AT&T Wants You to Float Your Security Off into a Cloud

March 16 2007

Edward G. Amoroso, chief security officer for AT&T, says most of us have no business running a network. Businesses' infrastructures have allowed complexity to spread like a cancer, he says, and most times we simply don't know what's going out or coming in.

"We have a service where we send out advanced notice that attacks are on the way to customers," he said.

"We'll say, ' - Check out - UDP 1712, something's brewing. Looks like a worm is coming.' And they say, 'Oh.' We ask, 'You got anything coming in? Anything going out?' They say, 'I dunno.' Most companies' answer is 'We have no clue.' Or 'We have no budget,' or 'Not enough people,' or this or that, or 'My department doesn't do that.'

"And you say, you shouldn't be running a network. If you can't monitor and understand goesintas and goesouttas of your network, you shouldn't be running a network."

This was all during Amoroso's keynote speech, titled "From Reactive to Proactive: The Case for Cloud-Based IP Security," at Ziff Davis Enterprise's Security Summit 2007 here on March 14.

Amoroso is calling for a stop to the cycle of network attacks, followed by network fixes, followed by attacks on those fixes, and on and on.

"The whole thing has gotten kind of ridiculous," he said. "Something's

not in balance when we're spending - as much on security as we spend on the initial technology - ."

At the heart of the problem are three issues, he said. First, the state of software engineering now is in "an abysmal mode."

"It's absolutely embarrassing. … It's like gangrene was treated - before modern surgery - , when they gave you a shot of whiskey and tied you down and hacked off the arm. Contrast that with how we treat it today, with surgery. Where we're at with software engineering" is the pre-surgery days, he said.

The second issue to Amoroso's mind is that system administration is also in "an abysmal state."

Amoroso was referring to what people do in their homes, not at work, with ISPs delivering attacks to our laptops and not lifting a finger to stop them.

"Right now the situation is we don't look at anything, we don't touch it, don't sniff it. We pass it along, truck bombs and all," he said. Then again, who wants their ISP sniffing around at their surfing habits? Amoroso said.

"The majority of Internet traffic and queries may be something you don't necessarily want your carrier to be logging about you," he said.

Still, it's too difficult to administer a computer in 2007, he said. Look at Vista with its vast lines of code: features keep going in, but nothing ever seems to come out of operating systems and other software.

"The less software you run, the better off you are," he said. "Look at Unix: It's bare bones, simple switching. The core fabric is pretty simple.

That stuff is still running, 40 years later. There have been a couple of problems in 40 years - and that sounds about right, that's what it should be. How come we can't do that?"

The answer, of course, is that Unix wasn't written to make money off of, Amoroso said. But it's that urge to shorten time to market, to get new technology into business and consumers hands fast, that's causing the industry's lackluster record on product security, he said.

"All this discussion around security, we're talking about the wrong thing," he said. "We should be talking about the correctness in software. It's the bugs that are the problem, not the scaffolding you build around - things like kernels - ."

Meanwhile, ISPs like AT&T are sitting back and watching the problems roll in like black clouds on the horizon, Amoroso said. They know the graphs of IP backbone traffic like the back of their hand.

One example is Super Bowl Sunday: ISPs can chart the traffic dropoff as soon as the game comes on. At half-time, ISPs see a partial traffic recovery as fans check scores and stats on their computers, and traffic rebounds after the game is over.

That intimate knowledge of IP traffic can be translated into malware awareness. In this day and age, Amoroso said, AT&T is seeing some 10 million PCs every day that are actively exhibiting scanning behavior. Do businesses recognize it? No, Amoroso said, and yet we still persist in recognizing exploits as an enterprise problem and tell businesses to shut off port 25.

Obviously, things have got to change, Amoroso said. "We need to redefine our relationship. We have a broken relationship between carrier and end user."

What AT&T sees first-hand are the class signatures of a worm: A patch is applied, an exploit is revealed, a slight ramp-up of traffic sounds a warning, and then the worm is off and running, causing IP traffic to soar off the charts as its infection rate explodes.

"It's predictable and synchronous," Amoroso said. "Post day zero, you have a code snippet, you see the - activity on the Internet become - more rapid, it spikes, you see fizzled - worm - tests, it ramps up, - it gains - volume, - it exhibits - varying strength, - and then you see worm - variants."

And much as we'd like to pat ourselves on the back when we miss getting infected, it all amounts to Russian roulette, he said.

"It's - techie people's - little secret: When you're not hit, - your supervisor - says 'Good job,' and you say, 'Thank you, we're a vigilant group. We took proactive vigilance steps, not like those chuckleheads in that bank across the street,'" he said. But next time, he said, you'll be the chuckleheads.

Meanwhile, enterprises own and operate and pay for a legion of technologies in their demilitarized zones.

"Something does not smell right about this," Amoroso said. "You watch revenue decreases in telecom, but do you feel like you're spending less in this? Of course not. It's not that there's this big giant hacking problem. It's that, architecturally, things are out of whack."

Offload it all to your carrier, put the DMZ into the cloud, and what do the hard numbers look like? Amoroso said that AT&T's statistics on the reduction of software licensing fees that would result from putting security into the cloud - for example, into the hands of your carrier - brings about a reduction of 35 percent of what businesses formerly spent

on protecting the perimeter.

Next Page: Audience reaction.

Was the audience swallowing it? Not wholly. After Amoroso's keynote, during a panel on "Security Strategies That Work," panel members brought up multiple reasons why they'd rather keep security where they can see it.

Steve Runyon, information security specialist at the Federal Home Loan Bank of New York, said that he couldn't fathom the scenario working when a business has more than one ISP.

"You have to get them to work together, and you have to manage them all," Runyon said.

Another panel member, Eric Latalladi, chief technology officer and vice president at J.B. Hanauer & Co., said that the idea of security in a cloud doesn't address an inherent flaw of centralization: namely, that vulnerabilities "seem to hover where the majority of business is," he said.

"If it collapses into all the carriers, the focus will have to be on how do carriers architect security?"

Yet another panel member, Lloyd Hession, vice president and chief security officer at British Telecom Radianz, said his business would be pleased as punch to sell security services, but he wondered if people would actually buy the add-on.

"I'm sure they'd be able to sell those additional security capabilities," he said. "But on one hand the sales guy says 'That's a fine service.' And then you have the service that's charged extra for security. It's going to take a

while for people to realize it's worth it."