CYBER SECURITY PREDICTIONS FOR 2018

Brian Chappell *outlines security considerations for the year ahead*

Picture credit: Getty

The cyber security threat is expected to continue to grow in 2018

THE BIGGER THEY ARE, THE HARDER THEY FALL

If we think the headlines shocked us with Equifax, SEC, and NSA – we will very quickly discover that large organisations have poor cyber security hygiene, are not meeting regulations and are failing to enforce the policies they developed, recommend and enforce upon others. The news over the coming 12 months will have even more high-profile names and the root causes will be just as shocking as the OMB breach.

INCREASE IN MOBILE PHONE SPAM

With there being more mobile phones in most countries than there are citizens in those countries, mobile phone spam will see a significant rise by 10,000 percent due to automated spam and dialling 'botnets' that essentially render most handsets unusable because they receive so many phone calls from unidentified numbers. This rise in phone spam pushes cellular carriers to start to require that end users adopt an "opt in" policy so only those in their contacts can call them.

MAJOR HEALTHCARE BREACH RELEASES DIRECT MEDICAL HISTORY OF CELEBRITIES

Here's a salacious one for you. Direct attacks on celebrities will continue in order to "one up" the competition with leaks of celebrity information. Healthcare records will be stolen that indicate celebrity plastic surgery, pregnancies and full disease history, causing the total downfall of some and the rise of others.

MAJOR INCREASE IN 'GAMING DELETEWARE' INFECTIONS

'Gaming deleteware' infections across most major platforms will increase as botnets continuously attack gaming networks and devices such as Steam, Xbox, PlayStation and Nintendo systems with the sole intention of rendering the machine inoperable. The malware is downloaded as an embedded game add-on, causing millions of devices to need to be replaced.

THE FIRST MAJOR APPLE IOS VIRUS HITS WITHIN A POPULAR "FREE" GAME

As users click on the 'ad' to play a game for free, their iOS11 device will be compromised, leaking all data stored in the local Safari password storage vault.

CONTINUED GROWTH IN THE USE OF RANSOMWARE AND CYBER-EXTORTION TOOLS

2017 has proven the model that vulnerabilities nearly 20 years old are being exploited in organisational networks (Verizon DBIR 2017), so the opportunity is too great and too easy for organised crime to ignore. Further, the commoditisation of these tools on the Deep Web opens the door to anyone who feels the risk is worth the reward. This is likely to continue until organisations get the basics right and the risk/reward balance tips making ransomware far less appealing.

MORE END-USER TARGETING

Penetration through unpatched servers like in the case of Equifax will happen, but hackers will continue to target end users with more sophisticated phishing and targeted malware taking advantage of unpatched desktops where clients have far too many privileges. Again, don't take your eyes of the end users.

BIOMETRIC HACKING WILL TAKE FRONT AND CENTRE

Attacks and research against biometric technology in Microsoft Hello, Surface Laptops, Samsung Galaxy Note, and Apple iPhone X will be the highest prize targets for researchers and hackers. The results will prove that these new technologies are just as susceptible to compromise as touch ID sensors, passcodes, and passwords.

CYBER RECYCLING

As we see a rise in the adoption of the latest and greatest device, we will see devices and now IoT, be cyber recycled. These devices, including mobile phones, won't be destroyed, however. They will be wiped, refurbished, and resold within the US and overseas even though they are EOL (end of life). Look for geographic attacks against these devices to rise since they are out of maintenance.

MORE MONEY FOR SECURITY, BUT THE BASICS STILL WON'T BE COVERED

Organisations will continue to increase spending on security and new solutions, but will struggle to keep up with basic security hygiene such as patching. Hackers will continue to penetrate environments leveraging known vulnerabilities where patches have existed for quite some time. Regardless of whether it is an employee mistake, lack of resources, or operational priorities, we are sure to see this theme highlighted in the next Verizon Breach report.

IAM AND PRIVILEGE MANAGEMENT GOING HAND-IN-HAND

IAM and privilege management adoption as a required security layer will continue. We will see more security vendors adding identity context to their product lines. Identity context in NAC and micro-segmentation technologies will increase as organisations invest in technologies to minimise breach impact.

ACCEPTANCE THAT "COMPLETELY SAFE" IS UNOBTAINABLE

As 2018 progresses and more and more organisations accept that breaches are inevitable, there will be a shift toward containing the breach rather than trying to prevent it. This doesn't mean abandoning the wall, but rather accepting that it isn't perfect, can never be and shifting appropriate focus toward limiting the impact of the breach. Organisations will refocus on the basics of cyber security best practice to enable them to build effective solutions that impede hackers without impacting legitimate users.

CHAOS ERUPTS AS THE GDPR GRACE PERIOD ENDS

As organisations enter 2018 and realise the size of the task to become GDPR compliant by 25 May, there will be a lot of panic. This legislation seems poorly understood, which has led to many organisations tabling it for 'later' and, for many, they will wait until the first prosecution is underway before they react. The EU gave over two years after GDPR passed into

▶

law (27 April 2016) for organisations to become GDPR compliant, there is likely to be little tolerance for non-compliant organisations which are breached after 25 May and, more than likely, some example setting. Those that complete their GDPR compliance ahead of the deadline will be right to feel smug as they watch their competitors flail.

THE US LAUNCHES A CYBER ATTACK AGAINST AN ENEMY

Bombshell! Following announcements by US President Donald Trump to "Wait and see" how the US will handle foreign enemies, the US will launch a coordinated cyber attack on Iran and North Korea rather than sending in physical troops. This "act of war" will be launched pre-emptively as the first public internet attack from a first-world nation, and will cause the near total destruction of internet resources in these countries.

INCREASED AUTOMATION IN CYBER SECURITY RESPONSE

The size of the cyber security threat continues to grow through 2018, with increasing numbers of attack vectors combined with increased incidence of attacks via each vector (driven by commoditisation of attack tools) leading to massive increases in the volume of data being processed by cyber security teams. This demands improvement in the automation of responses in cyber security tools to do much of the heavy lifting, thereby freeing the cyber teams to focus both on the high-risk threats identified and in planning effectively for improvements in defences. Increased use of machine-learning technologies and, from that, more positive outcomes will lead to a significant growth in this area.

GREATER CLOUD SECURITY INVESTMENTS

Vendors will begin to invest more heavily to protect cloud-specific deployments for customers migrating to the cloud. Supporting docker/containers, DevOps use cases and enforcing secure cloud configurations are some initiatives that will be driven by customers.

RICHER CYBER SECURITY VISION

As organisations' needs for more comprehensive cyber security solutions grows, so will the need for effective integration between the vendors of those technologies. This will lead to more technology partnerships in the near-term and to industry standards for integration in the longer term. The ability for systems to work with relatively unstructured data will allow for more effective information interchange and, as a result, far richer and more rewarding views across our cyber landscapes.

IT IS NOW LAW

Governments will begin passing legislation around cyber security and the basic management of IoT devices required for safe and secure computing ●

Brian Chappell is Senior Director, Enterprise & Solution Architecture at BeyondTrust. His role ensures the delivery of world-class solutions built around BeyondTrust's leading vulnerability management and privilege management platform. He is a regular speaker at industry conferences as well as a regular contributor for the press. He focuses on guidance and opinion pieces helping organisations on their journey toward best practice.

Ransomware and extortion look set to continue to be popular

Picture credit: Getty