Keep security simple, stupid

by Andrew McKay

Ira Winkler's well-known in security circles for his ability to break into a location – physically or virtually – and expose flaws in a company's security.

This week, Winkler, who used to work with the National Security Agency in the U.S. before moving into his current role, came to Toronto to share his experiences and shed some light on the issues he's seeing in the security world today.

The first myth Winkler addressed was that cybercrime is an art. Nonsense, he said; it's more like a science, where repeatable actions and results are put into practice.

"The most important part of being a security professional is just like there's a process to break into things, there's a process to protect things," Winkler told attendees at SecTor 2007 in Toronto.

"If you have a good process and good training, even if you have someone with aptitude that really sucks, they can be competent."

However, the rising number of amateurs makes it harder for security companies to anticipate attacks.

"What happens with most of these stereotypical hackers out there is they have this natural ability and start breaking into systems," he said.

"That makes them very dangerous because they don't have a repeatable process."

One major mistake he sees from enterprises is the belief that just because they have a person charged with security, they're protected. In fact, he said, that security staff may have fallen into a pattern of routinely checking known exploits or threats, while missing other threats.

"There are way too many people in this business who have critical applications that are insecure and they don't even know they're insecure because they're not looking for it," he said.

That being said, Winkler said it's important not to overcomplicate the issue of security. It boils down to two things: software and configuration.

"All software has bugs," he said.

"Some of those bugs are just going to create elevated privileges and leakages. 99.8 per cent of problems, in my opinion, are completely preventable, if people would have provided patches or set the firewalls."

Winkler even pointed a finger at the audience, saying that when they're dumbfounded by the supposed stupidity of a user in their organization, it's the security staff's fault.

"It's funny because it defines common sense," he said of common mistakes and errors committed by users (for example, one employee at the NSA whose last name was Kirk used the password "Captain", which Winkler said he guessed on the first try).

"But if it defines common sense, why does it happen? Because they don't have the common knowledge to apply common sense. If you don't provide your uses common knowledge, they can't exercise common sense."

He also said there's not enough emphasis placed on educating users on the possible risks posed by technology. He believes that if uses were more educated, they'd be less afraid of technology an less likely to commit simple mistakes.

"In a car, you can kill yourself in thirty seconds if you put some thought into it. But nobody's afraid to get into a car. Old people who are afraid to use a computer aren't afraid to get into a car and go out and mow down 100 people."

Joking aside, Winkler said that with automobiles, security is engineered, and apparent throughout, and the users are aware of that engineering, and what they can do to increase their own security.

" They don't say 'gee, there's a lot of ways to get into trouble," he said.

"How many people would just go drive into a random garage?"

In the end, Winkler said companies are probably approaching security the wrong way anyway, by chasing after a perfectly locked-down environment.

"Frankly, I've come to the concept that security is impossible, because security is freedom from risk," he said.

But that freedom is impossible, Winkler believes, because any environment that has vulnerability and value automatically has risk. The secret is in applying adequate countermeasures that balance out the potential loss from those risks. It doesn't make sense to piut in $15 million of countermeasures to protect $10 million in assets, he said.

"You're not trying to minimize risk, you're trying to optimize it," he said.

"You want to go ahead and determine the amount of acceptable level of risk you're willing to live with, then determine the budget for the countermeasures."