IBM Podcast

MATHENY: Welcome to this IBM Podcast, What, Why and How of Application Security. I'm Angelique Matheny with IBM. In today's podcast, Jack Danahy will explain why application security is a critical priority for 2010 and beyond. Jack will highlight the drivers in the marketplace, define what application security encompasses, and explain the business impact of developing an application security strategy.

He will also provide some insight into how to get started on implementing an application security process and give examples of best practices of a solid application security approach.

And as I just mentioned, joining us is Jack Danahy, Security Executive with IBM Rational Software and formally the founder of Ounce Labs, an IBM Company. Hi, Jack, welcome to the podcast. Thanks for joining us.

DANAHY: Really happy to be here.

MATHENY: Let's start with this. Why is application security such a hot issue moving into 2010 and beyond?

DANAHY: Well, I think we're in the middle of a crescendo of application development and application deployment. We find that the new framework, SOA oriented

architectures, the extension of things like the electrical grid to include more applications intelligence, are all examples of how applications themselves are becoming so much more pervasive, such an essential part of the way in which organizations are growing and changing, the way they're dealing with their customers, their partners and their own businesses internally.

And so it's natural that the security ramifications of deploying all these applications are becoming, as well, a very, very important source of concern for people. And so as organizations begin to look at these applications and they begin to think about the ways in which they're exposing themselves in a positive way, they've also taken time to look at the ways in which they could potentially be jeopardizing their existing business and jeopardizing the success of their ongoing, forward looking business goal.

And so applications is that place where they're focusing a lot of their effort. They've typically done a very good job over the last 10 or 15 years in understanding the established security technologies for things like networking and operations, and managing things like access control or authentication.

But now, as these applications roll out, they're really changing the game. In many ways, these applications can

live in a couple of worlds. Sometimes they can have portions of their behavior inside a firewall and sometimes a portion of it will be external to the firewall, perhaps the Web facing front end to a legacy back end application.

And so the problems are not just the threat surface that gets exposed with this new application, but it's also this composite: this composite of behaviors of what goes on outside the firewall at the front end of the application and all of the possible unintended consequences of that new exposure to the internal application.

And so all of these things are conspiring. The influx of new applications, the increased importance of those applications for core business goals, and then the difficulty in terms of understanding the way in which all these components will play together, these things are all driving application sort of prominence in the current year.

MATHENY: Jack, application security is very broad. Can you define what technologies are included in this space?

DANAHY: You know, it's interesting when you think about application security, because it's really two very different sorts of technologies.

There are enablers of security with an application, and then there are those applications themselves and those

technologies which will try to protect an existing piece of software or application.

So if I think about the enablers, these are things which have been around for some time. Application security is often times enhanced by things like cryptography and good identification management. And, monitoring systems -- again, technologies that have been around for a while.

Protecting the applications, though, is a space that's relatively new. There has been in existence a bit of testing for security for a number of years. You know, going back to the beginnings of the Internet age where people would test Web sites and would test the infrastructure itself to make sure it was up to current versions of software. This type of security has existed for a while, and it has more recently been applied to the application.

Good testing technologies have existed for some time. When one looks at technology such as penetration testing which is an application, particularly a Web application focused approach to the security. What's going on as an exercise of that application, a look at the application from the outside the way in which an attacker might view it?

And so in this way one can exercise the various inputs and outputs of an application and understand whether or not

there is an exposure in that threat surface that could cause the application to have some problems.

Newer technology that is arriving are testing the application in different ways, applying application security earlier in the development lifecycle. So while a penetration test is an excellent way to find prior to deployment whether an application in its fully functioning sense will be secure enough...

There are also ways in which to apply analytic techniques to look at the application while it's under construction or as its being acquired prior to its deployment by looking at the component building blocks of it, by trying to understand the way in which the application itself will actually behave over time by looking at the ways in which it has been built.

So application security covers this wide range of topics, ranging from those technologies that one uses to integrate within the application to make it behave securely. Those technologies which can be used at build time to scan source code, to scan binary objects, to really look at the way in which the application is developed.

And then also, application security refers to those technologies which are used against an application as it's deployed or as it's about to be deployed to see how it's

going to function in real time.

MATHENY: So what are the benefits to an organization of rolling out an application security strategy or policy?

DANAHY: You know, a lot of organizations have taken the tack over the course of time that security strategy was I'm going to go test and see if I'm insecure -- that I'm basically going to look at the world in which I operate and I'm going to try to figure out how insecure it is.

That's very much a reactive approach. It's good if you've got nothing else. And it's particularly good if you're just getting involved in terms of Internet work. But for most organizations, particularly organizations of any size, those days are far behind us.

A real security strategy is trying to think about, how do I avoid running into those problems at the end at all? How do I find a way in which to save the time and money and embarrassment of having application security breaches at the end of the cycle by figuring out how I eliminate them further forward in either the development or the acquisition of the software?

So when I think about organizational benefit, you know, it can be captured in a couple of different ways. Number one,

there is this lack of disruption that happens with a good strategy.

When a security event happens to an application, you can think about it as sort of being on a ship and somebody suddenly sees something right in front of the boat and say, oh, stop. Right, so you've got a business, it cruising along, applications are servicing customers or partners and everything is great until something bad happens with security.

Then really everyone has to evaluate and everybody has to stop. You know security vulnerabilities are not like functional flaws. They're exposing information or they're exposure services or they're exposing customers to real damage and danger.

And so what ends up happening is there is an enormous disruption of the way in which that organization would typically be doing its business, and particularly in the way in which that organization would be dealing with these applications.

So, disruption is one thing which one can really minimize by doing a style of strategic application security. And one less catastrophic way in which it eliminates some of this disruption is by the way in which it enhances testing of the

technology.

So if I plan ahead of time to check my components, to check my application as I build it for security problems, then I'm much less likely to run into serious issues at the end of a product development lifecycle, as an example, which could cause me to slip my schedule or to be forced by schedule pressures to deploy a piece of software that I know is not secure enough. So really, one key goal is this sort of elimination of disruption.

And disruption doesn't just cost time. Right? So a second benefit of having a real strategic approach is one of cost. The idea that at the end of a lifecycle, I'm going to suddenly have to redo everything and retest everything, that is an unbudgeted expense. No one expects to screw things up as they come into the end of product delivery. One expects that the product is going to be delivered.

And so there's an enormous amount of cost that can be saved by eliminating that end run at the end of the lifecycle where everybody has to get all hands on deck and they're forced to redo a pile of work that has already been done.

Secondly, money can be saved through better relationships in the strategic application security perspective by outsource providers, by articulating strategically to the outsourcer

the type of security that's looked for and the types of testing one expects to have done.

You can have a much greater sense of confidence that when the application arrives from a vendor, it's going to be constructed to the security standards of the organization that's asked to have it built. So the second value of this application strategy is one of cost savings.

The third, and I don't think you can really oversell this, is the fact that it's a very good awareness generator. Any time I begin a strategic program, it typically doesn't end up happening in a room with three people sort of with an idea of their own.

A strategic program forces buy in and communication among various organizational groups. The management team has to buy in to the fact that people will be working on it. The development team has to buy in to the fact that this is an important criteria, that's as important perhaps as functionality. Business unit members understand that this may have an impact on schedule and on cost, and will have to measure the benefits of it.

And through the course of this conversation between everyone from financial officers, the business unit managers, the development managers, the developers, that communication

will force a discussion in a common language about what the application should do and what the priorities are for the organization in that application's ultimate function.

And so the third benefit -- that benefit of awareness that this kind of a strategic program can bring -- is really enormously important, particularly in these dynamic times when its very likely that the same organization may well be developing another and another and another application over time, all of which will benefit from this raising of the baseline of knowledge of what secure behavior and secure applications really mean.

MATHENY: Jack, we'll end with this question today. Where should organizations begin?

DANAHY: When I'm asked by various groups I see about where to do I start, it's a very common question, its been a common question since anyone's bothered to take a look under the covers for the very first time in security, because invariably there's a lot of things that you find.

You know, I try to ask people to take a step back and figure out why they're doing what they're doing. You know, why do they care about application security? Why do they care about security in general?

There is a piece of all of us which cares about it because it's the right thing to do. We are worried about our organization, we're worried about our employees, we're worried about our customers, we're worried about our data and our business.

And so it's natural to worry, but in the abstract about security. But that abstraction it's not really something that's actionable. And so if you start acting out of emotion on security, you're going to tend to try and do things which will give you a very short-term view of improving your security and you won't be doing all that strategic work we talked about in the earlier question.

So I ask people to take a step back and think about why: why are you worried about this and why are you creating an application security program? For some people, it's going to be very straightforward. It's going to be compliance as an example. They're being asked to comply to either the internal or industry standard, one which calls for them to demonstrate why they're secure.

And so in this case, the application security planning and the security strategy is geared to generating automatically or at low cost those artifacts that will help them demonstrate that compliance while also enhancing the security position.

A second people why people can get involved tends to be that they've had some sort of horrible event. They've lost some customer data, they've had an insider breach, integrity has been lost somewhere in a financial system. And so for these people, they have a different set of priorities.

Number one, they are naturally acting with a very high sense of urgency. They either have to understand what's happened to make sure it doesn't happen again or perhaps they want to find out what happened so they can figure out who to capture or punish for the behavior that's gone on.

And so their decisions are going to be different. Their decisions are going to be based on understanding the root cause of the behavior and understanding ways in which perhaps the next time they can gather more information more naturally through the course of the application's operation.

The third reason why organizations may get involved is because they sort of see the train coming. And I think we're seeing more and more of this inside the marketplace -- that organizations see that applications are the massive driving force, and they also see that in a variety of industries, everything from industry bodies to legislative have recognized that software is going to be a big and critical component at the center of things which are

important.

If you looked at regulations in banking or in energy, you will find that there's reference to ensuring that components are secure. And so organizations which are looking ahead will recognize that in the coming three, five to 10 years security is going to be a table stake.

And you're going to have to have a good security program in place or otherwise you're going to be running around like crazy, disrupting the rest of your business to make up lost ground that you could be proactively planning for right now.

And so the first step for so many of these organizations is to look inside themselves and understand why they're getting involved in security, and particularly in application security.

And based upon what they're looking to get out of it, ensure that the progress they make along that path is appropriate to goal they intend to hit and not just take short-term stop gap measures that may solve symptomatic application security issues, but not really achieve for them the overall benefit that they're looking for. It's a complicated problem, but the way in which to start is to look at why you're trying to solve it.

MATHENY: Jack, thank you so much for sharing your time today to explain the what, why and how of application security. We really appreciate it.

DANAHY: It's been my pleasure.

MATHENY: That was Jack Danahy, Security Executive with IBM Rational. If you're interested in more podcasts like this one, check out the Rational Talks To You page at www.ibm.com/rational/podcasts.

To learn more about how to automate application security, download a trial copy of AppScan from developerWorks. We'll include the link on this page to help you get started today. This has been an IBM Podcast. I'm Angelique Matheny. Thanks for listening. Keep tuning in as Rational Talks To You.

IBM Podcast

[END OF SEGMENT]