Can your security keep up with the pace of innovation?
As the pace of innovation is vastly outpacing security improvement, unless organisations start planning for the increased risk they have to face, they are putting themselves in the firing line.

This paper provides an overview of the view of Jon Tullett, Research Manager for IT Services at International Data Corporation (IDC) and Patrick Rhude, Head of Product Management in Nokia’s Security product unit.

Jonathan Tullett is research manager, IT services for IDC sub-Saharan Africa. His specialist areas include IT services, outsourcing, and cloud computing, as well as information security and digital.

Patrick Rhude, Head of Product Management in Nokia’s Security product unit, is responsible for the next generation of security management products, guiding all aspects of product evolution, including new product introductions and growth.
Organisations need to account, plan and scale for growth

“Today, most companies find themselves in the 3rd platform of the traditional IDC model, which means they are steadily adopting technologies such as cloud, mobility, big data analytics and social business,” Jonathan Tullett, research manager, IT services for IDC sub-Saharan Africa says. “It’s that proliferation of devices, endpoints, apps and a ton of users, all of which is growing exponentially. Now, as we move beyond the 3rd platform, we’re starting to look at an innovation ecosystem.”

The focus is, therefore, shifting to what organisations are doing with 3rd platform technologies. “We are starting to see apps being created on the fly, for specific purposes, and then broken down again. We are seeing more customer interaction. Even if you aren’t seeing more customers, but the actual interactions they are having with organisations, their data and their systems, is going through the roof. Organisations need to account, plan and scale for that, and they need to secure it.”

Most people have seen the graph that depicts the length of time to reach 50 million users and how that has decreased on an exponential curve. It took 75 years for the telephone to reach that number of users, while Angry Birds took just over a month. “One of the things you have to bear in mind is that none of this happened in isolation. Angry Birds didn’t reach 50 million users in 35 days by building the internet from scratch. They leveraged the internet and social media platforms that had come before it. They also leveraged the change in user behaviour. So, it’s not that Angry Birds was that much better of a technology, it’s just that we’ve built a marketplace where huge technology adoption can happen overnight.”

Tullett believes that while that technology adoption might not happen overnight, organisations must understand that it may well happen. “If you build new technology and put it into the field, you can reach millions of people incredibly fast and you probably haven’t planned for that. You probably haven’t planned for the load that it will put on your systems or the exposure it could bring you in making you a target.”
“The number and different types of security alerts we are seeing, are growing exponentially,” says Patrick Rhude, Head of Product Management in Nokia’s Security product unit. These have been brought on by many technology innovations, with each innovation increasing the exposure dramatically. With organisations somewhere between moving from cloud to IoT, there is a lot of focus on the disappearing perimeter. “Traditionally, security was about building a fence and trusting that fence to make you feel secure, but you never actually check to see if someone has cut a hole in that fence and is moving around within your perimeter. So, it is becoming key to move beyond your perimeter defences, whilst keeping them intact, and start doing analytics on breaches that have happened,” he says.

Rhude says most of their customers already assume that they are going to be breached, but what will separate them is how quickly they can respond to those breaches. In the event of a breach, they want to be able to say that they responded and were back up in a matter of hours as opposed to a matter of weeks.
Only 30% of incidents get investigated

70% of them are false positives

54% of incidents that should get investigated, don’t

“The reality today is that the number of security incidents has become so high, that only 30% of incidents get investigated. Of that, 70% of them are false positives. As a result, 54% of incidents that should get investigated, don’t and the people working on that spend 54% of their time trying to do detections. We also know that there is a lack of skilled security experts out there. So, how do you make these limited resources more effective? Also, how do you automate responses as quickly as possible so you can close those breaches or discover them earlier?” he asks.

The global convergence of IT and telecommunications is adding a layer of complexity and seeing the issues traditionally only seen in IT networks move across to the telecoms environment. Bringing IoT into the fold, adds further complexity and a lot more attacks, as the attack surface is increased.

Tullett agrees. “I’m not saying don’t deploy IoT devices, but understand that the threat model is far more advanced. The attackers are a couple of generations ahead of you. They have built the automated tools, exploits and they know how to monetise it,” he says. “So, deploy these securely. Put them on a segregated and encrypted network, make sure that you monitor their telemetry with a fine-toothed comb looking for signs of misbehaviour. Make sure you buy devices that can be updated and that you do so regularly, along with updating default passwords. There’s a tremendous amount of interest in IoT in this country and, although we are slightly behind the curve in terms of adoption, there are solutions being introduced to the market. The biggest question being asked, however, is how do I secure it?”
“Organisations must prioritise monitoring and tracking that their IoT devices are performing their intended function, whether they are doing anything else and whether they have any other impact on the network that is not readily seen, based on traffic patterns. At Nokia, we combine things like monitoring the traffic in the network, correlating that against a baseline of what that device is supposed to do and then looking at any anomalous traffic that is outside of the norm as this generally signals that an IoT device has been compromised. By monitoring this closely, you are then able to act to either block the device or reconfigure it, bringing it back to its previous state,” says Rhude.
About Nokia
We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry’s most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience.

www.nokia.com

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2017 Nokia