itWorldCanada.com

Print

Xbox Live exec leans on his security background

A Microsoft executive tells the SecTor 2008 crowd how to get every business unit thinking about protecting data without shelling out big bucks on new training and services

By: Rafael Ruffolo

ComputerWorld Canada (08 Oct 2008)

TORONTO -- Encouraging security professionals to branch out and spread their knowledge to other business groups will increase an enterprise's overall security without increasing the budget, according to a former program manager with Microsoft's Security Response Center.

In a keynote address at Wednesday's Security Conference Toronto (SecTor), Stephen Toulouse – who now works as a lead program manager for policy and enforcement at Xbox Live – credited his background in security as the primary factor to his success as a well-rounded IT professional. At Xbox Live, Toulouse and his team help ensure that customer data is protected and that the online gaming service's privacy policy is properly enforced. Although security no longer has a direct impact on his day-to-day work anymore, he said that many of his security skills have been completely transferable to his new role.

One of the greatest skills a security researcher can bring to the table, he said, is their ability to understand the potential misuses in functionality in a new tool. "The first thing a security persona asks is 'what's the worse thing a person could do with this new functionality to hurt the customer," he added.

Along with that, Toulouse said, security pros are also conditioned to think about the unintended consequences of this user functionality. When preparing to rollout a new Xbox Live feature called "friends of friends – which enabled users to view their friend's contact lists – the development team almost failed to create an opt-out feature for users who didn't want the added functionality.

"We started to realize that some parents would want to have their children's friend's list restricted from this feature," he said. "And what if you're friend's with a celebrity who doesn't want their profile to be exposed?"

The bottom line for Toulouse is that security pros often put a greater focus on the customers and always thinking about the best way to implement features or business practices that keep the end-users in mind.

"Sometimes it will lead you to actions that other people in your business see as counter intuitive," he added. When working on the security designs for Windows Vista, Toulouse recalled, many features were killed off after rigorous penetration testing and security reviews.

"It takes a strong customer focus to look at all your hard work, time and money and simply scrap something," he said.

But while this might work in theory, getting others to listen and trust you might be another story. Christopher Hoff, chief security architect with Unisys Corp., advised security people to be farmers, rather than lumberjacks.

"Act as an advisor rather than a dictator," he said. Offering up suggestions and insights to your colleagues and letting them decide is often the best way to get people to trust you, Hoff added.

Toulouse agreed, saying that working with other business units is often a two way street.

"When we get into security we have a very heavy hammer to bend people to our will simply because the stakes are so high," he said. "One of the things I stress is the need to be flexible."

"When you become a perfectionist with security you're really throwing the baby out with the bathwater," he added.

The need for security pros to tune in to business is not unlike the situation IT experienced about a decade ago, when organizations started thinking about technology as a strategic asset, according to Chad Mead, head of infrastructure security for global technology infrastructure at New York-based JPMorgan Chase. Then, IT directors learned that presenting technology plans to the board or operational units without emphasizing business benefits was an exercise in futility.

"Businesses have to understand and be willing to listen to security people, but it's up to security managers to coax the business folks along," Mead said. "It's up to security professionals to change perception of security as impediment, and help business managers think of incorporating security upfront."

Security professionals who have operations backgrounds might find changing their mind-sets and becoming a partner to business easier than most. But an operations background is not essential. More important is that

security managers get out of their offices and ask questions.

-- with files from IDG News Service