bsi.

...making excellence a habit.™

Emerging trends in the cyber landscape

2018

BSI Cybersecurity and Information Resilience has begun to take a look at the emerging trends across the cybersecurity landscape for 2018 and what we can expect to see. With 2018 upon us, already two critical vulnerabilities have been uncovered, dubbed “Meltdown and Spectre” which are broad in scope, potentially affecting nearly every computer and device with a modern processor. It poses a particularly high risk to public cloud service providers and its customers. It has left every major vendor scrambling to develop a patch in order to plug the information disclosure vulnerabilities. This is already evidence that we are potentially in for a bumper 2018.

It is of course impossible to predict the future; planning for the unpredictable can be extremely challenging. However, with the rate of change of technology leading to increased innovation accompanied by advancing threats, we can’t afford not to plan and prepare our defences.

Based on research and real-time feedback from our experts, these are the following trends currently predicted which will affect the cyber landscape over the next 12 months.

Advanced malware

Over the past few years malware has been the top threat across the cyberthreat landscape; 2018 will be no different. A new wave of malware attacks known as fileless malware is gaining popularity by cyberattackers and we’re likely to see an increase in this type of method in 2018 as the attack allows a hacker to remain undetected in a breached environment for extended periods. Fileless malware attacks do not install malware files on a victim’s system in order to execute an attack. They use existing tools installed on computers or execute malicious scripts via Windows PowerShell and are typically hidden in the Windows Management Implementation (WMI) and/or system registry. For this reason, it makes it very difficult for traditional signature based end-point protection software to identify and block the threat. These types of attacks are typically launched by delivery of phishing links via email social engineering methods or by clicking on malicious links on suspect websites.

In order to mitigate the likelihood of these types of attacks, organizations must ensure that all systems are up to date and protected as well as providing adequate user awareness training in order to help staff identify and avoid those social engineering based attacks that allow such malware to enter an organizations’ systems.

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

Ransomware

In 2017, we witnessed a proliferation of ransomware attacks where cyber criminals digitally extorted and coerced their victims into paying a ransom in the form of a cryptocurrency before providing the decryption keys in order for victims to decrypt and retrieve their data. These types of ransomware attacks all begin by deploying the ransomware payload in a form of malware to their victims, most frequently via email and social engineering channels (and to a lesser extent via drive-by download or compromise of otherwise legitimate installation programmes). In 2018, we expect to see a continuation of these types of attacks which will continuously disrupt organizations with the attackers setting their sights on large organizations where they are able to cause the most damage, potentially leading to bigger monetary gains. We also expect to see a change in the ransomware variants – as noted above – where attackers begin adopting fileless delivery in order to circumvent the traditional signature end-point protection mechanisms.

Internet of Things (IoT)

In 2017, we witnessed massive Distributed Denial of Service (DDoS) attacks which leveraged millions of compromised IoT devices. This was possible as historically IoT devices have been found to exhibit inherently weak security settings, particularly in the home user space. As more and more of these devices come online in an interconnected world, we expect hackers to begin further leveraging these devices to deliver large-scale botnet attacks. Furthermore, an increase in compromised IoT devices may in the future force governments to step in and begin regulating IoT security on manufacturers.

Hackers will also begin hijacking IoT devices for their personal gain, leveraging audio, video and other available services these devices offer. We may even begin seeing persistent attacks on home devices with hackers creating backdoors, gaining access to home networks and potentially holding these, often expensive, devices to ransom.

Artificial Intelligence (AI) - Defence versus attack

Over the last few months there have been many vendors selling their end-point protection systems, Intrusion Detection Systems (IDS) or similar software suites which boast AI or Machine Learning (ML) capabilities as an effective defence mechanism. Historically, the main focus in AI has been on prevention and detection systems, however, 2018 may just be the year where we see threat actors become more advanced and begin using AI type attacks to rapidly identify zero-day exploits as well as to explore and exploit their victims' networks, post the initial intrusion. Machine learning protection mechanisms can be seen as an effective defensive tool, however, one should not solely rely on one defensive tool; rather, organizations should adopt a multi-layered in depth defence approach.

Increased regulations

2018 will see organizations needing to prepare for the looming deadlines of the General Data Protection Regulation (GDPR), Payment Services Directive (PSD2) and the Directive on Security of Network and Information Systems (NIS Directive) for EU member states. These regulations will affect many organisations across the globe, not just those within the European Union.

GDPR

The regulation requires businesses to protect the privacy and personal data of EU residents, regardless of whether the company is incorporated in any of the EU member states; if a global organization is targeting and collecting personal data of EU citizens, they will need to comply with the strict rules of the regulation by 25 May 2018. Non-compliance to the GDPR comes with steep penalties, with companies being faced with fines of up to €20 million or 4 percent of global annual turnover. Various types of Personal Identifiable Information (PII) that will need to be protected are basic identifiers such as name, email and physical addresses, social security and ID numbers including geolocation information such as IP addresses and cookie data. Additional special categories of PII have been clarified which relate to biometric data, genetic and health data, political opinions, racial data as well as sexual orientation.

The compliance requirements will put pressure on existing security teams as new expectations are set on them in order to protect the information by providing an 'adequate level of data protection'. However, the drive to be compliant is being supported by senior management and accompanied by an increase in security budget spending which is a positive step in the fight against cybercrime.

PSD2

Is an enhancement to the current PSD which aims to standardize, improve integration and payment efficiency, promote innovation and emerging payment technologies, reduced costs, offer better consumer protection as well as improve the security of payment processing in the European Union.

The regulatory requirements for financial institutions offering account-based payment services, in accordance with article 109 of the new Directive, states that those financial institutions already authorized to continue to operate as financial and payment institutions, shall submit, to the regulatory bodies, a report certifying that certain conditions set out and are met by 13 July 2018.

PSD2 will bring new and innovative features such as allowing retailers to 'ask' consumers for permission to use their bank account details in order to streamline the payment and checkout process.

With new features, new risks are identified. As more sensitive information is now being shared with retailers and other service providers, this leads to an increase in third party risk and an increased focus now needs to be maintained to monitor third party risks. However, PSD2 will also bring enhanced security features to the table such as a strong two factor authentication system and better consumer protection against fraud.

Call: +44 345 222 1711 /+353 1 210 1711 Email: cyber@bsigroup.com Visit: bsigroup.com

NIS Directive

This is the first cybersecurity legislation passed by the European Union (EU). Its objective is to achieve a high common standard of network and information security across all member states within the EU. The Directive was published on 19 July 2016 and member states have 21 months to transpose the directive in their own national laws with a further six months to identify which companies will be subjected to the NIS Directive; making the deadline November 2018. Organizations identified as Operators of Essential Services (OES) and Digital Service Providers (DSPs) will be subject to the NIS Directive.

Operators of Essential Services are referred to in the legislation as any entity that fulfils any of the following criteria:

- provides a service which is essential for the maintenance of critical societal and/or economic activities
- the provision of that service depends on network and information systems
- an incident affecting those systems would have significant disruptive effects on the provision of that service

As for Digital Service Providers, there are three types of DSP's covered under the directive, other than essential services:

- online marketplaces
- online search engines
- cloud computing services

The requirements are designed to improve cross-border cooperation in network and information security as well as foster a culture of risk management. A huge effort is going to be required from organizations and information security teams in order to meet the various applicable regulations. Aligning and adhering to these regulations will not only ensure compliance and avoid potential fines from regulatory bodies; but also allow organizations to bolster their cybersecurity capabilities, protect critical assets and improve business resilience.

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com

bsi.