iTWeb SECURITY

Cyber counter-intelligence makes a difference

By Tracy Burrows, ITWeb contributor.
Johannesburg, 29 Apr 2014

With enterprises and governments losing the cyber security battle, cyber counter-intelligence has the potential to sway the balance of power, says Professor Basie von Solms, director of the Centre for Cyber Security at the University of Johannesburg.

He qualifies right from the outset that the case for cyber counter-intelligence should not be misconstrued as a call for a free-for-all cyber "wild west". On the contrary, correctly understood, it is a call for legitimate cooperative action by state and private sector role players in breaking the traditional security mould which is proving so ineffective against sophisticated adversaries, he says.

Taking a traditional "fortress" approach to cyber security is an exercise in futility, says Von Solms, "Building on perimeter defences when the enemy is likely already in your systems is pointless," he says. "It is clear that traditional approaches to cyber security are failing. Now we need to draw on successful strategies from history to devise new models for cyber security."

Von Solms says there is a growing interest in applying long-established counter-intelligence models for use in the cyber era. In fact, the "Know Yourself - Know your enemy" approach attributed to the ancient Art of War treatise by China's Sun Tzu is still highly relevant today, he says. So are aspects of Cold War theory and practice.

"The traditional approach to cyber security has been mainly a defensive one. Now, we need to be more proactive - and possibly even slightly aggressive - in our approach. We need to go to the next level and gather counter-intelligence that allows us to know our enemy and plan our defences accordingly. For example, we might put out a ‘cyber honeypot' to attract cyber criminals and gather information about who attacks it and how. It may be also be used to pro-actively mislead and disrupt the criminal. Of course, there is a fine line between being proactive and overstepping the mark and becoming a cyber criminal yourself," he says.

He says the counter-intelligence approach to cyber security is raising concern in many quarters, with detractors citing ethical and legal concerns. On the other hand, many enterprises feel it is becoming necessary to have "cyber guns ready and firing", he says. Embarking on cyber "war games" is just one approach to defend enterprise systems in an increasingly fraught environment, he notes. However, he believes it presents great potential if approached in a balanced manner.

Von Solms says cyber counter-intelligence is not a novel concept, but outside of the statutory arena, it is not widely practiced. While cyber counter-intelligence is not a "wonder cure for all ills", it could offer a conceptual and practical approach for more role-players to assert their interests in the cyber arena - if based on sound models and a cooperative, legal posture. In addition to models, adopting a counter-intelligence approach to cyber security would require new skills within the IT and other departments.

"You would need to train existing staff or find people with the right strategic, proactive approach and tactical skills. You need multi-disciplinary experts, who understand how to gather the necessary information and use it to your benefit. The more you can gather, the better you can defend yourself."

Von Solms will present a talk at the upcoming ITWeb Security Summit 2014 on the case for counter-intelligence as well as its challenges and benefits. Co-presenting with Von Solms, Dr Petrus Duvenage will be gauging with the audience the practical feasibility of an academic model currently being developed at the University of Johannesburg's Centre for Cyber Security.

Source: ITWeb:
http://www.itweb.co.za/index.php?option=com_content&view=article&id=134136