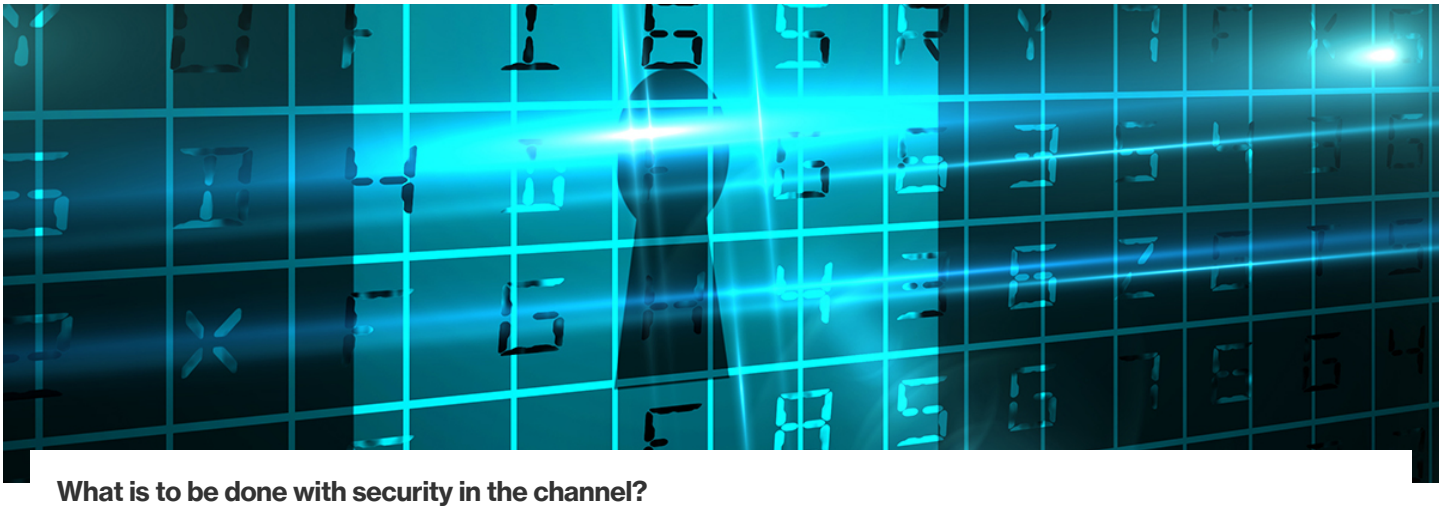
WAVEBREAKMEDIAMICRO - FOTOLIA



What is to be done with security in the channel?

1

Anthony Savvas

Cyber security experts met in Dublin in November to discuss how the channel can play its part in offering more secure and easier-to-deploy protection to organisations, and MicroScope's Antony Savvas was there

The Zonic PR security symposium in Dublin, held in conjunction with the annual IRISSCERT cybersecurity event, sought to address the key issues faced by companies as data security incidents proliferate.

Delegates at the symposium discussed cloud deployment for products and services, security skills shortages, new product solutions and how they are being taken to market, and how the channel can hold the hand of the customer through the dark arts of data protection.

Widening attacks

Although companies are generally spending more on data security to tackle threats, organisations are still failing to fully address the issues, and it doesn't help that the “attack surface” is widening. IT professionals network Spiceworks recently surveyed 600 of its members in the UK and the US, and found that 80 percent “felt confident” in their ability to respond to cyber attacks on traditional endpoints like laptops, desktops and servers.

However, they were less confident in their ability to respond to cyber attacks when it came to newer IT devices and services, such as tablets (58 percent), smartphones (52 percent), cloud services (44 percent) and Internet of Things (IoT) devices (36 percent). Different technology often means the need for different security technology.

Only a few years back, most organisations simply focused on getting up-to-date anti-virus software installed on desktops and laptops that connected to the corporate network. A firewall deployed at the gateway to the network was also thrown in for good measure to help filter threats, but now firms are expected to do so much more, and many are confused.

Do your homework

Jason Steer, solutions architect, EMEA at anti-malware vendor Menlo Security, told the Dublin delegates: “Many customers still believe buying one product can solve everything, but it can't.” He called on both resellers and end customers to do their homework.

He also added that UK firms were “security laggards” when it came to new technology to protect their systems, and that they were behind their counterparts in Germany and Scandinavia, for instance.

“In the UK, they look to see what others are doing elsewhere first before adopting new technologies,” said Steer.

Carl Gottlieb, technical director at channel security solutions provider Cognition, claimed: “Customers are being mis-sold security technology by the vendors. They should get away from the sales guy and do more testing on their systems themselves, to make sure they know what they are getting.”

As a VAR in the market, Gottlieb says Cognition is also practising what it is preaching. Cognition sells Cylance “next generation” anti-virus software which recently hit the EMEA market, and which uses artificial intelligence/machine learning in the cloud to help prevent threats reaching user endpoints in the first place.

Gottlieb said of the technology: “We heard of it but stayed away initially as we didn't believe the promises, and anti-virus software is dull in my mind. But we did take a look and were very impressed. We tested it ourselves on an independent testing site and listened to Cylance users too.

“All vendors say they're the best but customers are still getting infected, so which is it – are they the best or among the worst? The only way to address the matter is to do your own testing.”

But while technologies are clearly key, the holistic approach to data security is important too. Dave Lewis, an infosecurity consultant and global security advocate at data delivery optimisation vendor Akamai, said: “Organisations do need help to find what security they're looking for and we need less of the system administrator versus the users approach. The system admin should not be seen as the enemy by the users, stopping them from doing what they need to do, and the users must not be viewed as stupid by the system admin.

“Every person in the organisation should effectively be part of the cybersecurity team, all working together to prevent and mitigate threats.”

Spending more but still falling foul

Dennis Davis, founder of security software firm MyCrypt, which provides access control, identity management and data encryption, said: “Despite customers spending on security and making improvements, sometimes they are not going back to close existing holes in their systems.”

Which is something that was echoed by Anton Grashion of Cylance. He said: “People are under time pressures. They just need to get something done, so mistakes will happen. A SQL injection attack is one of the oldest tricks in the book. We know how they work but they still happen.” TalkTalk, of course, suffered a major loss of customer data last year as a result of a SQL injection attack.

Cognition's Gottlieb said security awareness training should be done regularly across organisations, despite the increasing automation and artificial intelligence being bundled with products and services – being done to make security easier to manage on-premise or in the cloud.

He said: “There will always be an element of social engineering in threats. Look at 'whaling' – all it takes is a phone call from the CFO to the CEO, for instance, to make sure a fund transfer request is legitimate, and that type of threat can be prevented. So regular security awareness

training is essential."

Whaling sees senior executives targeted with phishing emails or other communications by criminals, requesting they transfer funds from company accounts to a rogue one to complete fake business transactions, and their incidence is increasing.

Software-defined WANs for greater security

The type of network deployed is key to data security and the conference discussed the growing market for software-defined wide area networks (SD-WANs), to not only deliver easier connectivity in cloud environments, but also provide improved security.

Many organisations assume VPNs or virtual private networks are automatically more secure than standard network connections, but they aren't unless data encryption is added to them, and that isn't done automatically by many providers. The same is true for MPLS or multi-protocol label switching networks used by many enterprises for larger amounts of data traffic.

Like VPNs, MPLS networks deliver more reliable data connectivity with less latency, but the security comes with what encryption and other protection measures you add. With SD-WANs, the customer can usually expect bundled security, even though SD-WANs are generally cheaper overall.

According to analyst Arcluster, the European SD-WAN market will be worth 1.3 billion euros by 2021.

Mike Wood, vice president of marketing at VeloCloud, one of about 30 vendors now pushing an SD-WAN solution, says of the security benefits: "PKI (public key infrastructure and IPSec (IP security) tunnels are complex, are arduous to set up and exhausting to maintain."

He says: "An SD-WAN architecture envelopes this complexity to let you set up security with a click in a centralised orchestrator. VPN tunnels are built automatically to cloud-hosted gateways, and the tunnels and PKI are managed by cloud-based controllers and gateways."

Wood says companies are increasingly demanding an SD-WAN solution from their MPLS service providers, who include the likes of BT, Orange, Deutsche Telekom and AT&T.

Wood said: "MPLS is more expensive and there is resistance from MPLS providers, which is understandable as they don't want to cannibalise their revenues. Enterprises value the services they get from their carriers and often want to stay with them, but those providers can't continue to simply sell pipes and boxes.

"Carriers that say they aren't doing SD-WAN now are often giving discounts on their MPLS offerings when approached by customers."

In addition, said Wood, organisations are also approaching VARs and MSPs to do the leg-work and find them an SD-WAN solution to quote on.

While security has always been one of the top technology priorities in IT spending, the Dublin event showed that the channel still had lots of work to do to stay ahead of the curve and keep taking advantage of the opportunities out there.

This was last published in November 2016

Read more on Threat Management Solutions and Services

ALL NEWS IN DEPTH OPINION

Selling security: Focus on services

Selling security: best of breed versus integrated suites

Ransomware the sweet spot for Trend Micro

Security is the way to monetise IoT

Load More

Join the conversation

1 comment

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] **ParkerErickson**

- 30 Nov 2016 12:30 PM

Great insight, Antony! Your article raises some very interesting points regarding how organizations can mitigate cyber security threats within the channel. Intermediaries as well as end-users should be wary of any IoT solution that claims to be totally secure. From the component supplier to the OEM, to the end-user and then the hosting provider, security is an ongoing battle where success is a product of participation and partnership between multiple allies. In my opinion, the most effective way to build and maintain IoT device security begins at the component level because security is not a “one and done” thing. Just as security in the IT world requires constant vigilance, there is a dawning realization that equal if not greater precautions are needed when it comes to IoT security.

Reply

This survey of business leaders by the Economist Intelligence Unit for Pegasystems finds that businesses are mostly confident ...