Attackers profiting from IT blinders

BRIAN BOURNE AND DAVID SENF
GLOBE AND MAIL UPDATE
NOVEMBER 16, 2007 AT 12:40 PM EST

Front Lines is a guest viewpoint section offering perspectives on current issues and events from people working on the front lines of Canada's technology industry

The confidence of Canadian firms in their IT security is irrationally high – and it's up from a year ago. In contrast, attackers looking to exploit weaknesses have found new and creative methods to earn more money. Lack of awareness and most alarmingly the lack of leadership in Canadian firms helps the now organized criminal attackers enjoy greater success and profits.

The threat environment is now driven largely by underground economy, where there is no shortage of creative ways to make money. Phishing, spamming, theft of intellectual property, corporate espionage, personal identities and credit cards are only a few of the revenue opportunities. The troubling reality of attackers motivated by money instead of notoriety and fame is that they are highly motivated to do everything possible to go unnoticed. It is not at all uncommon for an investigation to uncover that hackers had system access for many months or even years, and in some cases, the hackers were even helping the company maintain over all IT health to ensure that the systems they were abusing stayed online and their activities continued unnoticed.

This all said, there is the overwhelming belief by Canadian companies that nothing bad will happen to them. Optimism even prevails when something bad does happen – surely lightening won't strike twice. Perhaps it's our good Canadian nature. Or it might be that ignorance is bliss. Whichever it is, there is a lack of knowledge regarding security risk – particularly among business executives.

Brian Bourne is co-founder of SecTor, IT Security Education Conference being held this year Nov. 20-21, 2007 at the Metro Toronto Convention Centre in Toronto. David Senf is Director of Security and Software Research IDC (Canada).

Although the buck stops with business executives they do not place a high priority on IT security. Granted, their job is to focus on delivering business results. But research from IT market research consultancy IDC shows that security consistently rates low even when comparing with other IT priorities. They'd rather invest in additional business applications and better performance than improved security. Not coincidentally, Canadian firms are saying that they need more leadership from management on security. Doing risk assessments, setting priorities, training employees and enforcing policy relies on management leadership. But first, Canadian business executives need a better grasp of security to take on this role.

Security vendors compound the problem in their enthusiasm to sell more product. They'll promise full security in a box or in a piece of software. The truth is, there is no holy grail of security, and no product or service can guarantee security or cover all areas and levels. As an organization, you must first figure out what you are trying to protect and its value, then figure out if you have adequate protection measures. Rinse, then repeat, as security is a constantly changing field, and so are your assets. What is important to the business this year, may not be critical next year.

No one works with an infinite security budget, and determining where to spend each security dollar will depend on your specific environment and no one else's. Avoid purchasing a system because it's popular or it seems many businesses also have it; understand exactly what it will do for you. Replacing your $2000 firewall with a $50,000 firewall doesn't necessarily improve security in any way. In security consulting, far too often we see an expensive security purchase made, which is not properly implemented, monitored, or maintained. It happens that solutions are purchased to protect something of much lower value than the solution itself.

The maturity and complexity of attacks is not something the average firm can change. The fact is that the bad guys are getting better at an alarming rate. However, firms can spend a little more time understanding the threats and what assets need protection most. The security community realizes this, and endeavours such as the Toronto Security User Group (www.task.to) and the recently launched Canadian IT Security Week (www.itsecurityweek.ca) have grown as part of the Canadian security community coming together. But ultimately business executives need to lead by supporting IT executives and IT management in their security efforts. After all there are many attackers happy to make a dollar off your insecurity – and remind you that you can't spell confidence without con.

Brian Bourne is co-founder of SecTor, IT Security Education Conference being held this year Nov. 20-21, 2007 at the Metro Toronto Convention Centre in Toronto. David Senf is Director of Security and Software Research IDC (Canada)

Recommend this article? 6 votes

View the most recommended

globeandmail.com and The Globe and Mail are divisions of CTVglobemedia Publishing Inc., 444 Front St. W., Toronto, ON Canada M5V 2S9
Phillip Crawley, Publisher