http://www.cso.com.au/article/541698/why_aren_t_we_winning_security_battle_/

Why aren’t we winning the security battle?

31 March, 2014 22:12

Given the billions of dollars that have been invested in security over the last decade or so, you'd expect that malware distributors and data thieves to be scurrying away with their tails between their legs. But that's simply not the case.

According to Dennis Moreau, the Senior Engineering Architect for Software Defined Security at VMWare, "We've seen very rapid advances in security-centric technologies. Whether that's web application firewalls, next generation firewalls, IPS systems, sandbox detection of advanced threat stuff. All of this stuff has shown significant advance and is deployed in data centres. Yet what we're doing isn't working … whether it's the Darkleach exploits of hosted Apache servers or the gumbler exploits of hosted WordPress sorts of instances".

In Moreau's view, the complexity we've added to our architectures has created an environment that, by design, is harder to manage and secure.

> "When we bring the cloud into the data centre discussion, we are bringing in multiple provisioners into the stack. You no longer are provisioning everything you would have in an on-premise enterprise data centre. So there's a coordination of multiple actors. There is also the dynamics associated with it".

The challenge is that you no longer see all the additional movement, load balances, mechanics with scale-up, scale-down, all of the stuff that goes on behind the scenes. This is why there has been a reduction in visibility and an increase in movement. Managers have to coordinate a number of technologies, all of which have different ways of expressing policy.

Steve Pate, the Chief Architect at HyTrust, says that we have consolidated risk over the last several years. "We've gone from tens of thousands of physical servers managed by many administrators in different buildings, in rooms with locks on the doors to single box storage and compute with thousands of virtual machines, managed by a single or a few separate administrators".

That's created operational environments where we have administrators with uncontrolled amounts of power. "We've got to have a lot more control over administrators, we've got to understand what they're doing, said Pate. "Things like a two-man rule and multi-factor authentication, which needs to come into play. Shionogi was a great example, a disgruntled employee was thrown out of the company, sat inside a coffee shop, got back into the network and deleted all of their production virtual machines".

Shionogi is a Japanese pharmaceutical company. In 2011, Jason Cornish was working as a consultant for the US subsidiary Shionogi. His contract was terminated in a round of cost cutting so he exacted revenge by using his network credentials to log into the firm's computer systems from a public Wi-Fi hotpot. He deleted 15 virtual hosts, taking down 88 virtual servers.

> Pate said that " We've got the same in the cloud and we've got a whole set of issues around virtualisation, especially with data security, that people really don't understand".

Dr. Hongwen Zhang, Co-Founder and Chief Executive Officer of Wedge Networks, says that service providers are ideally placed to deliver security.

> "When we, in old days, tried to drink the water from the tap system, tap water, you had to boil it, otherwise you'd get infected. Nowadays, if you open up the tap you can drink the water. Who is there to provide a clean Internet that is not contaminated with security risk? It's the service providers – the guys who provide pipes for the end users. And hence they are in a very good position to deliver service knowing fully well that the security breach is mainly coming from networking".

Another element that remains poplar in security is the use of encryption. But, in Australia, there are moves afoot to compel users to handover encryption keys to authorities during an investigation.

Moreau said "This has pushed us to precisely what we see in the market dynamics, that there is a strong movement toward the encryption keys being handled by the folks who are responsible for and interested in protecting the data and are not available to the service providers and the plumbing".

Zhang added that there is a need to establish trusted relationships so that businesses, whether they are enterprises or SMBs, can access services that have been tested and certified as secure.

> "So I think the emergence of this app store idea, you can go to Amazon and you can buy a whole variety of third party images that you can load in your virtual private cloud. We're also seeing the same thing, the idea of OpenFlow and SDN controller, the really interesting thing is you have this ecosystem of application developers that can develop on top of the SDN controller. So there's also going to be an emerging app store ecosystems".

Pate added "Prior to putting an application in the marketplace, Amazon will scan it for malware and viruses and vulnerabilities. Not perfect but it's much better than where we were before".

Anthony Caruana attended the Cloud Innovation Forum in Saratoga, California as a guest of NetEvents.

This article is brought to you by Enex TestLab, content directors for CSO Australia.