Top 5 IT security trends to watch in 2015

What does 2015 hold in store from an IT security perspective? Read on as Dimension Data experts discuss the top trends to watch and their expected impact on business.

Introduction

The security industry is entering a period of change. The market is consolidating, a transformation that’s being driven not only by leading vendors such as Blue Coat, Palo Alto Networks, and FireEye, but also by venture capitalists, and global carriers.

‘The security industry, by its nature, has always been entrepreneurial, and abundant with start-up companies,’ says Matthew Gyde, Dimension Data’s Group Executive – Security. ‘While this spirit of entrepreneurship will remain, I think we’ll see even greater levels of consolidation in the year ahead.’

So what else does 2015 hold in store for IT security professionals? “We’ve identified what we believe to be five of the most significant trends in our industry, using the insights gathered by our 700-strong team of security experts during their daily interactions with clients,” says Gyde. ‘Of course, these are by no means the only areas where change is happening, but they certainly warrant discussion.’
1. Incident prevention evolves towards incident response

Technologies and services focused on incident response – rather than just incident prevention – will be high on the agenda for security professionals in 2015. That’s according to Neil Campbell, Dimension Data’s Group General Manager for Security. ‘Recent data breaches such as the ‘Target hack’ and allegations of state-sponsored hacking have taught us that that we need to move beyond focusing purely on the prevention of security incidents or, in IT security terms, trying to stop “bad actors” from dwelling on the network,’ he explains. ‘You need to accept that it’s inevitable that they’ll find their way into your environment at some point. That’s not to say you should become complacent; rather, you need to turn your attention to identifying what we call ‘indicators of compromise’ and ensuring you have a comprehensive incident response plan in place. All too often, IT teams don’t know how to respond to a security breach; they panic and react instinctively, which increases the severity and the length of the incident ... and ultimately its impact.’

Campbell draws a comparison between effective incident response and fire drills. ‘Today, every company has a plan to deal with an outbreak of a fire in the building. Regular fire drills are a critical element of the plan and ensure that, in the event of an incident, everyone’s clear about what they need to do and are therefore less at risk. Likewise, you need to be sure your IT teams understand – and rehearse – the appropriate course of action in the event of a security breach. This will include:

- recovering evidence
- identifying and resolving the root cause of the incident, not just the symptoms
- possibly undertaking a forensic investigation

‘Recent data breaches such as the ‘Target hack’ and allegations of state-sponsored hacking have taught us that that we need to move beyond focusing purely on the prevention of security incidents or, in IT security terms, trying to stop “bad actors” from dwelling on the network.’

2. Managed security services move front and centre

For most businesses, identifying IT security incidents in a timely manner requires 24/7 coverage of the network environment. This can be costly. IT security professionals are scarce, and require regular training to keep abreast of continually evolving technologies.

Campbell points out another drawback to the insourcing model: ‘To become truly proactive about incident response, you need visibility of other networks, so you’re aware of attacks that are occurring elsewhere. That’s why it makes sense to engage the services of a managed security services provider, as they have this depth and breadth of insight.’

Gyde agrees: ‘In recent years, security management and monitoring have become more complex and time-consuming. Today, you need to prevent what you can, and manage the inevitable compromises. This means optimising your detection, and response capabilities. Many businesses lack the skills required to detect and effectively respond to threats in this manner.

Managed security services providers such as Dimension Data have teams of security professionals focused exclusively on identifying potential malware and monitoring thousands of clients’ networks for precursors to denial-of-service attacks. Such incidents don’t happen out of the blue, usually there’s a lot of “chatter” on the popular “dark Web” channels beforehand. We monitor these channels closely and can therefore increase the likelihood that our clients are forewarned of impending attacks.’

3. IT security gets cloudy

Campbell and Gyde predict a continued increase in the adoption of cloud services for security in 2015. Says Gyde: ‘This holds true for software-as-a-service solutions, such as secure Web proxy, and secure email in the cloud. These solutions are particularly attractive as the implementation effort is negligible – you’re simply redirecting traffic to take advantage of the service through a consumption-based model. And the services are highly scalable. If you need to support 20,000 users today, but in six months’ time, you acquire a company and your headcount suddenly increases to 30,000, you simply amend your licence agreement, and your new employees will be up and running immediately.’

Application security in the cloud and cloud-based, distributed denial-of-service controls such as those offered by Akamai are other areas of growing interest.

Campbell also believes that security of the cloud will become increasingly important as more organisations move their workloads to the cloud. ‘It’s no good adopting this model only to be told by your auditors a year later that your cloud provider’s security protocols aren’t up to scratch. I think we’ll see cloud providers investing heavily in building rich network architectures that support the gamut of security controls, so that they’re able to assure their clients that enterprise-grade security technologies are being applied to their workloads.’

Gyde agrees that there’s still some work to be done within the cloud industry on the security front. ‘Just because your provider says “Yes, I can offer you a hosted firewall”, doesn’t mean that its services are secure. The most secure platforms in the world can still be compromised by human error or poor management. Another area that needs attention is integration with existing organisational policies and processes. It’s very easy for start-up companies to transition to the cloud as they have no legacy physical infrastructure, and can implement “greenfield” security controls. Larger, more established businesses find the prospect of cloud more daunting, as they’re unsure of how to adapt their security controls, policies, and processes to this model.’
4. From security technologies to secure platforms

According to Gyde, 2015 will see the notion of security being a secure platform – rather than a series of point products or devices on the network – gaining traction. The expectation on security professionals will be to deliver a secure platform that allows the business to confidently run multiple applications, in a secure environment.

For many years, organisations typically bought multiple security products from different vendors. While this helped create ‘defence in depth’, it also introduced complexity and potential risk. After all, 95% of successful attacks may be attributed to human error, rather than technology. Increasingly, organisations are weighing up their risks and making buying decisions that aren’t necessarily based on best-of-breed technology and are instead adopting a pragmatic, risk-based approach where they work with their existing infrastructure and partners to manage their risks to an acceptable level, rather than aiming for, but never achieving, ‘perfect’ security.

The concept of cloud and its pay-per-use model is also relevant to this discussion. Organisations want to replicate the consumption-based approach of cloud in an on-premise model, either independently owned, or owned by a trusted service provider or vendor. Increasingly, organisations’ preference is for security partners that are prepared to take on some of the financial risk, while also offering a flexible service construct, for example, one that allows them to turn on a firewall at short notice to deal with a specific event, and the spin it down when the requirement has passed.

The notion of a secure platform directly relates to organisations’ desire for a ‘single pane of glass’ through which to manage their security assets, delivered on-premise, hosted, or as cloud infrastructure. Essentially, this enables robust security to ‘follow’ an organisation’s applications, data, and workloads without any compromises or changes in technology or management being required. This approach also supports and aligns with enterprise mobility requirements for corporate data to be accessible to users anytime, anywhere, and from anywhere.

5. Endpoint security – back in vogue

Campbell predicts a resurgence in interest in endpoint security in the industry. ‘This is closely tied to the first trend we discussed – incident response – and the fact that some traditional network-based security controls aren’t as effective as they used to be,’ he says. ‘Security professionals will be looking at devices – whether they’re PCs, Macs, or smartphones – for indicators of compromise, and then enabling some form of incident response process. They’ll deploy technologies to endpoints to make incident response easier.’

Application control is also expected to re-emerge as a key focus area for 2015. However, the emphasis will be on identifying malicious activity on the endpoint, rather than malicious code. Campbell explains: ‘As well as you may try to build user awareness of information security best practices, at some point someone’s going to click on something they shouldn’t ... so you need a way to be proactive about managing the impact of such events.’

Conclusion

‘A trend that’s not made our top five list, but is closely linked to each is the use of data and machine learning, which, when coupled with human interaction can create actionable and contextualised intelligence. This enables organisations to make rapid decisions on how to protect themselves against a pending attack, how to respond during the attack, and what action to take post-attack,’ says Gyde.

‘This is an exciting time for IT security professionals. We foresee security remaining high on the boardroom agenda throughout 2015 ... and beyond,’ he concludes.

‘This is an exciting time for IT security professionals. We foresee security remaining high on the boardroom agenda throughout 2015 ... and beyond.’