itbusiness.ca
Business Advantage through Technology

Print

How security pros can do their job well and still be liked

To avoid turning a security expert into a "no" man, organizations should try making security part of the bigger picture.
10/9/2008 4:00:00 AM
by Brian Jackson

As part of Microsoft's X-box Live team, Stephen "Stepto" Toulouse was proud of the first application he helped develop – a system for accepting user complaints.

But he was dismayed to come in to work one morning and find that system was completely frozen.

Toulouse is lead programming manager for policy enforcement on the team, and found the user interface for his admins wasn't responding. There was no apparent explanation for the problem until Toulouse used his security background to think about the problem differently.

"I started to think: *what could [have been] put into those fields from the user side*," he says. "It turned out someone had used characters to create a script that we were trying to render on our end."

The script was created as a joke, but the results were similar to that of a denial of service attack. It was the first time he discovered his experience as a security expert could apply elsewhere.

Security professionals have skills that they can bring to bear on other problems, Toulouse says.

He was speaking at SecTor, a security education conference held in Toronto Wednesday. A key theme at this year's annual conference was to drive home that security can't operate in its own silo, explains SecTor co-founder Brian Bourne.

"When your only job function is security and that's what you're measured on as an employee, the easiest way to do something is to not do it," Bourne says.

He says security should be about enabling things in a safe way, not about disabling things just because of the potential of attacks. To avoid turning a security expert into a "no" man, organizations should try making security part of the bigger picture.

Microsoft Corp. spread out its core of security experts to several different product groups to accomplish this, Toulouse says. The Redmond-based company's *Trusted Computing Group* was his own work area before becoming a member of the Xbox Live team. Bringing a security mindset to other parts of the organization can be beneficial.

"The entire eco-system becomes better because that security knowledge moves all the way out," he says. "It's not siloed amongst the experts."

A security pro can help to identify when an application might have unintended consequences, Toulouse adds.

For example, his X-box live team introduced a "friend-of-a-friend" feature that allowed video gamers to see the friends list of the people they had on their own lists. It was intended as a way to help gamers connect, but turned out to have some tough privacy problems.

Parents might want to block their children from taking part in such features. Or celebrities might not want their gamer tags widely circulated.

Toulouse worked with the team to come up with a communications plan that informed X-box Live players of the coming change. They gave people the ability to opt-out long before the mandatory download ever hit the system.

"Customers turned it off weeks in advance, before they even downloaded it," he says. "There were so many ways to opt out of the plan."

Still, much effort and expense could have been saved if the team had implemented the feature with security at top

of mind in the first place, he adds.

Security professionals with a technological bent are a segment of the market that should be considered more often by companies, says Johnny Long, an author that writes about hacking. Organizations should be looking at these sort of skill sets when hiring for various positions.

"Hackers have a unique perspective on problem solving and when you are recruiting employees, that's what you're looking for," he says.

One area that could definitely use some help from a security mindset is an organization's help desk. Long practices ethical hacking and has first-hand seen how easy it is to gain access to sensitive systems by asking a couple simple questions to the employee who's in charge of answering the phones.

Long was attempting to break into an organization's firewall by dialling in to a server remotely. But when he was stopped short because the server being accessed wasn't online, he had to go about the break-in with some social engineering. Some research revealed the name of a systems administrator.

"We called the help desk and used that name and asked them to turn on the server," Long recalls. "They did it with no questions asked."

All the more reason that organizations should be looking to get their security pros into the mix, Toulouse says. Try letting them have a job swap experience by putting them in a different department on an intern-basis. It doesn't have to be long, just a couple of weeks can make a difference.

"It can make the conversations of security versus accessibility a little bit easier to have when both parties have experienced the challenges," he says.

Security pros might even like working in different parts of the organization. "Stepto" did – he likes to brag to his friends that he plays video games for a living.