Discussing APTs
How do we fight APTs?
The issues are identified and tackled P24

Securing the IoT
Are multiple connected devices fueling a corporate security nightmare? P12

Anne-Marie Eklund Löwinder, CISO at .SE, sheds light on some of the issues surrounding DNSSEC and its slow uptake internationally P16
NEWS/FEATURES

6 IQ Information sharing; CISO skills - debate; risk management teams; news; Bash; movers and makers

12 Securing the Internet of Things
Multiple connected Internet of Things’ devices could be fuelling a corporate security nightmare suggests Kate O’Flaherty

16 Keys to the Internet
Anne-Marie Eklund Löwinder of .SE explains the background to DNSSEC and its benefits

21 Russia revamps its infosec strategy
Eugene Gerden in St Petersburg reports on Russian strategies to cope with cyber-crime – while also seeking international cooperation

24 APT Attacks: Time to respond
Advanced persistent threat (APT) attacks are designed to evade detection, leaving IT security teams in the dark. These issues are identified and tackled, plus the SCMagazineUK Roundtable report

OPINION

5 Editorial
Rising to the challenge

34 Last word
A cyber-security health check by Nick Polland

PRODUCT REVIEWS: INDUSTRY INNOVATORS

28 Industry innovators: These tools address the rash of large-scale attacks and can fend off those to come by Peter Stephenson

29 Access control

30 Virtualisation and cloud security

31 Innovators

For any questions or enquiries regarding the virtual event, please contact:
Payal Padhiar, payal.padhiar@haymarket.com

For sponsorship opportunities, please contact:
Martin Hallett, martin.hallett@haymarket.com • Dennis Koster, dennis.koster@haymarket.com
Rising to the challenge

While the specific security threats in the year ahead are unknown, the trend is clear – there will be more frequent attacks and they’ll be bigger and more sophisticated than ever before. And regardless of the budget increases we may receive, we’re likely to be stretched in terms of both technology and qualified manpower.

However, we are not defenceless, neither less bright nor less well resourced than our adversaries – but we need to raise our game as fast or quicker than they can.

In this issue we look at some of the best advice on dealing with Advanced Persistent Threats (APTs). These have become increasingly common as nation-state level attacker-tools have shifted down the food chain to organised crime groups, hacktivists and even disgruntled individuals. As delegates at SC’s APT roundtable pointed out, knowing what’s happening on your network enables rapid identification and remediation, with technology and automation options growing while outsourced cloud services also reduce the threat landscape (p 24).

Conversely, the nascent Internet of Things (IoT) is clearly increasing the attack surface for hostile actors, making corporate strategy a nightmare (p 12). Devices not intended to be connected have weak defence and often poor patching – if any, while even new ‘internet-enabled’ things, such as domestic appliances, certainly don’t have a network manager plugging newly discovered vulnerabilities. The result? Treat all networked devices as computers.

The services we use also contribute to our security, with the internet at the core of all modern communications – along with the ISPs and registrars that provide our access. While the security extensions to DNS are endorsed by most internet pioneers as a good thing – including Anne Marie Eklund-Lowinder interviewed in this issue – there are critics of DNSSEC too, and consequently uptake is slower than expected (p 16).

Also in this issue, we look at Russia’s internet strategy – from a Russian perspective (p 21).

We end this issue with the call for companies to use the New Year to carry out a security health check and audit (p 34), preparing for the year ahead – as we’re expecting a challenging 2015!
And it burns, burns, burns

Radware’s Global application and security report, Ring of Fire (illustrated right), shows that the likelihood of attack (highest at the centre) has increased for all categories except finance – which Radware regional director UK & Ireland, Adrian Crawley, noted to SC, has invested heavily in defense in recent years – though Sarb Sembhi, director of Storm Guidance suggested this may also be due to a ‘glut’ of financial details in the market putting down their value.

Attacks are larger and longer lasting, using a mix of vectors, with some organisations under constant attack. The growth is both in volumetric attacks and application attacks – 50:50. Application and reflection techniques are pushing DDoS attacks up to 100GB and beyond. They are also dynamic. One retailer blocked all traffic from Russia, and the attackers switched location on the fly to China.

These courses range from digital forensics to the recruitment of the appropriate cyber-security staff, and are open to individuals and companies (acting on behalf of their employees). Chris Ennor, deputy director for the National Technical Authority at CESG, explained to SCMagazineUK at the time that the course is part of the wider National Cyber Security Programme Objective 4: Building the UK’s cyber security knowledge, skills and capability.

Ennor told SC that a primary purpose is for those in the industry seeking to improve or demonstrate their skill level to have independent criteria to help them navigate through the cyber-security training landscape and choose from the options available.

European cyber-criminals have created new ‘Daredevil’ malware that explicitly targets electronic ticketing machines and kiosks such as those found in train stations. And, in another leap by the bad guys, users of European bank ATM machines are being hit by a new, almost invisible ‘wreapping’ device which chews up bandwidth but doesn’t deny it.

Hackers GDP have since demanded a halt to the release of ‘The Interview’ - a comedy film which features a plot by the CIA to assassinate North Korea’s leader Kim Jong-un.

They said it

“IT complexity will continue to be the single biggest risk to financial services organisations in the coming year”

—from A KPMG REPORT ON IT FAILURES

NEWS BRIEFS

>>When US film and TV company Sony Pictures Entertainment (SPE) was hit by a blackmailing hacker attack it refused to pay and saw the attackers shut down its IT systems, hijack Twitter accounts and steal confidential documents and passwords plus leak films pre-launch.

The attack was launched by the ‘Guards of Peace’ (GOP) group who threatened to expose the company’s ‘top secret data’ if their demands were not met. SPE subsequently hired FireEye’s Mandiant forensics team to clean up the damage from the attack which the US Federal Bureau of Investigation (FBI) has been investigating.

North Korea was suspected as being behind the move – although it had denied it, and some security experts agree. In one of the biggest data breaches in recent times, five films including one unreleased, were leaked onto file-sharing websites, while thousands of employee records were also compromised.

SPE was then reported to be launching distributed denial of service (DDoS) type attacks on websites containing its stolen data. A report on US website bârâzî said it was using hundreds of computers in Asia to execute the attacks via Amazon’s Web Services (AWS) cloud computing unit. If Sony is responsible, it is apparently using a method of restricted access to “make the website crawl,” Tony Reeves, IT security expert at PA Consulting Group, told SCMagazineUK. “Instead of bombarding the address, it is a slow trickle attack on it. A crawling attack makes it awkward to access the information: it chews up bandwidth but doesn’t deny it.”

Hackers GDP have since demanded a halt to the release of ‘The Interview’ - a comedy film which features a plot by the CIA to assassinate North Korea’s leader Kim Jong-un.

>>ATMs and electronic ticketing machines are facing further hacks as fraudsters focus on inadequately defended environments.

>>KPMG released a surprising report which revealed the real problems UK businesses are having in terms of recruiting the right staff – in so far as almost half are considering hiring former hackers or those with a criminal record. Surveying 300 senior IT and HR professionals in organisations employing 500 or more staff, the consultancy found that three in four of these (74 percent) believe that new cyber-challenges will require new skills, with 64 percent admitting that these skills are different to those offered by conventional IT.

Skills shortages were most keenly felt in data protection and privacy (70 percent of firms admit they lack expertise in these areas), while almost half (57 percent) admitting concern at holding onto those with specialised skills. Most interestingly, 53 percent said that they would consider hiring a hacker or someone with a criminal record – something which did not go down well with leading experts.

They said it

“IT complexity will continue to be the single biggest risk to financial services organisations in the coming year”

—from A KPMG REPORT ON IT FAILURES

Movers and makers

Giovanni Buttarelli

Giovanni Buttarelli becomes Europe’s new data protection watchdog, with his role as the next European data protection supervisor (EDPS). His assistant supervisor will be Wojciech Rafał Wiewiórowski.

KPMG has completed the acquisition of P3, a privately-owned German cyber-security firm offering risk management services across fixed and mobile networks.

Looking ahead are Allen Cockerill and David Helter at its leadership team, as vice president of enterprise product and vice president of worldwide channel development respectively.

Technology services company, Telenet, will acquire Telindus UK, in a deal that will bring additional multi-vendor capability and accredited engineers into the Telent fold.

After nearly 12 years at McAfee, Bryan Barney joins Sophos as senior vice president and general manager, running network security. The company also added Karl Heinz Warum, previously of Dell, as regional vice president of sales for much of Europe, the Middle East, and Africa.

MetricStream adds to its executive leadership team with the appointment of French Caldwell as chief evangelist. Caldwell is former vice president and Gartner fellow at Gartner Inc.
Announced as part of the government’s £860 million Cyber Security Strategy back in 2012, CERT-UK launched on 31 March 2014 and was set some challenging objectives, including liaising with public and private sector – as well as national CERTs – on emerging threats, and offering guidance and protection to companies working on the UK’s national critical infrastructure.

Integration initiative tested

A key component, and early success, of the group has been the integrated CiSP initiative which – after being tested on 160 UK companies across a range of sectors in a pre-launch trial – has been set up to offer a secure virtual ‘collaboration environment’ where government and industry partners can share real-time information on threats and vulnerabilities.

CERT-UK opens the door to cross-sector information sharing

The UK’s National Computer Emergency Response Team (CERT-UK) has shown some promising signs in its first year, with the connected Cyber Security Information Sharing Partnership (GiSP) initiative looking to improve cross-sector information sharing on security threats.

Announced as part of the government’s £860 million Cyber Security Strategy back in 2012, CERT-UK launched on 31 March 2014 and was set some challenging objectives, including liaising with public and private sector – as well as national CERTs – on emerging threats, and offering guidance and protection to companies working on the UK’s national critical infrastructure.

Integration initiative tested

A key component, and early success, of the group has been the integrated GiSP initiative which – after being tested on 160 UK companies across a range of sectors in a pre-launch trial – has been set up to offer a secure virtual ‘collaboration environment’ where government and industry partners can share real-time information on threats and vulnerabilities.

CERT-UK head Chris Gibson said that it is for all organisations – with even a primary school having joined the project. “The most interesting stuff is on GiSP – so if you’re not on GiSP, why not, get on GiSP,” he told delegates at the Cyber Security Summit this past November.

Gibson admitted that there are challenges ahead – not least with security awareness in a country with 4.9 million SMEs – but his team are forging ahead with new initiatives including local GiSP intelligence ‘nodes’ that will establish around the country. But for now, it is receiving the plaudits from the wider industry.

Vital contribution to intelligence sharing

“CERT-UK will provide a vital service in cyber-threat intelligence information sharing,” said Ben Densham, CTO of 500, and CERT-UK head Chris Gibson said that it is for all organisations – with even a primary school having joined the project. “The most interesting stuff is on GiSP SMEs - but his team are forging ahead with new initiatives including local GiSP intelligence ‘nodes’ that will established around the country. But for now, it is receiving the plaudits from the wider industry.

Vital contribution to intelligence sharing

“CERT-UK will provide a vital service in cyber-threat intelligence information sharing,” said Ben Densham, CTO of 500, and CERT-UK head Chris Gibson said that it is for all organisations – with even a primary school having joined the project. “The most interesting stuff is on GiSP SMEs - but his team are forging ahead with new initiatives including local GiSP intelligence ‘nodes’ that will established around the country. But for now, it is receiving the plaudits from the wider industry.

Vital contribution to intelligence sharing

“CERT-UK will provide a vital service in cyber-threat intelligence information sharing,” said Ben Densham, CTO of 500, and CERT-UK head Chris Gibson said that it is for all organisations – with even a primary school having joined the project. “The most interesting stuff is on GiSP SMEs - but his team are forging ahead with new initiatives including local GiSP intelligence ‘nodes’ that will established around the country. But for now, it is receiving the plaudits from the wider industry.
Debate

CISOs must have a technical background

Pro

Gareth Lindahl-Wise, CISO, ITC Secure

My starting position would be that a technical background is not critical but it can be helpful, if it’s not at the expense of other things.

I think a high-level tech overview can tell you when something sounds right or when something doesn’t tally. The ability to translate technology responses and risk to the senior level is important, as is the ability to challenge the advice and information you’re getting to keep staff and suppliers honest and on their toes.

In a big organisation, there’s probably a big IT security function so that a base of knowledge can come from elsewhere. There’s probably a skills curve, where the technical skills drop off at a bigger organisation. But in any environment, a broad base of knowledge can come from elsewhere.

Technical skills drop off at a bigger organisation. But in any environment, a broad base of knowledge can come from elsewhere.

Anti

Quentyn Taylor, director of information security, Canon EMEA

To be honest I agree (with Gareth) but the most important skills are non-technical. You can get dragged into the detail and you don’t want to do security for security’s sake.

Many of the people I’ve interviewed recently lacked these business skills, and the biggest challenge with a lot of CISOs is that they say that the board doesn’t understand their language. But you’ve got to ask ‘how many of them understand me?’ If they don’t, surely it’s you – the CISO – that has the problem, not them.

IT security is not alone; IT, CSR, legal and the marcoms departments have all been doing this for a long time – they’re talking in different terms and they have their own common lexicon.

The business people make the money so you need to listen to them. You are there as loss prevention and risk management to save the company money. As they make the money, from that perspective they’re much more important than you.

If I were a CISO my first focus would be on communication – if they can’t communicate internally or externally, to shareholders (or the board), they’re not going to be very useful at their jobs.

They’d also need to understand the business and its risks, what those risks are, how they impact you and when to take risks. And understand what the business process is – every business is different and there will be unique and different risk tolerances.

CISOs must have a technical background

The SC Awards Europe 2015 are the highlight of the industry’s calendar – and not just for the highly enjoyable social evening at Grosvenor House on Park Lane among the main players in the industry. But also because it ensures well deserved public recognition for all the hard-work behind delivering excellence, with your peers, in the knowledge that winners really have achieved something special, judged by informed independent experts who are passionate about rewarding the best.

Professional Awards - benefits of winning

The professional awards apply to individuals and teams, recognising excellence among the people that make up this fascinating and dynamic industry. People are the greatest strength of the industry, and independent recognition is career-enhancing for those judged the best in their category, and it’s a fantastic testimonial for company teams recognised as being at the top of their game.

Delivering excellence

M

What is it?
The original vulnerability in Bash, dubbed ShellShock, can be exploited to execute arbitrary shell commands to compromise a vulnerable system. More vulnerabilities also have been reported.

How does it work?
Multiple attack vectors for Bash exist as many organisations use products which contain Bash in multiple parts of their infrastructure.

Should I be worried?
Yes. With the vulnerabilities came a host of patches with varying degrees of efficiency. At the time of writing, all known bugs in Bash have been fixed with official upstream patches.

How can I prevent it?
Apply the patches provided by Bash. However, not all products containing Bash have been fixed yet so keep a close eye on those products and patch them as soon as possible. If you are a system administrator, you need to diligently assess the risk to your systems; apply the patches and look for other ways to mitigate where no patch is available, and then go back to verify the result.

– Kaspar Lindgaard, director of research and security, Secunia
Multiple connected ‘Internet of Things’ devices could be fuelling a corporate security nightmare suggests Kate O’Flaherty

The damage that can be done by Internet of Things (IoT) devices is already being seen. Last November, thousands of CCTV pictures capturing baby monitors and home surveillance systems were broadcast on a Russian website.

The problem is growing in scope and scale. In the US, the Department of Homeland Security has reportedly been investigating cases of suspected security flaws in medical devices and hospital equipment.

But this is not slowing the growth of IoT in the enterprise. Machine-to-machine (M2M) sensor technology is infiltrating the retail, manufacturing and logistics industries. ‘Smart’ machines such as coffee makers are increasingly likely to plug into the corporate network - and this is on top of the connected devices brought to work by employees.

Meanwhile, IoT poses a very real threat to the consumer in the form of automated cars as well as smart meters in the home, which could be compromised by hackers to devastating effect.

Experts predict the security problems associated with IoT will soon begin to surge. According to analyst Gartner, there will be nearly 26 billion IoT devices by 2020. The firm says this will lead to over 20 percent of enterprises having digital security services devoted to protecting business initiatives using IoT devices and services by the end of 2017.

Problems associated with IoT can be complex: the technology requires a new understanding of how devices must be secured. It is said that infrastructure is IoT’s weak point, due to the wireless networks that enable communication between devices, which could be exploited by hackers as a point-of-entry to the corporate network.

The effort needed by would-be attackers is small. This was recently
If you have a coffee maker that you want to connect to the corporate network, then you need to either treat it as a major system or not connect it.

— Jon Collins, GigaOm research analyst

IoT devices, you can quickly instrument them and there is no way to track you as the attacker - you are anonymous,” says Larson.

Adding to this, says Larson, most discreet distributed denial of service (DDoS) attacks are very small and remain unseen. “They are going unnoticed by today's security infrastructure, which means they are a latent risk in the environment,” he says.

This indicates that over the long term, IoT devices could be a favoured point of entry for compromising other, bigger targets, says Derek Manky, global security strategist at Fortinet. “For example, if organised crime wants to take down a bank, the in-vehicle infotainment system of an employee's car might be an early starting point; one that could legitimately allow access to their address book, business applications or intellectual property.”

IoT devices use IPv6 systems, which themselves have been built with robustness in mind. However, although these are “safety critical”, they are not necessarily “security critical”, says Haydn Povey technical advisor at Beecham Research. “If you have to be robust, you may not encrypt data because you don’t expect a man in the middle attack.”

And the threat has the scope to get much bigger. According to Povey, IoT technology could be exploited to impact on critical infrastructure such as that used by the broadcast and energy industries, making the UK vulnerable to cyber-warfare-type attacks. Collins advises a domain-based architecture - a sub-network for ‘things’ - dividing the corporate network into ‘zones’. “It’s an extension of BYOD,” he says.

Additionally, Collins says: “If you have a coffee-maker that you want to connect to the corporate network, then you need to either treat it as a major system, or not connect it.”

This ethos should be applied across the board, with firms reviewing the corporate network to make sure low and high security devices are not combined. Collins explains: “Treat it as another network device. It doesn’t matter if it is a coffee machine or central server; they are both computers.”

Another IoT device that you may find in your workplace is a print server, or wireless access point. Most attacks do not target these devices per se, but instead the underlying network infrastructure. The printer or access point may be used by the attacker to gain an entry point into the network or to have a lower privilege account.

It is important to note that many connected devices are not properly secured, with a significant number of devices using weak or default passwords. This means that attackers can easily gain access to these devices and use them as a pivot point to attack other devices on the network.

Security measures

The threat of these large-scale attacks is not immediate, but experts advise firms to take preventative measures as soon as possible. This can be fairly simple: IoT as a concept creates very similar issues to those posed by Bring Your Own Device (BYOD).

However, the answer isn’t to ban devices: “It never works,” says Collins. Instead, he says, IoT security centres around education and scenario planning.

He explains: “The information security question is the same as the address: ‘things’ generate information and that is subject to the same risks - confidentiality, integrity and availability. The downside is that every single time we invent a new technology mechanism, security is left until last.”

In practice, a secure IoT application must protect the transmission of private and confidential data, says Olivier Beaujard, VP market development at Sierra Wireless. “This involves data encryption and secure transmission technologies across multiple segments of the M2M application – the network as well as the cloud management platform and the enterprise application,” he says.

If corporate information is available in devices, it is important to have a good understanding of the security architecture. Collins advises a domain-based architecture - a sub-network for ‘things’ - dividing the corporate network into ‘zones’. “It’s an extension of BYOD,” he says.

Additionally, Collins says: “If you have a coffee-maker that you want to connect to the corporate network, then you need to either treat it as a major system, or not connect it.”

This ethos should be applied across the board, with firms reviewing the corporate network to make sure low and high security devices are not combined. Collins explains: “Treat it as another network device. It doesn’t matter if it is a coffee machine or central server; they are both computers.”

Securing devices in the workplace centres around ‘hygiene’, says Povey: in other words, making sure they have sufficient encryption and authentication mechanisms. “It comes down to simple things like passwords and making sure they are changed, making a log of these devices and being specific on what they can and can’t talk to. That is just good practice.”

Additionally, he says, policy management and orchestration is key. “You need to make sure policy management is around devices so if they start to spew out a DDoS attack, you can quarantine it and shut it down.”

Life cycle management is also integral in managing IoT, says Povey. “As we have recently seen with Heartbleed, even fundamental technologies can be broken. The challenge with IoT is these devices have a ten-year lifecycle. You don’t swap a fridge every two years like a phone.”

Updating devices

Disparate software run by IoT devices - which often has to be updated manually - can also pose a problem. According to Johansson, low-power and embedded IoT devices run old software stacks.

“They are made and manufactured with low security, often Linux-based,” he says.

Additionally, Johansson warns: “Devices will have their own update cycles and mechanism and some will be totally embedded. It creates a divide: one device may be fully pre-armed and the other could be manual. This requires a proactive approach to security.”

The state of security for IoT devices is “nowhere near comparable” to that driven by the likes of Microsoft and Adobe, says Manky. “Many IoT vendors will not have proper updates, or patch management – which is a huge risk to businesses in places which means plenty of holes will remain open for a long period of time.”

The Internet of Things is still in its infancy: it will have to grow much bigger before large scale attacks are a threat. But as the technology becomes more sophisticated, the risks will multiply. Collins says: “I’d be less worried about connecting dumb devices that could be hacked; what about smart devices that could turn rogue? What if the coffee machine has a powerful enough processor that could be turned into a surveillance device?”

“This means that enterprises should begin to guard now against what could eventually become an overwhelming security issue - rather than wait for a high-profile incident to occur. Skipper warns: “While controls are rapidly being introduced to improve security, there is a huge amount to do, and we should expect at least a handful of high profile incidents before everything is properly locked down.”
International uptake has been slow for the DNS security extension (DNSSEC) which authenticates URL queries. Tony Morbin spoke to Anne-Marie Eklund Löwinder to get a better understanding of the issues.

Anne-Marie Eklund Löwinder, CISO at .SE and one of the crypto-officers with a key to manage DNSSEC for the internet root zone, explained to SC: “We were all pioneers who just wanted to do the best for the internet, but by 1994/95 we had found that it was easy to cheat the DNS, to put false information in between the sender and the receiver,” and this led to development of DNS Security Extensions (DNSSEC). DNSSEC provides DNS clients (resolvers) with origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

Sweden was the first country to adopt DNSSEC and Eklund Löwinder explained her role: “I’d been interested in DNSSEC since 1999, when I was with the Swedish government in their ICT. When the Domain Name System (DNS), the internet’s ‘phone directory’ or registry, was developed 30 years ago security and confidentiality were not considered issues - the aim was to be a scalable distributed system that was open and accessible.

Improving uptake

James Galvin, director, strategic relationships and technical standards at Afilias, in his blog summarised below, reports that DNSSEC technology standards have been stable and mature since 2007, with only updates, clarifications, and new functionality added since then. Yet only 12 percent of global DNS queries involved some kind of DNSSEC validation by October last year, leading Galvin to assert that “waiting until the standards are final” is no longer a valid reason to delay deployment.

Major stumbling blocks identified are that: “The new ICANN policy for gTLDs (generic top level domains) mandates signed TLD zones, but not signed second level delegation. In addition, the 2013 Registrar Accreditation Agreement (RAA) requires registrars to offer “DNSSEC services,” but only for those registries that require it. (Also) It is not possible for a gTLD domain name registration with active DNSSEC to be transferred from one registrar to another without breaking the security chain of trust.”

Galvin adds: “DNSSEC is not just about protecting the DNS, it is about building a secure infrastructure foundation upon which new and innovative services and applications can be built to benefit us all. Registrars are the linchpins to advancing the deployment of DNSSEC.”

Usually the registrar registers and hosts a domain, but where domain name owners use a third-party DNS service provider for DNS hosting, or host the names themselves, for the domain name owner to sign their name, the DNS service provider must do the DNSSEC signing for them, thereby creating what Galvin describes as a ‘functionality gap.’ The registrar can potentially bear an administrative burden for a service the domain name owner chose to obtain from a third party.

Galvin concludes: “We cannot let these critical yet granular key-passing processes impede the deployment of DNSSEC and its promise to deliver a more secure internet infrastructure for every internet user.”
**Analysis**

**Dns itself, in the original version, is very forgiving**

– Anne-Marie Eklund Löwinder, CISO, .SE and crypto officer, DNSSEC

**Keys to the internet**

Being one of seven key holders to the internet’s ‘command and control’ system sounds like something out of Lord of the Rings, and there are in fact physical keys – not just digital keys – involved in an elaborate ceremony where the key holders meet in a secure facility watched over by armed guards.

Eklund Löwinder told SC: “When we start-ed in 2005 we were the only ones signing our DNS, checking and validating, so as we were the first we became the ‘trust anchor’. In cryptography and key management, a chain of trust should be unbroken from the lowest level to the top level. So the Trust Anchor, the thing that you have to trust – was .SE at that time.

“More and more TLDs (Top Level Domains) are signing their zones, checking and validating the signatures. Before the roots were signed, the internet service providers needed to keep track of every key for every TLD. In 2010 we finally convinced ICANN with a global chain of trust. During the six hour ceremony, within a barred cage inside the secure facility the crypto officers open their safe-deposit box in the safe using their physical key to open it to reveal the credentials (smart cards) to activate the hardware security module.

ICANN is neutral, but based in Californi-a, controlled by NTIA (the US National Telecommunications & Information Administration) and the US Department of Commerce, so some people don’t trust their independence. Consequently signing and key management for the root needed to be very transparent and open – that is where the crypto officers come in, because they are from different parts of the world, elected or nominated by their local internet communities. Their main task is to put trust in the system. ‘We are observing, monitoring the way that the management performs and saying, with our name and reputation at stake – that, yes, this is following the processes promised, and that we think they are doing it the best way, and that we can guarantee that nothing odd happened during this ceremony.”

People are putting their security credentials within their DNS system using DANE to get it distributed in a safe way. And it is not reliant on certificate authorities – and they have had some issues lately. There has been fraudulent behaviour within their staff, or they have been issuing certificates to people who shouldn’t have them.”

DNSSEC also has a role in the smart grid environment and the Internet of Things, from voice over IP to automated cars and connected fridges. It’s communication – you need to look up function, thus IP address to connect you to the domain. So a refrigerator can have the serial number as the domain, and @.uk. Lack of human involvement means it’s difficult – requiring excellent monitoring, and constant scrutinising of log information - to detect if something is going on.

If DNSSEC is so good, why isn’t it used more widely implemented? Eklund Löwinder responds: “One of the problems is that there has been no huge incident - though there have been smaller ones. You are adding a complexity to DNS that we are not used to. DNS itself, in the original version, is very forgiving. You can do a lot of things wrong but it still works – its amazing, really amazing.”

Will such complexity not have both cost and performance issues? Eklund Löwinder says not, adding: “People who argue against DNSSEC always say, ‘It will affect the performance of my systems; it will cost a lot to implement; it will need more people,’ but we have proved that’s not true. This is a natural evolution. Meaning that you have the infrastructure which needs to be updated, you need to replace older servers with new servers, old software with new software. It’s just business as usual.”

Not everyone is convinced. In fact there is an entire website devoted to cataloguing problems with DNSSEC (http://www.isani.com/pubs/dnsec-outages.html) – but defenders of DNSSEC say that some of the information on the site is clearly wrong, and some of the incidents on the list have nothing to do with DNSSEC.

Issues include: some faults in DNS are only visible in DNSSEC – and then only when validating; several faults exist in DNS software that apply only to DNSSEC – and this has led to disruptions detailed in the website above; the DNS software must be updated more frequently; it is more difficult to debug DNS with DNSSEC; DNSSEC requires keeping track of additional details; in certain cases, different types of DNS software do not work together and it can be difficult to locate the fault.

Dan York at the Internet Society’s Deploy360 Programme adds: “There are two sides to DNSSEC – signing of domain names and validation. You can enable DNSSEC validation by changing just a single configuration line for a DNS server. Issues of the sorts that may have caused outages in the past are not as prominent today.”

Signalling can be more complex, but some DNS operators and registrars have made it as simple as a single checkbox. There are some 60 TLDs signed with DNSSEC and millions of individual domains. York says: “DNSSEC requires network operators to pay more attention to DNS and add new operational practices. As DNSSEC deployment continues, these practices are being documented so that over time the level of education within network operators will ensure that DNSSEC.”

**Dns spoofing in the wild**

Last November there was an attack by pro-Bashar al-Assad group the Syrian Electronic Army (SEA) which was believed to use DNS hijacking when it hacked the websites of several UK newspapers and a host of global and tech firms.

The hack appears to have resulted from the compromise of a third-party service, GoDaddy-owned marketing company (CDN) Gigya, with SEA getting credentials at GoDaddy, and then directing Gigya domains to websites controlled by the hackers via DNS hijacking. Ernest Hil bert, a security con-sultant at Kroll Cyber, was reported as saying “It is a DNS takeover, and this is what the Syr ian Electronic Army does. (When searching for a URL) not every user can get in through one connection, particularly at bigger sites. A CDN (Content Delivery Network) means that, because you can’t all fit in through the same door, it sends you to another version of the content. And one of those versions, which hosts copies of all those affected sites, appears to have been compromised by the Syrian Electronic Army.”

Raj Samani, CTO EMEA at McAfee, said in an email to SCMagazineUK: “This particular hack would appear to echo what was done against the NYT last year by edit-ing the DNS records to point to systems of their choosing. (However) I think the attack itself says less about DNS and more about the authentication requirements required for the edit of DNS records. We are not entirely sure what was done, but based on the information we have then we have a pretty good idea.

“If we look at the SEA in much of their recent attacks then this would appear a successful vector. The registrar did have 2-factor authentication as an option. There-fore questions will arise about whether this was used by the affected administrators. If not why not? We could even dive into the third party supplier issues as well – eg do companies go into this level of detail when assessing third parties they have a business relationship with?”

**with a global chain of trust. During the six hour ceremony, within a barred cage inside the secure facility the crypto officers open**
operations run even smoother.”

York concludes: “The reality is that despite the additional requirements, DNSSEC provides the best mechanism we have today to add more trust and security to DNS.”

Also, DNS allows you to find the right IP for a domain, so you can’t make it secret or confidential. But when implementing DNSSEC, you need to be able to tell someone if they are looking for something that doesn’t exist, you need to give a reply which is signed, but has not accepted the connection and this has proven very hard to do.

“You would receive a message, ‘This is what you asked for, this is the name before, and you realise there is nothing in between and you sign that reply. But attackers found that if they kept asking questions they could do the ‘zone walk’ or zone enumeration to identify a valid IP. “But we know there are other ways of getting the information about certain addresses; we don’t consider it a huge problem,” said Eklund Löwinder. However, it is reported that some registrars and many large organisations told the original working group members that DNSSEC as currently defined was unacceptable, and that they would not or legally could not deploy it. Hashed Authenticated Denial of Existence” (INSEC 3) is a way tackling the issue, putting a ‘checksum’ on the reply you get from DNS and by adding Salt and iteration, you get a reply that you can validate so that it’s not as easy to get the next domain in the list.

There is more work going on within the IETF using more cryptography, even in DNS, because it has become more obvious that you have to do more about both information security, and communication security. So further changes in the way DNS is implemented can be expected in the future, but not for some time. Eklund Löwinder says, “We need to find ways to do this as automatically as possible. That is where DNSSEC is lacking – tools; tools to define the zones, tools to renew your keys and signatures, something that makes it more automatic so that you don’t need human interference in the way that you do today. Absolutely, that will be essential for the Internet of Things.” She adds: “Using DNSSEC is only a part of secure communications. You have to be aware that information sent on the internet is open and available to anyone with enough interest to get it, no matter what, so you may need encryption between client and servers, like in TLS. Users shouldn’t need to think about security. It should be the vendors.”

Analysis

Users shouldn’t need to think about security. It should be the vendors

Anne-Marie Eklund Löwinder

DNS spoofing and man-in-the-middle

When you put in a web address on your computer or phone, the closest main server (the resolver) helps you to look up the right IP address for that specific service or that specific domain. The resolver converts the domain name to the IP address and connects to that service so you get to the right place. An attacker can put a false reply to your request and redirect you somewhere else that could look exactly like what you were expecting – eg your bank website. Alternatively, a man-in-the-middle can re-direct all the email you send to another mail server, and then (after looking at it) send it all off to the receiver as if nothing happened, and from the user’s perspective, you are not able to tell that this has happened.

When DNSSEC signs DNS lookups, the look-ups are cryptographically verified at the recipient, ensuring that the responses truly derive from the right source and have not been changed during transmission between name servers on the internet. It adds a key and digitally signs the reply that you get from the request adding a few more records per top level domain to the root zone file so that you can validate that this is the right net server, mail server, that you are talking to. DNSSEC thus provides a validation path for records. It does not encrypt or change the management of data and is ‘backward compatible’ with the current DNS and applications. It incorporates a chain of digital signatures into the DNS hierarchy with each level owning its own signature generating keys. During validation, DNSSEC follows this chain of trust up to the root automatically validating “child” keys with “parent” keys along the way. Since every key can be validated by the one above it, the only key needed to validate the whole domain name would be the top most parent or root key. Users also need to check and validate the signature received to get the full picture. It’s described as like banks checking your ID or credit card and verifying that you have used a valid signature on the paper.

Cyber-crime is as much a threat to ordinary Russians as anyone else, and the country is developing a strategy to cope – while seeking international cooperation too, as Eugene Gerden in St Petersburg reports

F rom a western perspective Russia’s cyber-activity is mostly seen as one of threat – whether engaged in espionage, organised crime, or hacktivists either supporting or opposing their country’s foreign and domestic policies.

But for Russians, the threats in cyber-space are exactly the same as in the West – even though the government has a radically different set of views about who and what constitutes a threat, including a different perspective on individual liberty versus the interests of the state. Consequently, the Russian government is now taking action to fight cyber-crime and identity theft as well as ensuring information security through the introduction of a new cyber-strategy. It is interesting to consider where points of common interest and potential cooperation may lay, and also what differences are likely to be irreconcilable.

The primary aims of the new strategy are to protect Russian web resources and internet activity from attack by hackers, cyber-terrorists and foreign cyber-spies. A key focus is protection of public networks and state internet-resources. As part of the new strategy, the government intends to consider cyber-attacks on its websites and resources as attempts to seize power, hence they will incur strict criminal liability.

The new strategy is expected to be implemented as part of a decree, “Principles of State Policy of the Russian Federation in the field of international information security for the period up to 2020” signed late last year by Russia’s President Vladimir Putin.

The decree was jointly drawn up by the Russian Security Council, the Ministry of Foreign Affairs, Ministry of Defence,
Russia’s cyber-criminals

Russia has a serious problem with organised cyber-criminals. Some reports suggest that at best there is an official indifference to Russian crimes, targeting foreigners, making international enforcement against Russian suspects difficult, and at worst, it has been suggested that there may be direct collusion between the Russian state and organised crime groups across the state’s borders.

Among the local crime groups alleged to have strong political connections is the Russian Business Network (RBN), which has been described by VerGign, as “the baddest of the bad”, offering web hosting services and internet access to all kinds of criminal activities, with individual activities earning up to $100 million in revenue. The RBN is not a registered company, and its domains are registered to anonymous addresses. Its owners are known only by nicknames. It does not advertise, and trades only in untraceable electronic transactions.

In a Wikipedia report, summarised here, it is described as a multi-faceted cybercrime organisation, specialising in personal identity theft for resale. It is the originator of Mirai and an alleged opera- tor of the now-defunct Storm botnet.

One known activity of the RBN is delivery of exploits through fake anti-spyware and anti-malware, for PC hijacking and personal identity theft. McAfee SiteAdvisor reported 279 “bad” downloads from malwaredomain.com, and found that MalwareAlarm is an update of the fake anti-spyware Malware Wiper. According to a new-issued Spammers report, RBN is “among the world’s worst spammer, mal- ware, phising and cybercrime-hosting networks. It provides ‘bulletproof hosting’, but is probably involved in the crime too.”

Ministry of Communications and the Ministry of Justice.

The intention to create a cyber-strategy was first announced by Vladimir Putin at the beginning of 2000, as a result of a perceived rapidly growing criminal and terror threat on the internet.

According to an official representative of Russia’s Presidential Administration, following the September 11, 2001 terrorist attacks in the United States, the methods used by terrorists have changed dramatically, forcing the Russian government to come up with new security measures to tackle them.

An (unnamed) official representative of Russia’s Presidential Administration comments: “The ever growing popularity of social networks and micro-blogs has contributed to a massive spread of terrorist ideology on the internet. Modern computer technologies have provided an opportunity for terrorists to recruit suicide bombers. At the same time the number of cyber-criminal groups has been increased and in particular those that steal personal information online and hack into electronic payment systems. The new strategy should help us to raise the level of information and IT security in the country and to start to more actively fight cyber-criminals.”

The new strategy outlines four main information and cyber-security threats in Russia.

One is the use of information and communication technologies as information weapons used to achieve national objectives, with the aim of carrying out hostile and aggressive acts.

The second one involves the use of information technologies for terrorist purposes.

The third threat is the ever growing number of cyber-crimes, which involve illegal access to computer information, as well as the creation and distribution of malicious programs.

The fourth threat is distinctive Russian and involves the use of internet technologies for intervention in internal state affairs, disturbing public order, stirring up national hatred (which is viewed as a very big problem in Russia, given its many regional groupings) and state subversive propaganda.

Impact of Arab Spring

According to sources in the Russian government, the main reason for the existence of the fourth threat in the bill is a result of recent political events and mass unrest in parts of the Middle East following the ‘Arab Spring’, which demonstrated the potential of the internet (especially social networks) to be used to organise and coordinate anti-government action.

Implementation of the strategy is intended to happen on both an internal and international level. In the latter case, the government plans to implement the strategy in cooperation with its allies, and especially the countries that are members of the Shanghai Cooperation Organisation, Collective Security Treaty Organisation and the BRICS nations.

In addition, Russia hopes to see several of its key international information security initiatives adopted by the United Nations, creating a convention on ensuring international information security, developing an internationally accepted code of conduct in cyber-space, as well as internationalising the internet management system, and establish- ment of an international legal regime of non-proliferation of information weapons.

To date most Western countries have opposed Russia’s information security initiatives, viewing them as being primarily to strengthen state control over the internet. However in recent years the Russian government has made strenuous efforts to overcome this view. This includes what is described as an ‘unprecedented’ agreement, signed last year by the Presidents of Russia and the US in Northern Ireland with the aim of preventing cyber-incidents escalating into international conflicts. These agreements are considered as very important in

Russia, and are viewed as comparable with the ‘hotlines’ between the USSR and the US during the cold war designed to prevent nuclear war and military conflict.

As part of the agreement, information security cooperation by the signatories will be based on the National Centres for Nuclear Risk Reduction, established in both countries in 1987. These centres operate around the clock, allowing the countries to notify each other of any missile tests, so they are not perceived as acts of aggression, as almost happened in 1983, when prior to the NATO Able Archer military exercises a false alarm in the Soviet warning system reported about a nuclear attack on the Soviet territory. Under the terms of the agreement the centres/facilities will be used for mutual reports and notifications of attacks on critical information infrastructure of both countries. In addition, two special channels will be created for the exchange of information about computer incidents and cyber-crimes.

UN cybercrime convention mooted

The first of these channels will be used for communication by the national security agencies of both countries regarding information security, while the second emergency readiness channel for computer incidents will specialise in the monitoring of malicious activities on the internet.

The Russian government plans to accelerate negotiations with other NATO countries in the near future with the aim of signing similar agreements.

In addition, the Russian government plans to propose to the UN that a universal UN convention on cyber-crimes be developed, and that cooperation with the US on this issue be further strengthened. This is reflected in recent agreements about fighting cyber-crime and ensuring information security, reached by Vladimir Kolokolcev, Russia’s interior minister with Robert Mueller FBI director during their meeting in Washington last year.

According to Kolokolcev, such cooperation will include drawing up and enacting laws on joint operations, as well as the exchange of information, to help curb cyber-crimes as well as identify model schemes for such crimes.

The Russian government also intends to design an effective security system against powerful malicious programs, similar to the highly-complex Stuxnet worm, which destroyed hundreds of uranium enrichment centrifuges at the Natanz facility in Iran in 2010. (Report written prior to public exposure of the Regin spyware).

There are also plans to abandon previously proposed initiatives of the Federal Security Service of Russia to ban Skype and Gmail e-mail services in the country as their traffic is not able to be controlled by intelligence agencies due to its encryption.

However it is expected that a ban will be imposed on the use of the RSA cryptographic algorithm in Russian information systems.

Another part of the new strategy will see increased use of biometric security, starting from fingerprint and iris scans, and in particular the use of fingerprints for biometric passports for all of the country’s citizens from the age of 12.

Implementation of the strategy will be carried out by a special state commission, headed by Russia’s senator Ruslan Gattarov.

According to Gattarov, currently only the United States has ‘digital sovereignty’ and a good level of information security. Implementation of the new strategy is intended to raise the level of information security in Russia, supported by a high level of domestic development in crucially important information systems.

Another driver is the increasing importance of the Russian internet (RuNet) to the economy as a whole, with a report ‘The Russian Internet Landscape’ by Frost & Sullivan, highlighting how its dominance by domestic players and its huge growth potential, with the Russian internet user base forecast to increase by up to another third over the next five to seven years.

The new strategy should help us to start to more actively fight cyber-criminals” — Russian Presidential Administration representative
APT ATTACKS: Time to respond

Advanced persistent threat (APT) attacks are complex, multi-layered and designed to evade detection, leaving IT security teams in the dark and sensitive data at risk. Doug Drinkwater asks how to respond

Cedric Pernet, threat intelligence analyst at Airbus Defence & Space and former law enforcement officer for the OPP in France, said: “I would define APT as a persistent targeted computer attack, aimed at compromising and keeping access to selected targets networks in order to steal information.” The complexity of these attacks is harder to gauge. “The sophistication of attacks can vary greatly,” admitted Pernet. “There is usually no talk about the ‘persistent’ aspect of this kind of threat, yet the word ‘advanced’ can be misleading. I still think this word is appropriate, not to describe the technical level of the attacks, but the way it is organised.

“An APT attack is not the work from a single attacker - it is an attack launched and handled by a team of attackers with different skills. Each one has specific tasks and responsibilities. Some of these attackers are in charge of collecting information about the target company from open sources, others are responsible for the first stage infection of the attack campaign or to infiltrate the attacker’s network infrastructure.”

Ed Wallace is director of incident response and advanced threats at MWR InfoSecurity - a consultancy which tracks 90 countries with APT-like capabilities to steal information or take-down computer systems – and he says that the sophistication is over-stated.

He says that “90 percent” of countries simply rely on email phishing, with the minority having more advanced capabilities for water holding attacks and data exfiltration. Other experts say social engineering is – along with software vulnerabilities and poorly-configured security - the best entry into an organisation.

Where there has been a change, Wallace says, is that nation states are now looking to steal contract bids, Joint Venture agreements and McAs. “It’s a lot more commercial focused – but it’s not necessarily that sophisticated,” Wallace told SC.

Attribution is trickier. Attackers are using various methods – including Tor and SSL encryption – to hide their activities, while nation states will often deny any involvement by blaming cyber-criminal groups instead.

“There is a change between criminals and nation-states, a blurring of the lines,” said Wallace. “Five years ago there was regular communication between the two but it petered out. That’s potentially returning because if you blame the criminal group you’ve got the perfect smokescreen.”

But Pernet says that attribution is impossible. “We should not be naïve about cyber-espionage: it is just an evolution of traditional espionage. Everyone is aware of espionage, and citizens from all around the world take part in it for granted. Why should it be different with cyber espionage?” Seth Berman, the executive managing director and UK head of cyber-intelligence outfit Stroz Friedberg, agreed adding that it is another way of collecting information, although he noted that some governments may consider APT attacks as a way of ‘expressing anger or disapproval’.

Geographical targets are easier to ascertain with Europe and the UK targeted because of its innovation and ideas, with China, in particular, taking a liberal view of IP theft.

Defence should involve the board

Defending against these attacks is difficult. Attackers create their own ‘tunnels’ inside corporate networks by using SSL encryption, and stolen data is enclosed in zip:exe files, making it difficult for IDS systems, firewalls, antivirus solutions to detect, and almost impossible for packet analysis.

To make matters worse, new malware can change code on a peer-to-peer basis – evading signature-based detection. Hackers meanwhile have the same tools as IT security teams and can – for example - turn vulnerability scanners to web-facing servers to further hide their activities.

If you can’t provide 24 hour defence manned by experts – get someone who can

– Jay Colley, senior director Akamai Technologies

There is a blurring of lines between criminal and nation-state APT attacks said delegates at the SC APT roundtable.
It that wasn’t bad enough, studies have shown that most UK firms are behind when it comes to log analysis. Resolution1 Security’s incident response specialist Sean Mason believes that defending APTs can only be done at a political level – but says that incident response teams have a choice when ‘breaking down the attack’.

“The first thing I would do is to try and break down the attack, in detail. Really understand the depth of it, break it down, mitigate the noise...and kick them out.” But he adds: “You can’t prevent this. If you’re talking nation-state, they’re not going to tell their boss ‘sorry, I can’t get to them’. What I tell CIOs and CSOs all the time is that investing in compliance-based, preventive technology has failed time and time again.”

This is a recurring theme with a recent Lieberman Software study indicating that eight in ten information security professionals believe that the aforementioned perimeter technologies are not enough to defend against APTs.

On publication of the report, Tim Holman, CEO of USA 2.5sec and president of the ISSA UK security professionals user group, told SC: “That’s a worrying statistic and it kind of alludes to a large number of organisations employing IT security professionals that evidently haven’t a clue what they’re doing. It doesn’t take a highly-paid CISO to be able to explain what an APT is and how modern malware has been specifically coded to evade the firewalls and anti-virus solutions that were put in fifteen years ago to defend against yesterday’s threat.”

Involving the board in discussions is a heated subject, and some urge caution in this regard. One CISO, who declined to be named, told SC recently: “Don’t talk about APTs (to the board) - you will get thrown out of the room.”

But William Buchanan, professor of computing at the HDe/School of Computing at Edinburgh Napier University, said that the cloud, encryption and new ZTB USB thumb drives show there’s always going to be ways hackers can exfiltrate data – and the board must understand that. “CEOs really need to wake up to the possibility of losing IP and brand reputation, and in an instant. This is not script kiddies anymore,” he said. Wallace agreed adding: “What boards need to wake up and realise is that the environment has changed. Cyber is a big problem and it’s here to stay.”

“There needs to be a senior member of the board who has an understanding [of cyber-security] and who will take responsibility.” However, Stru Freidhberg’s German believes that boards have been taking note, particularly when it comes to defensive measures. “One of the things that has really changed last year has been the move from prevention, which has essentially failed. Boards and non-IT executives realise the problem requires very senior attention.”

He admitted that some of those board members “may not know how to deal with [such attacks] and said that the nature of security is sometimes to blame. “The problem with bad IT security is that it’s self-enforcing...you congratulate yourself on how little you’ve been attacked.”

Getting the response right
Security experts agree that stopping an APT is unlikely – if attackers determined they will get in – but say that response, and preparation, are key are reducing the damage.

In particular, they urge improved network visibility, regular security assessments, hiring the right staff and getting board buy-in from the get-go. Others say that whitelisting should be essential – while a more radical idea has been suggested of developing a separate risk assessment for APTs.

Wallace argues that more advanced endpoint security is needed where important data is held in a digital “strong room” and protected by advanced anti-malware solutions. SIEM and big data analytics are “useful but they don’t stop the attacker – you’re never going to catch them using traditional mechanisms,” he says.

However, Buchanan counters and says that SIEM can give you the visibility of the traces of an attack – even if it has already happened: “The best thing is to set up logging infrastructure, log everything on the network – positive or negative.” He said that is SIEM better than big data security analytics because the human eye is better than an automated robot.

Buchanan added that companies must seek to provide more security training, produce better software internally and leverage end-to-end encryption across email, disk and applications.

Continual testing should also be carried out, with pen testing often not good enough and done on a tick-box basis. “Companies need to understand what is a recurring theme with a recent Lieberman Software study indicating that eight in ten information security professionals believe that the aforementioned perimeter technologies are not enough to defend against APTs.”

AAPT Roundtable
Speaking at the SC Magazine Roundtable – sponsored by Akamai Technologies - in central London last November, experts looked at the various definitions and appropriate defensive measures available and emphasised the need for continuous risk assessment and that the threat should be discussed at boardroom level.

James McKinley, head of information security of data protection and PCI DDS at Worldline at Atos, opened the discussion by questioning whether the ‘P in Persistence’ stood for persistent hackers coming back repeatedly or gaining a digital ‘foothold’ in an organisation, while others, including Quocico’s Bob Tarzey, noted the focus of any attack would be on the network – positive or negative.” He added that other industries should push defensive measures into the cloud, and some delegates questioned whether cyber-terrorism was likely, and asked why we had not seen it yet. Tony Morbin of SC Magazine noted how a Swedish hydroelectric plant manager attending the 4SICS conference in Stockholm had confirmed that his plant had been put out of operation for a day by a targeted virus attack.

Others argued that risk assessment should be continually monitored, with Lacey stating that an independent risk assessment should be required. Save The Children CISO Ray Evans said that these firms “be very careful when subcontracting, and getting them to provide an assurance that they have an understanding of risk in accord with your own.” This communication extends to the boardroom, says Tarzey, who said that messages about the nature of a risk and its potential consequences, and the preventative action and resources required to prevent it, should be described simply by the CISO to the CEO.

“You’re trying to describe it to the CEO, who doesn’t understand cyber-security, that this is a targeted attack,” said Tarzey.

Experts summarised that information security teams should benchmark best practice, be open and honest with C-level about their capabilities, and – where appropriate – outsource risk management and log management.

When looking at potential solutions, white-listing of approved apps, services and connections came highly recommended, with the ability to provide category approval overcoming some of the issues related to constant updates and patches at a large organisation. Constant monitoring of all network traffic in real time, establishing what was normal, and then reacting quickly to any abnormal activity was seen as key to closing down attacks.

Resources to tackle a 24 hour opponent, and the skills gap, trying to get the right staff at smaller enterprises was also an issue, with one delegate asking, “I just don’t have the time or the staff to thoroughly investigate all our log files - what should I do?”

Unsurprisingly, Colley suggested that the solution might well be to outsource to an or- signerisation that did have the resources in place, such as a cloud provider, and which would take the focus of any attack away from the target company.

On a straw poll, half of the delegates said that they would use or were using cloud services, and half did not feel confident about outsourcing to a cloud provider due to security concerns – or, in the case of smaller concerns, a perception that the cost may be too high.

For more information on SC Magazine’s Editorial Roundtable Series please go to www.scmagazineuk.com

Also tune in to SC’s APT e- Conference on 17 February 2015
Industry Innovators

These tools address the rash of large-scale attacks and can fend off those to come, says Peter Stephenson, technology editor

2014 was a very interesting year for Innovators. For one, there were fewer companies than in previous years. We attribute that to the efforts necessary to address the rash of large-scale attacks and the convergences taking place within the industry. Many of our former Innovators have innovated their way into mergers and acquisitions and in some cases disappeared from the security scene as discrete entities.

However, we had a bumper crop of 2014 Innovators and they are about as good as it gets. First, we have seen a reorganisation of the industry with ever-increasing emphasis placed on cloud computing. Our view of the cloud is that it is a business, not a technical construct. Still, from a technical perspective, what cloud computing translates to is “using someone else’s computer.” That has huge information security implications. With those implications comes a whole new emerging branch of our field to address this sort of remote control computing. Also, some traditional areas have merged into other areas and, while the shift is not yet quite complete, there has been an impact upon the product groupings with which we are familiar.

Some companies have shifted their emphasis to address new challenges. But, those folks did not start a whole new river…they simply redirected the course of the old one. The results may well prove spectacular over time. First, the major breaches we saw over the past couple of years are just getting started. We have made a significant paradigm shift in the last decade from the script kiddie/adventurer type of criminal hacker to the well-paid professional criminal. These bad guys may be cyber-mercenaries, crime-ware developers or freelance crackers. They are all in it for the money.

The other major paradigm shift is the entry of state-sponsored cyber-attacks. While today these are largely emblematic of economic warfare, the time is not far off where political motivations will take over from simple financial considerations. When that happens it will become a matter of semantics when we talk about cyber-crimewar and cyber-war. They will merge into a single paradigm, both using the same techniques and separated only by subtle differences in motivation.

That’s where our Innovators shine. If they are successful in forming the rules of engagement into something we can win, it will be the first time in the history of cyber-security that this has occurred. Looking at this group of Innovators we believe it entirely possible that within a year or two some of these will have innovated their ways into a winning hand at the cyber-war game.

Access control

Access control is a fairly broad category that includes identification, authentication and authorisation. These three areas need to be covered but with the growth of the enterprise and the blurring of the perimeter other considerations impinge on the simple act of controlling access to systems, data and applications.

Add to that, the challenge of provisioning huge numbers of users – many of whom are completely unknown, but important nonetheless – with access controls that work, are easy to use and effective, and you have a set of Herculean challenges. What is most important, however, is the strong emergence of access control as much of a business challenge as a technical one.

As we move the user closer to the application and, thus, the data, we find that business issues not only drive but complicate the mechanics of access control. Now we must determine who should access what and why. That is as it always has been to a point but now there is an added dimension of complexity brought on by widely dispersed locations, users at all levels (from employees to customers), access directly to applications without any firewall to inter-vene, and the need to protect critical and sensitive data while allowing this extremely granular access.

The answer – as is quite common now – is to move to the cloud. Access control and many other security functions, as we will see, may actually work best in a SaaS environment. Centralised control of a very decentralised process used to feel like an oxymoron, but with SaaS we can achieve it and manage it well. That is the type of innovation that 2014’s access control Innovator has brought to bear on a very tough challenge.

RSA Identity Management and Governance

In years past, this company was RSA Aereko and we liked it the first time we saw it. The differentiation is the approach it takes in managing identity. For RSA, identity and access management (IAM) is a matter of business, not just a matter of technology. Its rationale is that tech folks do not understand the underlying business model any better than the business folks understand the technology.

Deploying this rationale as a product is its second innovation. It may be the original “have it your way” IAM product. You can get IMG as software, a hardware appliance or an SaaS deployment. How do they do it? When we asked, the answer was that SaaS is all about standardisation. Once you get that under control, different delivery platforms become practical and, from the user perspective, whatever deployment they chose is the right one because it just works.

The access space is complicated. There are lots of people with lots of accounts – so creating a business view of access simplifies the complexity. IAM often makes use of business roles and the mappings for those roles can be complicated. As SaaS takes over, there are many other applications that do not understand all of the roles or that have their own special ones. So IMG uses attribute-based access control. The attribute has entitlements. One way to make this work cleanly is to use standard tokens and they can contain tokens that Active Directory can understand.

The addition of governance to the mix allows organisations to bring business processes, technology and training all together in a holistic package. All of this points to RSA’s key innovation: managing identity, recognising that it is the key threat vector across all platforms in the enterprise. When identity is compromised the enterprise and all it contains is compromised.

AT A GLANCE

VENDOR: RSA, the security division of EMC
eMC.com
FLAGSHIP PRODUCT: RSA Identity Management and Governance
COST: Varies widely depending upon implementation
INNOVATION: Managing identity as a key threat vector across the entire enterprise
GREATEST STRENGTH: RSA has re-written the book on identity management making it far broader than traditional models allowing greater security, control and ease of deployment.
Virtualisation & cloud security

“...security management must address the challenges of the virtual environment...”

HyTrust

While HyTrust is not new to the Innovators section, it brings back a whole suite of new innovations this year. HyTrust looked at the new trends of cloud-based datacentre virtualisation and realised that there was a tremendous need for security mechanisms to complement virtualised infrastructures. HyTrust locks down the hypervisor and lets administrators control exactly who has different levels of access to administrative functions.

New for this year are even more virtualisation security features as well as robust logging. For the security features, HyTrust has introduced VM encryption. Encryption can be centrally managed from HyTrust, which can also handle key management. For organisations undergoing regulatory compliance, this is a massive plus because administrators can quickly and easily re-key any virtual machine without ever leaving their desk. Another new feature is virtual machine boundaries. This adds an element of early warning.

AT A GLANCE

VENDOR: HyTrust
hytrust.com

FLAGSHIP PRODUCT: HyTrust CloudControl v4.0 and HyTrust DataControl v2.6

COST: Cloud control: starts at £40,800 for a single data center site with 20 ESXi CPU sockets; Data control: for 100-1000 VMs, the cost would be £28,962 per year, which includes high redundancy for up to eight clustered key management virtual appliances.

INNOVATION: Virtual cloud-based datacenter security.

GREATEST STRENGTH: Innovative product that provides robust security to the cloud-based software datacentre.

Intigua

When we asked the folks at Intigua what they do, their reply was, “Intigua Virtual Management Platform virtualises existing management tools using proprietary container technology to encapsulate them in their entirety, and enables them to be centrally managed and automated via a robust policy engine.” That is a mouthful.

We’ve heard from these folks before, though, and they have proved their capability to our complete satisfaction.

First, the product is a virtual management platform and that is important because it can sit on the virtual system and communicate directly with the systems it needs to manage. It also containerises management tools so that they can be managed centrally giving a side benefit of policy-based control. The control extends to most industry-leading management tools.

Analysis consists of both event and flow analysis. Correlating this information allows MetaFlows to avoid false positives while not missing important alerts. Also, the correlation creates powerful new heuristics that can be used across the user base. This approach is unique and indicative of the company’s creativity and innovation.

The whole approach that the company takes is that perimeter defence is no longer enough, in fact, may not even be relevant. To protect the enterprise the focus must be on assets analysed using behavioural analysis. Using multi-session analysis, patterns emerge allowing a more complete defence than traditional perimeter tools.

This Innovator continues to blaze the trail for perimeter defence in an environment increasingly consisting of less and less perimeter to defend. MetaFlows has brought creativity and insight to the solution with one of the most positive uses of cloud for security purposes that we have seen in quite a while.

AT A GLANCE

VENDOR: Intigua
intigua.com

FLAGSHIP PRODUCT: Intigua Virtual Management Platform

COST: Starts at an annual subscription price of £32K.

INNOVATION: Containerisation of the complete management stack in a virtual environment.

GREATEST STRENGTH: Ability to seamlessly and effectively manage a hybrid/virtual environment that includes legacy management tools.

MetaFlows

The idea behind the MetaFlows model is that all of the security analysis is done in the cloud where a greater level of support is available. Taking advantage of aggregating responses from their large customer base, MetaFlows can disseminate the results of analysis to all customers.

This adds an element of early warning. Agents on the enterprise allow the cloud-based system to provide IDS/IPS as well as SIEM services. On the malware side, communication with ViruTotal is automatic and there is a new correlation engine rule API that keeps track of multiple sessions and creates incident reports as necessary. The new wrinkle here is that this all is based on a meta-description of the event being analysed and reported.

Analysis consists of both event and flow analysis. Correlating this information allows MetaFlows to avoid false positives while not missing important alerts. Also, the correlation creates powerful new heuristics that can be used across the user base. This approach is unique and indicative of the company’s creativity and innovation.

The whole approach that the company takes is that perimeter defence is no longer enough, in fact, may not even be relevant. To protect the enterprise the focus must be on assets analysed using behavioural analysis. Using multi-session analysis, patterns emerge allowing a more complete defence than traditional perimeter tools.

This Innovator continues to blaze the trail for perimeter defence in an environment increasingly consisting of less and less perimeter to defend. MetaFlows has brought creativity and insight to the solution with one of the most positive uses of cloud for security purposes that we have seen in quite a while.

AT A GLANCE

VENDOR: MetaFlows
metaflows.com

FLAGSHIP PRODUCT: MetaFlows Security System (MSS)

COST: Small enterprise: £1,790/year; corporation/university: £6,864-plus/year.

INNOVATION: Combination of one-on premise sensors and cloud analysis taking advantage of global intelligence.

GREATEST STRENGTH: They still pride themselves on listening to their customers and imagining the future beyond what the customers tell them.
Barrier1

This is another one of those very cool products that is based on sophisticated mathematical algorithms. The product works and it works exactly as advertised if not a bit better. We really like the notion of under-promising and over-delivering. That’s just Barrier1’s style though, and after a while we got used to it.

We first met this tool up close and personal – not just in the review lab – when we installed one in our centre for Advanced Computing and Digital Forensics. We did not install it to protect us – we installed it to gather data for analysis. Recently we had visitors to the lab and showed them the countries that had been knocking on our doors since we installed the Barrier1. Even we were surprised at the probes and potential attacks that the product had fended off.

Here are the reasons that this tool works so well – beyond the algorithms, of course. First it is at a significant advantage over other similar products due to its modularity. It is designed from the ground up to grow. The second advantage is its sensoring technology. We often have said that you can’t find the answers until you know the questions. In this product it is the sensoring that allows you to grasp the questions fully so that the sophisticated analysis capability can take over and provide the answers.

Barrier1 is a seven-layer device. It sees and analyses traffic on all seven OSI layers. Because of that it is hugely flexible. One of the objectives for the Barrier1 folks over the next year is to develop defences for specialised attacks peculiar to those markets. That suggests looking at such things as industrial control systems. We’ll just have to wait to see what this.

Innovator has up its sleeve for the next bigger challenge. They are looking at more sophisticated tools. They will have the pulse of the industry and continue to rise with newer and better analytics.

EyeLock

When we first met EyeLock it made some pretty wild claims. The big one was that it could spot people at a distance using iris-based biometric scans. The people could be in motion. Imagine picking out individuals passing through security at an airport or gambling at a Las Vegas casino.

Now, consider that deployment of this device – actually quite small – was industry compatible, requiring nothing particularly special. In fact, it could replace your existing card swipe system without a lot of trouble. Add that it is priced attractively and what else could you want?

Well, let’s start with physical access control. Can it do that? Yep. No problem. OK, we want this for our computers. We travel a lot and it would be nice to know that our system was secure from malware, phishing, etc., because it knows who we are. We want this capability to be able to be embedded in the Internet of Things.

Well, that was the latest innovation from this vendor.

The newest addition to their stable of tools is a device that is simply a USB device. It is a simple USB-powered peripheral called Myris that secures my PC just by plugging into it. That’s all there is to it. We can’t wait to make this part of our inventory of gadgets. It is truly useful in helping secure our computers and it is priced attractively.

First, they settled on a reliable method of biometric identification and authentication. Then they stepped back and considered how it could be used. Finally, without worrying about which products would be cool – and all of theirs are – they were more concerned with what problems needed to be solved. That’s the road to innovation.

Cellebrite

These guys pretty much control the mobile device forensic market. And it really is no wonder given the depth and breadth of their offerings. Here is a case where innovation, creativity and imagination all converge to provide a solid platform for some task. In this case, the task is understanding, forensically, the contents of a mobile device.

That sounds pretty straightforward, but in reality it is not so simple. There are thousands of different mobile devices. Two devices of the same type from the same manufacturer might still be different. As well, there are knock-off chipsets from China and other countries that don’t behave forensically exactly as one would expect. Finally, there is the need to acquire forensic data from multiple devices and, perhaps, with forensic data from a computer.

Cellebrite accomplishes all of this. We have been using Cellebrite tools in the SC Lab for more than three years and we are continuously amazed at their efficacy.

The big news over the past year, though, involved improving the utility of the tools. For example, you now can see an extraction immediately as it is done. JTAG decoding is now available and you can take screen shots of the phone while it is connected and they become part of the forensic report. Also, in link analysis the tool integrates with IBM’s i2 link analyser, the workhorse of link analysis. That means that just about anything that can be characterised using link analysis is fodder for the Cellebrite tools. It really doesn’t get much better than that if you are struggling with cases involving mobile devices.

ForeScout Technologies

The CounterACT appliance – software or hardware – is really a lot more than a simple security appliance. It is a platform for innovation. The ForeScout folks have created this platform based on customer use cases and they never have stopped listening to their customers.

They have the pulse of the market as well as just about any company in the security space that we have seen.

The key is the platform. With a platform that is flexible and has the ability to morph over time to meet new challenges, the company is free to listen to customers and innovate solutions to those tough challenges. An example is CounterACT's ability to work with the market to provide a comprehensive collection of tools that covers the full range of mobile device forensic needs.

What is on the horizon, thus? The natural evolution of the product suggests that at some point these use cases could be most effectively solved by the users themselves. They envision a sort of app store that integrators could use to add applications to the platform. Along with the solutions to use cases there are bound to be other customers who need the same solutions. It’s sort of like having an app store that supports Android devices. The devices are the platform and the applications satisfy the customers’ use cases. Now that’s innovation!
New Year resolution I: A cyber-security health check

Its important to identify the whole picture of risk

A new year resolution is important. The most important task is identifying where your assets are and how you can protect them.

Ensuring you know where all sensitive data is being held is a thorough stock take should assess how far your data has spread and onto what devices. This exercise can often uncover potentially sensitive data on devices where you simply weren't expecting it to be.

Evaluate processes
As threat levels grow, every team should have a plan which covers the key phases for incident Response, from planning, protection, detection, triage and response. Plans are great in theory, however, in this way that we'd carry out regular fire drills, teams should stress-test and refine response plans regularly. Only then can you really know how well equipped you are to detect, contain and remediate any threat. Drills should be tested based on different kinds of incidents through different threat vectors and should be organisation-wide; from C-level to HR and PR.

Know the enterprise
Assess if you really know what is happening across the enterprise, across every type of device, from smartphones to tablets and smartwatches - any device with an OS and internet connection. You need to baseline ‘normal’ behaviour at endpoints to identify any changes which suggest a compromise and investigate them.

Address staff training
Building a talented team with the skill-sets to manage and respond to cyber-threats is important, but so is keeping your team engaged and motivated by reviewing training and skills. A KPMG poll says nearly three-quarters of senior IT and human resources professionals report facing new cyber-security challenges which demand new cyber-skills.

Factoring in time for mentorship, study, or outside training is key for employees, for their own job satisfaction and the added value this brings to the team. This could be one of the most important strategies to ensure you hold on to talented staff.

It’s also important to have an ‘HR’ continuity plan to deal with security skills gaps should anyone in the team leave. Is there documentation in place to cover processes and systems so that a new entrant could quickly get up to speed?

Enforce security
Ensure all staff are aware of policies and their role in keeping the company’s systems secure. Even with the most robust security tools in place, plans can fall down if we haven’t educated end-users on their own ‘cyber-hygiene’. Phishing attacks and other ‘low-effort’ methods are still proving lucrative for cyber-criminals, so review all processes from practical measures such as reminders to employees about browser usage, attachments, and password choices, to more strategic plans to encourage security practices across the organisation. Being in support from the highest levels so that the importance of security is communicated from the top and work with executives across other departments to build concrete plans.

Nick Pollard is senior director of professional services at Guidance Software.

For more information on these and many other information security opportunities, please contact:
Mark Amplaford
mark@barclaysimpson.com
Oswatte Bestman
ob@barclaysimpson.com
Harish Parmar
harish@barclaysimpson.com
Chris Meager
chris@barclaysimpson.com
Oxanae Dale
ol@barclaysimpson.com
Sam Freedman
samf@barclaysimpson.com

Barclay Simpson, Bridwell Gate, 9 Bridwell Place, London EC4V 6AW
www.barclaysimpson.com
Cost effective Security and Risk Solutions

We provide high quality security and risk consulting solutions at affordable prices. We provide access to an established network of industry-proven consultants. Whatever your needs, Bridewell is able to respond quickly and efficiently.

We offer services in Information Security, Cyber Security, IT Risk, Security Testing and Data Privacy.

Tel no: 01189 255 084
Email: bc@bridewellconsulting.com
Web: www.bridewellconsulting.com