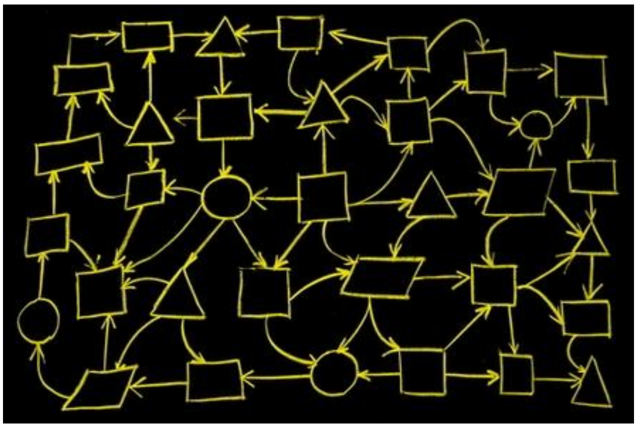
CSO
THE RESOURCE FOR SECURITY EXECUTIVES

http://www.cso.com.au/article/541697/security_driving_sdn_uptake/

Security Driving SDN Uptake

31 March, 2014 21:56



Software Defined Networks are here. In just a couple of years they have moved from theory and are now part of every CIO's planning. And that means a significant rethink is needed when looking at security. With many critical functions moving off proprietary hardware towards open platforms where core functions are abstracted to software, the way networks are managed and secured is changing.

Martin Casado is the CTO of Networking at VMware and the inventor of OpenFlow. He was the keynote speaker at the recent NetEvents Cloud innovation Forum held in Saratoga, California. He says that the move towards SDN was initially driven by the likes of Google and Facebook and Amazon.

> "These very, very technical companies with some of the most technical expertise on the face of the planet came up with their own architecture. And if you look at what that trend looks like, basically, what they did is they said, I'm going to move functionality that has traditionally been in the network, and I'm going to move it to software. So things like security, things like security, things like fault isolation, things like billing, things like visibility and debugging, instead of being traditionally put in hardware in the network, they were moved into software," he said.

Interestingly, Casado said that the security is actually a key driver in the uptake of SDN. He believes that about 40% of the actual adopters that are paying money for SDN network virtualisation are doing it as a security use case.

> "So before I went to Stanford, I actually did computer security," Casado explained. "I did kind of operations, where I would actually break into things. And let me tell you, a data centre has almost no controls in it at all. Like, 80% of our spend is on the perimeter, and that's a Maginot Line. So if I can pay somebody off or I can put on a black mask and I can break into the building and I can

> install some code on a server or I can remotely exploit a server, if I get in the data centre, I'm done. That's because that's where all the data is, and there's almost no controls within the data centre".

SDN allows data centre architects to segment operations so that interactions between systems inside the data centre can be better managed and secured.

> "So, for example, for every application I can create a virtual network. I can give it its own security services. I can give it its own L4 through 7 services, and if it gets compromised, the attack gets localised to just that," Casado explains.

Security, in Casado's view, is a balancing act between isolation and context.

> "The question we've been asking is, can you build a Goldilocks layer that goes ubiquitously throughout the data centre that provides both context and isolation?".

Given the penetration of virtualization – Casado speculated that about 70-80% of enterprise workloads are virtualized – then the hypervisor becomes a vehicle for providing that context, as information passes from one domain to another, and isolation so that unexpected data is not passed between domains or systems.

> "If you could use the hypervisor to both peer into the application to pull out meaningful context, like users and applications and what things are doing but also protect that visibility and provide protection and enforcement, you kind of have this optimal place, where you have both this visibility and context and the isolation," he said.

One of the challenges, in our view, that comes with moving key functions into software and away from hardware is that the time between development and deployment is greatly reduced. The can create an appetite for rapid changes. Although this has a significant benefit in that it can drive innovation it can also result in errors being put into production more rapidly.

Casado says that this can be overcome.

> "I think you should have a root of trust that's formally verified. I think it should be in software, because if there's a bug, I want to be able to fix it on the fly instead of shipping a new box, so I think software is actually inherently more secure for exactly that reason. So here's what I would like to do. When you get your hypervisor from me, there's a stack there that's 10,000 lines that I've formally verified that gives you a root of trust. It will use hardware TPM [Trusted Platform Module] and it will give you a root of trust. And then if you care about very secure things, you use that root of trust to build your very secure things, and if you don't use very secure things, you can do whatever the hell you want".

As well know, and as Casado agrees, there is no perfect security. Even in the 'Goldilocks layer' he alluded to, there can be problems. However, Casado used the metaphor of making your bed to highlight how security might be managed in future.

> "I don't believe in perfect security. I'm not a Pollyanna. I always think of it like this, so this morning, when I made my bed. So you get up and you make your bed and you're putting your blanket on. There's always that last bump, and you then you take that bump, and instead of getting rid of the bump, you kind of move it over to the wall, it looks nice by the wall, or you move it over the pillow. So I think this is a lot of security. I don't think you get rid of security vulnerabilities. You just move it to a place that you know how to protect. You kind of move that bump somewhere".