MATHENY: Hello, and welcome to this Rational Talks to You Podcast, Effectively Addressing Web Application Security with Limited Resources. Today's podcast will introduce you to IBM Rational Appscan Express, an automated tool that finds Web vulnerability and offers straightforward recommendations on how to fix these issues. The end result? Higher levels of security, reduced risk related to a security breach, and lower security testing costs.

To talk about just how this works, I'm joined today by Paul Kaspian, who's a product marketing manager specializing in Web application security and compliance at IBM. Hi, Paul. Thanks for joining us today.

KASPIAN: Hi, Angelique. Good to be here.

Paul, we've got an important topic to talk about, so let's get started. Web application security has clearly been a hot topic in security as a result of many of the data breaches we have seen in the news. It seems like we're seeing a new company every week that has suffered from this type of attack. How can organizations protect themselves from these types of attacks?

KASPIAN: Well, organizations really need to start testing their Web applications directly for vulnerabilities. It's just not enough anymore to just simply have a firewall, or intrusion prevention system to protect against

these particular types of attacks.

And also, many clients are using network vulnerability scanning as a best practice, but this doesn't really address the Web application layer. So by testing the actual Web applications, organizations can find vulnerabilities and fix them at their source, and then they can rely on better security mechanisms such as the firewall and intrusion prevention systems, many of which have some basic application layer protections as a real-time stop gap in the second layer protection.

MATHENY: So what is the best way to tackle this type of security testing and fix these problems?

KASPIAN: Well, many organizations started doing some degree of manual testing on their applications where they're doing some basic penetration testing on individual pages such as, you know, log-in screens, et cetera.

And this is better than doing nothing at all, but it doesn't give them the security coverage they need, and it's extremely time consuming to perform. Other organizations have opted to bring in an outside penetration tester to conduct audits once or twice a year, but this type of testing is extremely expensive so it really limits the frequency of how often they can test.

And since Web applications actually change very frequently, this typically doesn't provide the degree of testing most organizations really need.

MATHENY: Don't you think this must be even more difficult for many of the smaller organizations with less security resources and budget to deal with this?

KASPIAN: Exactly. So many smaller companies out there have the same risk level as larger enterprises, but they have less in-house security resources and expertise, and they lack the same amount of budget resources. And this makes it even harder for them to do manual penetration testing in-house, and in many cases they really can't afford to hire an outside tester to audit each one of their applications on a regular basis.

MATHENY: So tell us, how can IBM help with this challenge?

KASPIAN: IBM provides IBM Rational Appscan. It's a best of breed automated Web application scanning tool. And many of our clients have already benefitted from automating the process with this kind of testing to really improve their overall Web application security, and they've lowered their costs by reducing the amount of manual or outsourced

security testing.

So it's important to point out that this solution has helped clients deal with regulatory compliance standards as well, like Payment Card Industry Data Security Standard -- or, PCIDSS -- by providing a way to thoroughly test applications for vulnerabilities.

And many of our existing clients have been pleasantly surprised to find out that something they've already been doing all along -- which is using IBM Rational Appscan to test for Web vulnerabilities -- has actually significantly contributed to their ability to meet compliance standards.

And also recently IBM's introduced several new editions of IBM Rational Appscan including IBM Rational Appscan Express Edition, and that's actually tailored for smaller organizations.

MATHENY: Well, Paul, tell us about this new offering, Rational Appscan Express.

KASPIAN: Well, so I find this offering particularly exciting because it basically gives smaller clients -- those typically ranging in size from, say, 100 to 1,000 employees -- the same security testing suite used by large enterprises and gives them access to technology they may not have been

able to afford previously. And this includes special licensing and pricing, which makes it attractive for these organizations.

The other nice thing about this edition is that it also includes quite a few ease of use features, such as wizards. It even has fully integrated Web-based training modules. And this means a wider range of people within the organization can perform security testing with little experience or expertise, without a dedicated security resource.

MATHENY: So how does IBM Rational Appscan work?

KASPIAN: From a high level, a client can actually point IBM Rational Appscan Express Edition at the environment and it will actually automatically discover, start a vulnerability testing sequence.

And one of the things about the solution is that it not only identifies these vulnerabilities with a very high degree of accuracy, it clearly explains how to actually fix them. So this means that the user doesn't need to necessarily be a Web security expert.

In the case of a SQL vulnerability where a hacker can potentially get confidential information from the back-end

database, Rational Appscan Express Edition will actually recommend that a developer sanitize his character input on all Web forms. And what this basically means is that developers should remove the ability for users to enter potential dangerous characters such as the percent or the pipe sign -- characters typically associated with a command and not normal user input.

MATHENY: Well, thanks, Paul. This is interesting stuff. To find out more about how IBM can improve your organization's ability to protect its Web applications, contact an IBM representative at (877) 426-3774. Please reference Code 108BM46E. That's 108BM46E.

Also, to find out more about IBM's full set of security solutions including IBM Rational Appscan, please visit www.ibm.com/security. Paul, thanks again for joining us today for Effectively Addressing Web Application Security with Limited Resources.

KASPIAN: Thank you, Angelique.

MATHENY: If you're 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. Keep tuning in as Rational Talks To You.

[END OF SEGMENT]