NETWORKWORLD

CSO said Cisco security is growing up

By Robert McMillan , IDG News Service, 08/06/2008

John Stewart doesn't talk like your typical corporate executive. He said that his company, Cisco, has been lucky when it comes to security and that his company's Self-Defending Network marketing push has painted "a big bull's-eye" on its products.

But then again, Stewart has more important things to worry about. As chief security officer, he's the man responsible for directing Cisco corporate and business unit security practices. That means he gets the call whenever there's an important security bug in Cisco's products or if hackers were to hit the Cisco.com Web site. The way he puts it, it's his job to help lock down Cisco's products before he's forced to deal with what he calls "the burning platform" -- a serious flaw or attack against the most widely used routers on the Internet.

Maybe Cisco needs someone like Stewart, to steer clear of the mistakes that other major technology companies have made on security. Take Microsoft, for example. Microsoft first took a hostile attitude towards security researchers and critics, but that backfired and helped cement the impression that the company was ignoring security bugs rather than trying to fix them. Microsoft ultimately reversed its course, but not until its reputation took a serious hit.

On a smaller scale, Cisco has made a similar kind of reversal. The company angered hackers in 2005 by suing researcher Mike Lynn after he showed how it was possible to run unauthorized shellcode software on a Cisco router.

But instead of kicking off a new era of Cisco hacking, the Mike Lynn episode was more of an aberration. Cisco research was quiet for the next few years.

Stewart said that Cisco has been "a little lucky" in that it has not had major security flare-ups, but he's not taking anything for granted. He invited IDG News Service to his San Jose office to talk about the Cisco threat landscape. Following is an edited transcript of the interview.

Cisco got a lot of attention at Black Hat 2005. What's your take on things, three years later?

Part of the reason all the attention was painted on us at Black Hat three years ago is because we created a firestorm of, frankly all sorts of complicated issues, that felt like Cisco was suppressing communication and research.

I think arguably we did some silly things, like trying to put the genie back in the bottle, which you can't do. We were trying to do it for the right reasons: protection of intellectual property and our customers. But how it came out just completely went sideways.

And, in many respects, we did it anonymously. It was "a Cisco spokesperson." We sort of hid behind an anonymity context , which I think really goofed everything.

This is why I personally sponsored Black Hat at the platinum level ever since. Because I think we had some atonement to do and go, "Look, our bad. That was not the way to do that one."

Why do you think the Cisco research dried up like it did?

There are a couple of reasons. The first is, a lot of this is not remote exploitation, and a lot of what the research is about in any community is, "How do you do it remotely?" IRM's [Information Risk Management's] research, Sebastian's [Muniz, a researcher with Core Security Technologies] research, and to a certain degree, Michael Lynn's research, although it had a slight remote variant, it's not stable remote. And that's where the real game is.

You have got to figure out a way to get it in without being on the console. And that's what most of the development's been around: how do you do it on the console -- at least for Cisco, anyway.

And the second thing is, you want it to work. You're not trying to knock it out because you need the network up so you can get to the end point. So I think we sort of get a pass because no one wants to monkey with the infrastructure that they're using. It's like screwing up the freeway while you're trying to go to a different city. That's kind of a goofy thing to do.

Microsoft has been very public about how they changed the company to make security a priority. What's the story at Cisco? How did the security program get built?

We were probably in the same space. Many companies, including our own, started with building stuff first that solved communications problems and then thinking about the safety of communications afterwards.

About five years ago, we were fighting the company, my team. Mostly in the information security business. We were the "no" organization, the ivory tower. That's a dangerous place to be because my take is we ought to be a consultative fulfilment arm, not an adjudicator.

So we changed a lot of it and we started injecting things, like "You're going to have expertise in your team. We're not going to be even in the middle, so that way you can

invest the expertise for what you need and we're not holding you up or bringing you into a slower position."

The second thing -- that can't be underestimated -- is we were getting ready in 2002 to launch self-defending networks, which -- like it or hate it as a slogan -- effectively is a big bull's-eye on our forehead.

Like Oracle's unbreakable Linux?

In fact Mary Ann Davidson over at Oracle dropped me a note and said, "thank you very much for coming up with a slogan that takes the pressure off what we've done," [laughs] as if I had anything to do with the announcement.

And then third, we've really had a footprint grow. We got used in more and more places, and frankly for thinks we never imagined we'd be used for. We're transitioning health care communications, we're transitioning site-to-site communications for the military. We're doing all these wild things that 20 years ago we didn't think about at the time.

So did you do something like adopt a secure development lifecycles or change the way you built products?

We're not mature in this. We're in the awkward teenage phase. We're testing at the end of the development process and we're figuring out from that data how do you go backwards into the definition process. Now some definition happens anyway. So for example there are some baseline requirements of every product we built. However, I still say there's a lot to be learned. When you think you've got it right and you build it and you test it, the learnings from the test should benefit the next thing you build.

We haven't adopted a secure development lifecycle like Microsoft yet. We haven't nailed up equally on all product lines in a very consistent methodical measurable way, and that's why I say we're in that awkward teenage phase.

The IDG News Service is a Network World affiliate.