INTERVIEW WITH MARC VAN ZADELHOFF

Eric Green: Hello and welcome to a new podcast series from IBM software that explores the challenges IT managers and business professionals are facing today. I'm Eric Green and I'll be talking with a range of experts to discover new perspectives, approaches and examples that can help meet these challenges and introduce you to the capabilities of smarter software from IBM. So let's get started.

Welcome back to the show. So today we're going to have a security overview, after which we're going to drill down a bit to discuss security governance, risk management and compliance. To do this, we have Marc Van Zadelhoff, who is Director of Strategy for IBM Security Solutions. Marc, thanks so much for joining us.

Marc Van Zadelhoff: Great to be here, Eric.

Eric Green: So to start with, I was in hopes you could give us an overview of the state of security today.

Marc Van Zadelhoff: Sure, I don't think I need to help too much there. All you have to do is open the front page of the newspaper and I think the overview has been flashing before our eyes. So we had, you know, a whole bunch of activity – probably the fervor started with Wiki leaks, which is an excellent example of insider attack, essentially what we call an insider threat, where somebody that's very trusted ended up providing information externally, obviously violating policy, in this case, Army policy. It's really blossomed from there.

We've had the anonymous and other groups out there doing various activity and breaking into a number of companies, and it's been – I think, you know, what the headlines have shown is that we've gone through a lot of waves in security and, you know, people like to pontificate about those waves. But we're kind of back in a wave of prestige hacking. You know, we hadn't seen this for a while where the primary motive has been, you know, monetizing, data hacking to make money. But right now we're back in this prestige area, where the reason people are breaking in is really to show that they can, to maybe do some whistle blowing, some exposé on somebody to get some attention. So that's a – it's a very interesting world that we've come into, the headlines are showing that. And, you know, the other motivator that's been different is cyber attacks, you know, state and non-state actors trying to get in, not for prestige or for money, but literally for perhaps national security or corporate espionage.

So this has really taken it to a new level, the headlines are showing that, and every conversation we have today with not just security people but CIOs and CEOs, security is a topic that’s top of mind.

Eric Green: Yeah, I totally agree. It’s almost like we’ve taken several steps backwards in cyber crime, with these people who are now, you know, just doing things because they feel like it. It’s pretty frightening. It was a lot easier when we knew that organized criminals were after money and state sponsored folks were after intellectual property.

Marc Van Zadelhoff: Yeah. In fact, you bring up a good point, we had – our X Force research team had done a bunch of research a year ago on why people, you know, exploit certain vulnerabilities and not others. And as you said, money was the main motivator up until about a year ago. Now that’s starting to really become less predictable, to your point.

Eric Green: So that’s great stuff, and we’ve got the headlines sort of nailed there, but what are your customers really worried about?

Marc Van Zadelhoff: Well so they’re worried about that. There’s definitely a worry that’s resonating right up to, like I said, right up to the CEO on these headlines. And, you know, I lived in the Washington, D.C. area, subscribed to the *New York Times* as an example, and it’s all over those headlines. And, you know, lots of CEOs read that newspaper just for fun and so they can’t avoid this topic. But in truth, there are topics beyond that. So that’s an important one, but there are ones beyond that. I think the next one that really hits the radar is mobile devices. And when we’re talking to Sys-Os, Chief Information Security Officers, the typical scenario is oh, lo and behold my CEO’s birthday was apparently this weekend and his kids got him an iPad, so he showed up on Monday and said, “I want corporate e-mail on here.” So suddenly mobility has become a hot topic.

Securing Cloud. A lot of buzz around that term. How do I secure cloud? Should I leverage cloud? Can I maintain that level of security? We’ve done a lot of work in that area, you know, my personal opinion is that there is the potential that the cloud could be more secure, but there are huge risks that you need to think about.

Social business is another one. Customers want to start Facebooking and Linking In and my employees want to do this. I think I want to use this as part of my business model. It seems like the way to innovate right now, but it really scares me in terms of security.

And then a final one for you is compliance. You know, I've been in this business for quite a while and I was thinking that compliance would sort of go away at some point as a topic. But it's still there, getting into compliance is a big challenge.

Eric Green: You know, what I think is so interesting about where we find ourselves is, you know, you mentioned mobile, you mentioned cloud and you mentioned social media. They're all incredibly related when it comes to our security posture, right?

Marc Van Zadelhoff: Yup.

Eric Green: Because the only way you're ever going to secure I devices in the end of the day, because you can't do anything on them, or Android for that matter, you're going to be using the cloud. And even Apple turned around with this crazy iCloud thing, right?

Marc Van Zadelhoff: Yup.

Eric Green: What person is using their mobile device and not using social media? So you've got this blend of everything hitting you smack, you know, right between the eyes all at once.

Marc Van Zadelhoff: That's right. And you have this blend of personal and private in all those things you mentioned as well. I mean, so my iPad. I have my corporate e-mail on there, and so let's say my employer, in theory, says I have the right to wipe your iPad if you lose it. But my iPad's got my pictures of my kids on there and it might have, you know, personal data, like some records from a recent – I don't know, medical exam that I had or whatever that are critical to me. And let's say I lose it, and then my company the next day decides to wipe it. Right? Suddenly they haven't just wiped out my corporate e-mail and some files that I might have stored on there, but maybe they wiped things that are near and dear to me personally. And who has the right to do that? And is that the company's right to wipe a device? And so you get into this whole blurry area. It just used to be people would come to work and might mix, you know, shopping on Amazon.com or looking at their yahoo accounts with their work, on their work computers.

Now this is happening on personal devices. Who owns the data on them? How do you think about that problem? So it's really – it's causing a lot of deep thinking and we're helping customers think through these problems every day.

Eric Green: Yeah, the personal corporate liable thing is – I mean that's front and center too. So great, now how do you go about – I mean you were touching on this, but how do you go about organizing this security approach for customers given all of these things going on?

Marc Van Zadelhoff: Sure. So I think that's the challenge, and we're really trying to make it simple for our customers. And maybe I'll start with what we call the IBM security framework, and it really is a derivative of the cobit methodology for thinking about risk. You know, we try and go from all this confusion, the hundreds of headlines, the hundreds of topics that we could talk about down to, kind of, five plus one areas of risk that you need to think through. And I'll explain what I mean by five plus one.

So the five are people and their identities. Right? Think about people and their identities, how is coming in and out of your building. Right? That's one vector of risk you need to think about. Data and information is the second one. So where's the secure data in your building, how do you classify it, how do you know it's not leaving in a promiscuous fashion? Applications and your business processes. Same thing. How do you know your applications are well developed? How do you know that they are secure? How do you know they can't be hacked? Apps are one of the largest attacked surfaces today, as proven again by our X Force research team and other researchers. So, you know, think about your identity, your data and your applications to start off with.

The fourth dimension is think about your IT infrastructure, your network servers and endpoints. You know, do you have control of that infrastructure, where are they residing, who owns them, how many of them do you have? You know, we rolled out an endpoint management technology that we have called Tivoli Endpoint Manager out at a customer who thought that they had, you know, 10,000 endpoints out there. By the time we finished scanning, they had about 25,000 endpoints – just more than double what they thought was residing on their system. So do you have control of your IT infrastructure is a fourth category.

And the fifth is your physical infrastructure. You know, guards at the doors, badge readers, digital video surveillance, etc. Physical security – are the doors thick, are they well locked, are they, you know, secured. So those are the five domains of security that we help our customers think through to try and – almost any problem you can throw against that. You can say mobile devices. You know, what are the people implications, the data implications, application implications, the IT infrastructure implications, and then, you know, to an extent the physical security implications of those devices. So you can go through all five of those. And then the six, or the five plus one, the plus one is governance, risk and compliance. So even if you do all of that, it doesn't add a heck of a lot of value if you thought each one of those through if you can't step back and make sense of that from a governance, risk and compliance perspective. So whether that's the first of the six or the last, you need a good sense of your governance, risk and compliance posture.

Eric Green: That's a perfect transition. I mean all of these different pieces fit into your risk posture and how you're dealing with security as part of your overall risk management strategy.

Marc Van Zadelhoff: Yeah.

Eric Green: And as we've said, you know, governance and compliance are such a huge piece of that. Can you talk a little bit about that and how you're helping customers sort of grapple with dealing with governance and compliance in the different regulatory environments.

Marc Van Zadelhoff: Sure. So, in fact, it really is all around making risk management an enterprise risk process – part of your enterprise risk management process. You know, I think for a long time, security has been the red-headed stepchild of the risk management process. So people were really comfortable, you know, CFOs were thinking about, you know, what's my audit risk, what's my financial risk, what's my market risk? You know, should I enter this particular market? What's the risk of that? If I go do business in China or Russia, you know, what are my risks? Right? So people are very used to doing risks, you know, they're used to insuring their risks, they're used to mitigating their risks with various methods, and then there's security. Security was like yeah, yeah, you guys down there in the basement, you keep us secure.

And I think that, you know, going back to the beginning of our conversation here, Eric, is that the real change that all of these headlines have brought about is that companies more and more realize that security needs to be a pillar within your risk management program. And, you can really treat that risk very similar to other risks that you have. You can assess – if you have the risk, you can measure the risk, you can figure out, you know, if it's a high or low priority. Not all of them need to be handled equally. You can do mitigation strategies and then you can monitor whether those are working and improve on them. That's a normal risk process that we walk customers through.

So IBM's entire, you know, governance, risk and compliance practice starts with a risk assessment and starts with thinking about risk as part of enterprise risk and helping customers to do that. And it moves into other things, like how do you make sure that you're not doing this alone? You can think of a risk ecosystem that involves your partners, your employees, your customers, your auditors, your regulators. So how do you make risk part of your overall management system and security a part of that? So that's kind of at a high level how we think about GRC.

Eric Green: Are there some examples of success stories and/or ways customers are dealing with this whole security continuum?

Marc Van Zadelhoff: Yeah, I mean, you know, so IBM is one of the largest security companies out there, and so we have thousands of customers. So I thought you might ask about examples, and my only struggle is to try to narrow it down to a couple. You know, I sat down with a retailer the other day, and they are really deploying our technologies across the five plus one categories I mentioned, I think they cover almost each of them. They have our newly acquired database monitoring assets. We acquired a company called Guardian that they've deployed out to monitor all of their database security, so that's at the data layer.

They have rolled out identity management solutions that we have from IBM Tivoli, doing identity right into their service oriented architecture, right into their applications. They're doing a huge services project with us, where they're leveraging our application scanning technologies to go up and down the application stack, and they're deploying our endpoint management capability to help them think through how many endpoints they have and how to manage those, how to keep the patches up to date, how to manage software updates to that and how to manage anti-virus and anti-malware capabilities on those devices. So they are, you know, a pretty large customers using capabilities across the various parts of that stack that I mentioned.

You know, we have 4,000 customers using our managed security service. We helped a large industrial company recently to set up an entire security portal off of our managed security services. So they can log in and see how secure they are based on all of the events that we're monitoring. And you think about billions of events a day that we monitor on behalf of a customer. And so they are able to log into their own customized portal, see what events are happening, what we're helping to combat. That helps them get to PCI compliance. But it also gives them a whole level of security analytics. This is a whole new area that IBM is getting into is security analytics, that they are able to see on this customer portal because of all the data that we're monitoring.

And then maybe finally, you know, we're working with one of the agencies, again in the area of analytics. Not with our managed services but just with some of our analytics technologies, to go and troll through mega amounts of data and understand whether or not they might have some advanced persistent threat or other threat that they're not catching with their existing security technology. So it's an example of going above and beyond all of the capabilities out there with some advanced analytics on their platform.

So, you know, a lot of – like I said, we have a lot of customers to choose from, and I could go on and on about customer examples, but those are three right there to think about.

Eric Green: No, those are great. I mean they're very valuable. And the audience likes that, right? I mean that's great for listeners to sort of see where the rubber meets the road with this. And to that end, you know, how would you see, or how do you see IBM as innovating in this space?

Marc Van Zadelhoff: Yeah, so I think I would start with the whole area of analytics. I mean this is an area we see a lot of potential, you know, where you can take – what we're seeing customers come at us and say – you know, I've bought lots of security technology from lots of vendors, right? That's first of all a big challenge that customers have. And I'm not quite sure if it's actually working and if I'm secure. And so we'll help them with analytics, where we go and use some of our advanced analytics technology. I mean, think about the fact that we just won a game of Jeopardy with our Watson computer. Right? If we can answer Alex, you know, Trebek's questions about random facts, we've got to be able to bring some of that technology to bear on – am I secure? Right? There's a great Jeopardy question, right? Am I secure? Or I guess that would be the answer in Jeopardy. But this is one area that we're doing a lot.

The second area is mobility. We are rolling out our endpoint management technology, which we acquired Big Fix out to mobile devices. So that's been a huge area. And a third, again not surprisingly, because we talked about these in the hot topics, is around Cloud. We have a number of solutions that are helping to secure the cloud, you know, intrusion prevention in the hypervisor is one. Federated identity, that allows you to federate, as the name would indicate, identity across from your corporation into your cloud service provider would be another.

And we launched, last year we launched cloud security assessment. So if you're thinking of adopting cloud, we'll come in and send a SWAT team that understands the risks of cloud and do an assessment of that. So cloud is a third area of innovation. So we've done, I think we've done, you know, 11 acquisitions of security companies in the last ten years. And we've, you know, more than tripled that in terms of new offerings we've introduced in that same timeframe. So the innovation here will be both things that we build and things that we acquire, to make sure we're helping customers do what they need to in security.

Eric Green: Excellent. Well I want to thank you very much for your time. I think that's all the time we have for this podcast, but Marc, thanks for joining us.

Marc Van Zadelhoff: Okay. Thanks Eric.

Eric Green: So to our listeners, be on the lookout for the rest of our security podcasts, which will include such topics as data and information, people and identity, application and process, network security, and of course endpoint security, all of which we touched on during this podcast.

Thanks for listening. Please do visit IBM.com/software to connect with our experts, continue the conversation, and to learn more about smarter software from IBM. Let's build a smarter planet.