

Web Application Security Survey & Analysis with Jeremiah Grossman – CTO WhiteHat Security

Listen to Podcasts: <http://www.imperva.com/resources/podcasts.asp>

Brian Contos: Welcome to the Imperva Security Podcast. I'm Brian Contos, chief security strategist for Imperva.

Joining me today is Jeremiah Grossman. Jeremiah is the founder and CTO of WhiteHat Security. Welcome back to the show, Jeremiah.

Jeremiah Grossman: Thanks for having me.

Brian Contos: Jeremiah, before we begin, what exactly was this survey and why was this an important survey for us to conduct?

Jeremiah Grossman: Like a lot of experts, not just our companies - that is WhiteHat and Imperva - we had some ideas about how organizations viewed application security. We had some theories we thought were pretty well sound given the media out there, but we wanted to somehow validate some of our surveys and get some survey data. So we got in touch with the Ponemon Institute and said, "Here's a list of questions we'd like you to ask organizations, and let's see what the results actually are."

Brian Contos: What perhaps were some of the more interesting statistics or more interesting findings that came out of this research?

Jeremiah Grossman: Sure. Again, we wanted to focus on application security, but it looks like even today the mainstay of how security is approached is very network-centric. But if you look at the last several years of breaches, it's heavily weighted towards application security as the main vector to penetrate these companies and compromise their data. And if you look at all the spending, how companies invest in their IT and how they invest in security, it seems diametrically opposed to what the threats actually are.

To give you an idea, most of the focus and most of the dollars are spend on network security, which don't do anything to really prevent today's threats. So we wanted to put some hard numbers behind this stuff. Is application security seen as a strategic initiative? What is the spending really like? And start focusing on more high-level concepts.

Brian Contos: Yeah, I guess it's analogous to saying you've got a problem with people breaking into your building through the windows, so you keep on buying stronger doors.

Jeremiah Grossman: That's pretty much the way it worked. We had some interesting numbers. Just to give some numbers, by volume, of the last top 100 breaches, 93% were due to weaknesses in the application or database. Only 7% were network-related. But if you look at how budgets are allocated, only 18% of the security budget is allocated to protecting the web applications. So we have this diametrically opposed kind of budgetary thing, and we're hoping to see that change.

Brian Contos: Did these results, at least at present, help validate not what you think should be, but sort of what you thought the market was like, what you thought most businesses were doing in term of app sec?

Jeremiah Grossman: It really did actually. We have the benefit of being able to talk to a whole lot of companies. I talk to many Fortune-listed companies, many startups, all the time on their application security initiatives, how they spend, how it's allocated, how they view application security. So I've already done my personal surveys. But more than my personal feelings, I really wanted to get something more formal done, which is what this report was all about. Something that everybody else can reference.

Brian Contos: Yeah, absolutely. Even though we helped sponsor it, the results were what they were, good or bad. One of the things that I'm wondering, you've been in application security for a very long time, there's always been this, "We're going to invest in network security." We understand application security is a problem, but we're just not making a big enough investment in that arena.

Why does this still seem to be such an issue? Is it too abstract of a concept for some people? Is it because the security people that are championing the solutions that are put in place tend not to be application security experts? Why does this remain to be such a problem?

Jeremiah Grossman: The way I've seen it best said is by way of a gentleman by the name of Gunnar Peterson. The way he looked at it was if you look at how information security budgets are formed, you take last year's budget, you add a little bit more for today's threat, and then you add some fudge factor in there and, viola, you get an information security budget. Which has nothing to do with the threats that a company might be exposed to or their investment in their IT. As an alternative, one way to go about it - and this would require a complete cultural shift - is that the organization looks at how they invest their IT dollars and where their value assets actually are.

If you make 90% of your revenue via web-based applications, maybe we should start treating security as a tax of sorts, and say, OK, if you're going to spend X amount of dollars here, perhaps the security tax should be allocated there.

Just like many other areas, from car insurance on, you allocate your security commensurate with how much you invest in that particular asset.

Brian Contos: Very interesting. Like carbon emission credits for security.

Jeremiah Grossman: [laughs] That could be one way to look at it. And then what you might have is something more reminiscent, you spending the right amount of resources to protect something of the right amount of value. Right now we seem to be spending gobs of money protecting something that the business doesn't really value all that heavily. They value their applications, not the infrastructure below.

Not that we should leave it completely unprotected, it's just what the data showed is we're completely out of whack.

Brian Contos: Yeah. Because we're following what we did for the past decade, which was focusing on the network security as opposed to what today's newer threats are. Yeah, that does make a lot of sense. When you look at the report and it's talking about writing secure code and security development lifecycles and how much it costs to write secure code or how

long it takes for organizations to patch application vulnerabilities, what type of interesting things did you glean from the results that were focused on that arena?

Jeremiah Grossman: I think at a more fundamental level if a company is able to ask those questions, they're more mature than most. When you start looking at where companies actually are and are supported by the data, most of these organizations don't even know what websites they own, let alone what they're worth, let alone what they're vulnerable to. And without those three data points, you really can't even start going, "What should our SDL address?" It can't address everything under the sun all at once. These things take time. So you want to focus on the right areas. But without fulfilling those fundamental steps first, where most people are, you're building this gigantic engine that might not drive the business at all, because you're in a completely different place.

Brian Contos: What were the glimmers of hope, if any, did you get from this. Where there any, wow, this is great, I'm glad we're moving in this direction? Was there anything very positive that came out of this?

Jeremiah Grossman: Oh, I think most of the report was very positive. It showed that the information security people that we were asking these questions of knew the threats, they knew the real threats. They knew where the organization stood on it. They were like, OK, web security is the major threat, or organization doesn't see it as a strategic necessity just yet. Just the awareness of where we are and where we should be heading, it was there amongst the IT security professionals. Three years ago, five years ago, it definitely wasn't there at all. This very same survey, my thinking, would have been completely different three to five years ago.

So it shows we have to have the awareness, the idea first, and then we can start making progress. So that for me was very encouraging.

Brian Contos: Surely awareness is a big point. It would be interesting to have a similar survey a year or a couple years from now and compare those results as well, just to see if this awareness has increased and if that awareness has led to actual changes within this approach to security overall.

Jeremiah Grossman: And that'll be the thing. We have to start looking at our outcome-based metrics, continue looking at how the bad guys are breaking in, how they're stealing their data, and start tying our best practices to the eventual outcomes. We've got to stop doing the things that obviously don't work, and start doing and trying new things that we think will.

Brian Contos: Jeremiah, as we wrap up here, obviously you're representing VA and Imperva's representing the web application firewall side and the database security side. None of us, I think, would say that WAF and VA and end-all and be-all of security. But if you could just sort of summarize, why are these two pieces, especially these two pieces, operating in tandem really so critical for application security?

Jeremiah Grossman: Let me take a step back and address that a little bit differently. When you look at network security, nobody says network vulnerability assessment is the end-all, be-all. No, you need network firewalls, you need intrusion detection systems, you need patching and scanning and all these things to create a holistic network security program that might actually work. And the same thing has to start happening in application security and that's what happens with the awareness over time. Yes, you need application security and vulnerability assessment, because you have to know where your vulnerabilities

are so you can address them. You need visibility and to be able to have protective response via web application firewall.

Preferably, you would not want to have applications consistently full of holes. A nasty OF, that would be huge. And to get all these things working in combination are the big wins.

That's the big wins that our customers are seeing is when we find vulnerabilities that they may or may not be able to patch in a quick fashion, they may be able to do a virtual patch. Take the data that find at WhiteHat, put it into an Imperva SecureSphere, and the get a virtual patch, which gives them some breathing room to fix an issue.

Those are some really big wins, because it's not so much about getting code perfect all the time, much of winning the web security battle is about being able to react fast. It's usually those vulnerabilities that are in the system for months and years that are the cause of major breaches, not the ones that are in there for days or weeks. And that's what we have to try to get to with virtual patching.

Brian Contos: I guess one way to say that is that it's not 100% about the preventative mechanisms as much as detecting and being able to quickly respond to those in terms of a real-life solution.

Jeremiah Grossman: Exactly. Unless somebody is prepared to say we can get 100% effective guaranteed preventative measures, unless somebody can actually say that, you're going to need visibility, monitoring, and the ability to respond. So both halves are required.

Brian Contos: Yeah. I think to get that first half, first we'd have to build a time machine and go to the future and find and SDL that's absolutely 100% perfect.

Jeremiah Grossman: Yeah, that's on the next roadmap. [laughter]

Brian Contos: Jeremiah, as always, thanks for joining us on today's podcast.

Jeremiah Grossman: My pleasure, Brian. Thanks for having me.

Brian Contos: For more information on this podcast and Imperva, please visit imperva.com or send us an email, blog@imperva.com.



Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004