - Control and contain your vulnerability data and tests
- ASE provides built in web based training.
    - Training is important and this system lets users tap into training within the product and managers can understand who is taking training and how they are performing.

10. Describe the typical uses for AppScan Enterprise?

- Testing many applications in one system and provides high level metrics. Global scanning (scale) and reporting (dashboards)
- Scaling testing to many users without deploying software on the desktops. Web-based system can scale easily. ASE's QuickScan leverages administrator-defined Scan Templates, so running a scan is as simple as clicking a button. Shields developers from the complexity of configuring a scan. Keeps control in the hands of the security team
- Case Studies
  i. Major US City
     - Need to create a central application security service to support all agencies. Lack of internal security specific expertise to manage agency-wide issues.Challenge:85 agencies, each with many web applications
     - Difficulty deploying, managing & training users across the city with desktop tools
     - AppScan Enterprise
     - Benefits: Department heads and CIO's have visibility, through dashboards, to security risks across the enterprise

  i. A Worldwide Leader in Networking Equipment
     - Small, niche security team had become a bottleneck to the 2,000+ development organization
     - Web applications portfolio estimated at 2,500 applications – about 425 applications changed yearly
     - Had an experienced application team using AppScan, but needed a way to scale and involve many more testers in the process
     - Deployed Rational AppScan Enterprise, providing access to **ALL** developers to test applications and address security issues before being pushed downstream
     - Ensured security team could manage project, configure scans and control access to vulnerability data
     - Web-based training was a key component to project success

Dave, we've covered a lot today. Thank you so much for taking time out to discuss "**The critical challenge of application security and compliance"**. We really appreciate it.

To learn more about IBM Rational AppScan, please visit developerWorks downloads for the free trial.

MATHENY: That was Dave Grant, Rational's director of marketing, security solutions.

MATHENY: If you are interested in more podcasts like this one – check out the Rational Talks to You podcast page at www.ibm.com/rational/podcasts.

This has been an IBM Rational podcast. I'm Angelique Matheny. Thanks for listening. Keep tuning in as Rational Talks to You.