NTT Security 2017 Security Trends & Predictions

Garry Sidaway, SVP Security Strategy, NTT Security

Identity will once again raise its ugly head

We have known for a long time that passwords do not provide the necessary level of assurance that is required in the mobile digital age. Convenience and security are uneasy bedfellows and, whilst passwords are convenient, they are increasingly seen as weak tokens of identity. The demand for convenience by the consumer and digital workforce and the increase in mobile phone use will drive a renewed emphasis for identity solutions. Combining something you have with somewhere you are and something you know will see the decline of passwords as the primary authentication method. This combination of physical and digital, with the emergence of advanced authentication methods, will provide the catalyst for new identity solutions.

The phone for everything

The digital workforce lives and works in a society where mobile is king and most other things are being replaced by it – from mobile cash to social mobile. Our phone is now our digital hub, controlling how we are identified and authenticated into our world and how we control and interact digitally. Because of this we will see threat vectors concentrate on the devices in our hand rather than the devices on our laps. Security is traditionally focused on backend systems or containers – but this approach will have to change with protection built into mobile devices from the ground up.

User behaviour focus on insider threats

The threat from within has long been a headache for businesses, but advances in data analytics and increased focus on anomaly detection will continue into 2017. Defining normal behaviour will still be the challenge as businesses become increasingly dynamic, but advances in machine learning techniques will see user behaviour analytics added to endpoint solutions.

Deception rather than cure

We will see the increased use of deception technologies inside corporate boundaries. These are an extension to the honeypots that proliferate the Internet. It is a different approach that some organisations will adopt, but effectively accepts that an organisation will be breached at some point.

The end of signature detection

Whether we call this next generation AV or end point protection or endpoint detection and response, clearly we are seeing the evolution of endpoint protection beyond the use of just static signatures. The use of advanced data analytics now applies to any detection capability. The sharing of a known bad across the “platform” is essential and leveraging the cloud is a critical component of these solutions. The sheer volume and diversity of malware is driving a new approach that combines global collaboration – a ‘breach once, protect many’ philosophy, combined with threat intelligence to predict attacks and actively protect – to prevent the patient zero syndrome.

Blockchain

Data integrity has to be paramount as we increasingly rely on digital systems to hold every aspect of our lives. This reliance will drive blockchain adoption, Bitcoin being the most well known. Banks are clearly advanced in this area, but the underlying techniques and trust model will be considered in other areas where data integrity is paramount. New payments services are already being introduced because they offer greater security and are cheaper to implement than current systems. However, it will take greater industry adoption and collaboration before this really takes hold.

The rise of the complete services companies

The consolidation of the cybersecurity landscape is also leading businesses to focus on the complete services solutions across the ICT stack. Where previously the value from an MSSP was stitching together a complex and in-depth solution, the value now is in providing embedded security into the complete lifecycle of the business and providing business applications, network infrastructure, cloud and data centres, along with the single pane of glass and single provider solution. Components of a complete solution provided by different suppliers will no longer be the norm. Providers will have to be able to provide a co-ordinated and complete end-to-end service for the digital workspace.

Stuart Reed, Senior Director of Global Product Marketing

Consumers will demand transparency

Recent research by NTT Security into online shopping behavior highlighted the growing demand from consumers around transparency of both policy and incidents from organisations. High profile breaches – particularly of well-known household names – have heightened consumer awareness and understanding of data breaches. This trend is likely to continue into 2017 and beyond. Those businesses that can demonstrate their security policies and response plans to customers will help lower their exposure to risk and drive competitive advantage against their peers.

Innovation will continue to fuel consolidation

This year has seen significant consolidation within the cybersecurity market – both from a services and vendor perspective. This included the BlueCoat acquisition by Symantec, Cisco's various acquisitions, and from our own perspective, the formation of a specialised security company, NTT Security, bringing together advanced analytics technologies, threat intelligence and security experts. Market consolidation is fuelled in part by innovation, where smaller organisations with a particular specialism are integrated into a larger organisation, with a view to providing a more rounded offering to customers. But also it means larger companies can foster innovation through incubation programmes, made possible by efficiencies and expertise gained through economies of scale. This will continue, underpinning the importance of innovation in security to stay relevant to customers.

The Identity of Things

The emergence of the Internet of Things has further blended the physical and digital worlds and has driven both convenience and efficiency gains. IoT is driving an enhanced user experience and more effective way of doing things. However, criminals are looking at ways to exploit vulnerabilities that may exist. We have seen evidence already of cybercriminals using internet-connected home devices, like CCTV cameras and printers to launch DDoS attacks to immobilise sites like Twitter and Spotify. 2017 is likely to see further exploits of IoT devices and highlight the need to wrap them into a comprehensive security policy and ensure the identity and operation of these devices is legitimate.

DDoS attacks will cost businesses

Most businesses are failing to realise the potential impact of distributed denial of service attacks (DDoS) which is why they are not budgeting for them or implementing the right controls and response plans. DDoS attacks aim to disrupt or block an organisation's web services, and recent high profile incidents like the attacks though US company Dyn using connected home devices (as above) and the one on security website Krebs, will help push it up the corporate security agenda. But increasingly these will be driven by extortion, with ransom-based attacks becoming more common and companies prepared to pay off cyber criminals to avoid customer attrition and financial loss.

Advanced analytics will be a game changer

One of the big data challenges for cybersecurity is how to drive relevance and insight from all of the various pieces of technology used to protect an organisation. Data analysis has been used to give meaning, but as the threat landscape evolves, so too must the way we interpret and drive context from information. Advanced analysis will be key in making sure the right risk management decisions are made. This is far more than just looking at what is going on right now; it also means looking at historic patterns, and employing artificial intelligence that continually learns patterns of behaviour and ultimately anticipates or predicts when an attack may occur. A balance of sophisticated machine learning, automated analysis and "eyes on glass" security experts will be a powerful combination that will change the dynamics of managed security.

Kai Grunwitz, Senior Vice President Central Europe, NTT Security

Cybersecurity will become a critical success factor for businesses

But only when it is deeply and seamlessly integrated into all business processes from the beginning, will it be accepted by business stakeholders. In a connected and growing digital business world, customers expect cybersecurity to be fully embedded in their business and IT strategy. Protecting the key values of company data, IP or production environments and, in parallel, becoming an integrated part of the innovation and business transformation process.

Security will no longer be just a matter for the IT department; it has to be a vital part of business processes supporting the value chain of an enterprise. Efficiently managing the security lifecycle will become an important differentiator and key priority for a business-driven security strategy – creating competitive advantage and value.

Chris Knowles, Solutions Director, NTT Security

GDPR, GDPR everywhere!

If you thought there was a lot of coverage around GDPR this year, wait until you see what 2017 has in store. Every vendor will be positioning how their technology is the answer and why it is essential, legal teams will be debating what 'state of the art security' really means, and customers will start to plan for what it means to them.

In the land of the blind, the one eyed man is king, but not for much longer!

For many organisations, security is focused on the perimeter and on inline devices that should see all traffic and respond based on what it sees. However, as more of a company's workforce becomes mobile and more applications are running in the cloud (as they continue to virtualise everything) then multiple 'blind spots' are created. Traffic is passed in and out via encrypted tunnels, data is stored and processed outside of a secure data centre and virtual machines talk to virtual machines – all of this without being 'seen' by existing security controls. Companies will start to recognise this and look to put eyes everywhere to eliminate blind spots and take back control.