Print

**Canadian companies must 'urgently address' security skills gap**
By: Nestor E. Arellano
ITWorldCanada.com (24 May 2007)

COMMENT ON THIS ARTICLE

Canadian businesses need to act quickly to correct a "skills gap" in the areas of systems control and application protection, say security experts.

This has become imperative, with nearly half of all companies here experiencing security breaches over the past five years, they say.

The dire need for IT teams to be trained in these areas was expressed yesterday, after the rather disquieting results of an Ipsos Reid survey were announced.

According to the survey, 47 per cent of Canadian companies were victims of virus attacks and other security breaches in the last five years.

Little surprise then that – according to the survey – most corporate decision makers here see a need intensifying the "security" training of IT staff.

The survey was commissioned by Microsoft partner and IT systems builder, CMS Consulting Inc. in Toronto.

More than half (67 per cent) of the executives polled said they believed their staff would benefit from more security training.

"Organizations feel good about their [IT] structures but perceive a significant skills gap when it comes to dealing with the threats out there," said Brian Bourne, president, CMS Consulting.

The said ongoing training of IT staff was essential to bridge this gap.

In that context, Bourne announced the Security Education Conference Toronto (SecTor), would be held in the city later this year (November 20 and 21).

The conference, he said, will be a forum for identifying and discussing digital threats facing corporations.

The good news is many companies are keenly aware of mounting security risks and the need to urgently address these.

Seventy-six per cent of the firms polled in the Ipsos Reid study said securing their IT networks is one of their top priorities.

Bourne said 90 per cent of companies that conducted "self-penetration tests" reported their systems were "effectively compromised" by the testers.

This indicates a growing need to beef-up protection for control systems, according to another vendor who spoke at the event.

"Organizations haven't been able to scale up to the challenges," according to Chris Blask, founder and CEO of Lofty Perch Inc., a Toronto-based provider of cyber security products.

Blask said improving integration of company assets under a single IT infrastructure and control system has boosted efficiency but also elevated inherent risks.

For instance, he said most air traffic control facilities have perimeter security, operational systems, and IT components tied to networks, and switches monitored by a single control system.

Most networks are also accessible via Internet to enable remote access.

"While firewalls are deployed to protect these systems, connections to the PSTN (public switched telephone network) and wireless services are often inadequately defended against breaches," Blask said.

Another industry insider said a growing number of hacker attacks are now aimed at applications.

However, most IT employees are not trained in dealing with application security, according to Brian O'Higgins, chief technology officer of Third Brigade Inc. in Ottawa.

He said application software tools are "the Achilles heel of most organizations." O'Higgins said 75 per cent of attacks are targeted at applications, as hackers consider them the "low hanging fruit."

"It's easier to load malware onto applications because they are now [accessible] over the Internet, and are allowed to bypass firewalls."

Even basic training on how to protect applications would result in immediate benefits, the Third Brigade CTO added.

"Companies mustn't concentrate on the threats as they will always be there. Rather, they must focus on reducing vulnerability."

QuickLink 070623

COMMENT ON THIS ARTICLE