Computing Security

Secure systems, secure data, secure people, secure business

FORWARD FEATURES 2017

(This list is subject to change)

JAN-FEB 2017

I.T. FRAUD

Fraud, theft and abuse detection and prevention have become a big data challenge, especially as businesses move increasingly online. Patterns of internal or external fraud often lie in the massive amounts of unstructured machine data and log files generated by business applications and systems. Fraud detection— real-time (or near-time) correlation searches or anomaly detection can identify and alert on fraud as it happens, enabling organisations to take the necessary action to prevent the fraud before it adversely affects the business. But how exactly should you do that? What are your options – and how effective are they likely to be?

WHAT DOES 2017 HOLD IN STORE FOR YOU?

What will be the big security issues in 2017 and are you ready to deal with them? From cybercrime to BYOD; from insider threats to compliance; from identity theft, cloud and beyond, one thing is certain: the rate, intensity and sophistication of attacks and the need to be fully protected against these will only increase. We ask some of the industry's leading experts to predict what will be the biggest concerns for end users in the 12 months ahead.

PERIMETER DEFENCE/INTRUSION DETECTION

An intrusion detection system (IDS) monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). Some IDS can respond to detected intrusions – ie, intrusion prevention systems. What should an organisation look for when evaluating this technology and is it the 'be all and end all' to their security problems or just one link in building a failsafe chain?

NB: The absolute deadline for all submissions - copy and images - is 9 January 2017

MARCH-APRIL 2017

HUMAN ERROR/RISK

External attackers prey on human weakness to lure insiders within organisations to unwittingly provide them with access to sensitive information. Another common human error includes the use of default usernames/passwords or easy-to-guess passwords. The strength of your business security profile is only as strong as the passwords your users choose – something that any organisation must recognise and enforce. How can your organisation be kept safe? What authentication controls should be put in place?

ANTI-MALWARE

Malware damage can range from loss of files to total loss of security -- even outright identity theft Understanding the major types of malware can help you make informed decisions about acquiring tools to protect your computer. To prevent infection from any of these threats, having up-to-date antivirus software and ensuring your firewall is enabled on your computer are musts, as is installing the latest updates for all of your installed software – while always keeping your operating system current. But is that enough?

IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times… for the right reasons. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives. But what is the best way to implement the solution that fits the business?

INTERNET OF THINGS/EVERYTHING

The Internet of Things (IoT) delivers many benefits and advantages, and is to be embraced and welcomed. However, when machines start collecting data, privacy and security become an issue and can be seriously compromised. Estimates vary as to how many devices are currently collecting data and connected to the internet. One recent study suggests 13 billion – and that number is expected to nearly double within five years. How do you enjoy the pluses that IoT offers, while safeguarding your organisation?

NB: The absolute deadline for all submissions - copy and images - is 13 February 2017

MAY/JUNE – INFOSEC ISSUE

I.T. ASSET DISPOSAL

With the EU parliament's new European General Data Protection Regulations (GDPR) due to become law in all 28 EU countries by early 2018, many businesses will need to look closely at how they protect their data throughout its lifecycle. Even the UK, post-Brexit (voting wise, at least), must comply. In addition, any business that stores data on EU citizens will become subject to this law. This has the potential to affect a broad spectrum of both EU and international companies. But exactly how will this affect business? With the potential for huge fines (up to 4% of global turnover) will this see companies becoming more mature in their attitudes towards data protection and, if so, what methods will they adopt to achieve regulatory compliance?

MOBILE SECURITY/BYOD/DEVICE MANAGEMENT

A new report, 'On the Radar', from leading research company Ovum shines a light on the extent of the mobile security problem affecting businesses of every size around the globe. It exposes "the inadequate level of mobile device protection offered by most mainstream endpoint security providers who have failed to keep pace with market requirements and the subsequent threat this has created for businesses who are unwittingly exposed to cybercriminals". With mobile devices now in their multi-billions globally, more and more applications are flooding the market. That has made mobile monitoring and device management an imperative. But how exactly? *Computing Security* finds out.

ENCRYPTION

Encryption plays a vital role in ensuring an organisation's activities run smoothly, protecting their valuable information from potentially being stolen or altered. At the same time, encryption can be used by enemies just as readily. How do you stay one step ahead of the attackers, when it comes to employing the latest encryption technology? What is the right solution for your organisation? How do you make sure your systems aren't breached? In the wake of constant breaches, the time to focus on encryption has never been more urgent.

EMAIL/MESSAGING SECURITY

Email is built into almost everything – from phones and tablets to traditional computers to gaming devices, to your car. And yet email was not designed with any privacy or security in mind, making it highly vulnerable to attackers out to infiltrate your systems. So, what is the best way to protect your organisation's communications? How do you keep your data vital and easily accessible to you and yours, yet useless to anyone out to access/steal it? We ask the experts for their thoughts.

NB: The absolute deadline for all submissions - copy and images - is 10 April 2017

JULY/AUGUST

GOVERNANCE, RISK AND COMPLIANCE (GRC)

GRC is vitally important, especially as more and more legislation is introduced that could have grave consequences for any enterprise that flouts its rules. What are the key steps that any business needs to take to counteract the growing risks they are exposed to and avoid being in breach of legislation? What pitfalls should they be aware of that can surface along the way? And how do you balance all of these ‘musts’, so they align in such a way as to bring greatest benefit to the business?

DATA LOSS PREVENTION (DLP)

Sensitive information is increasingly leaving the safety of your corporate network as more employees share files over consumer cloud storage services and access those files on their own mobile devices. The number of targeted cyber-attacks is soaring, as cybercriminals develop effective new methods for defeating traditional security measures and stealing corporate information. So how do you manage and protect your information in this challenging environment? And what does a complete, successful data protection strategy look like, in the face of eroding security perimeters, increasing targeted attacks, and evolving user habits and expectations? We investigate.

PREDICTIVE ANALYTICS/SECURITY ANALYTICS

Predictive analytics is the use of data, statistical algorithms and machine-learning techniques to identify the likelihood of future outcomes, based on historical data. The goal is to go beyond descriptive statistics and reporting on what has happened to providing a best assessment on what will happen in the future. That streamlines decision-making and produces new insights that lead to better outcomes. But what route should an organisation take when implementing this strategy? Where do you start and who should be involved in the process?

CLOUD SECURITY

With the growth in data breaches and the potential financial penalties and loss of reputation for companies that fall victim, moving your private data to an external provider is more daunting than ever. A well-established cloud computing vendor will ensure they have the latest sophisticated security systems in place to defend against the threats any business might face. But how does any organisation know which vendor to entrust its priceless data to? What are the criteria they should use to establish the credentials of those that come courting you? And how do they spot the ones that will most likely fail them?

NB: The absolute deadline for all submissions - copy and images - is 23 May 2017

SEPTEMBER/OCTOBER

I.T. SECURITY TRAINING

Protecting your company online begins with ensuring your employees are prepared to assist in keeping your computers and networks safe. The best security technology in the world can't help you, unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks. But what should those practices and policies be? Who should be responsible for making that decision and how should employees be monitored to ensure they are adhering?

MANAGED SECURITY SERVICES

Many organisations turn to managed security services providers to deliver the expertise, knowledge and infrastructure they need to secure them from Internet attacks. The message is that not only do they have the superior expertise, but also that this can be done at a fraction of the cost of in-house security resources. How true is this? Or should a business rely on its own internal resources, thus ensuring much tighter personal control over their crucial IT assets? Alternatively, if an MSP promises better operational, financial and strategic efficiencies across an enterprise, how might they be asked to prove that?

SIEM

Security information and event management (SIEM) delivers greater intelligence and automation into the collection, correlation and analysis of log and alert data. And that should allow security analysts to focus on what is most important. SIEM is all about improving efficiency by enhancing the ability to deal with the soaring amount of data generated by network and security devices; or being able to detect an attack designed to elude a firewall or IPS. Even making reporting and documentation (for compliance purposes) more efficient. But how do you justify the cost of investing in SIEM to those who control the purse strings within your organisation? What are the compelling arguments? And what is the likely ROI?

TARGETED THREATS

A targeted attack seeks to breach the security measures of a specific individual or organisation. Usually the initial attack, conducted to gain access to a computer or network, is followed by a further exploit designed to cause harm or, more frequently, steal data. Future attacks could be focused increasingly on the modifying of data. Analysing the stages of an attack can provide insight into the tools, tactics and procedures of the attackers. This helps indicate whether an attack can be linked to a broader campaign and is key to building the intelligence that can be used to inform incident response procedures and mitigate future advances. We investigate how businesses can keep themselves safe from such assaults.

NB: The absolute deadline for all submissions - copy and images - is 25 July 2017

NOVEMBER/DECEMBER

CYBERCRIME

Regulators should be given significant beefed-up powers to tackle the escalating problem of online fraud in the wake of the cyber attack that compromised the security of millions of TalkTalk customers at the tail-end of last year. That has been one call from IT experts to emerge. But is that putting the cart before the horse? What should organisations be doing to prevent such attacks in the first place? And is TalkTalk CEO Dido Harding being defeatist when she says that it is not reasonable to expect such attacks not to happen again? Or is that the new reality in a world where the attackers seem to be gaining the upper hand?

APPLICATION SECURITY

Application security plays a pivotal role – through the use of software, hardware and procedural methods – in protecting applications from external threats. Security is becoming an increasingly important concern during development, as applications become more frequently accessible over networks and therefore vulnerable o many fronts. What security measures should be built into any applications as standard, if they are to be safe to use? And what application security routines will best minimise the likelihood that unauthorised code can manipulate applications to access, steal, modify or delete sensitive data?

ADVANCED PERSISTENT THREATS (APT)

An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection and harvest valuable information over the long term. According to the '2015 Advanced Persistent Threat Awareness' study conducted by independent global association ISACA, of those who took part:

- 74% think they will be a target; 94% believe they are at least somewhat familiar with APTs; 28% have been subject to an attack; and 67% believe they are ready to respond.

What can organisations who expect to be a target do about an APT? And how sure can anyone really be that they are ready to respond? We ask the experts how APTs are evolving and whether it is possible to keep out the more determined assailants.

NB: The absolute deadline for all submissions - copy and images - is 17 October 2017

GUIDELINES – THESE APPLY TO ALL SUBMISSIONS:

We are looking for 300-400 words of expert commentary on one of the above features, delivered to editor Brian Wall by email on or before the deadline date given for each issue. (NB: This may need to be edited down where space does not allow the submission to run in full and also where contributions from several sources overlap.)

The submission should come from a named spokesperson within the company, with full job title and **HIGH RESOLUTION** image, plus any other relevant HIGH RES 'action' shots.

Also, it is essential that the copy should be editorial – and therefore neutral – in tone, specifically addressing the issues raised in the synopses above. **If it is not editorial in style and content, nor in synch with the synopsis, it is unlikely to be used.**

Please contact me as soon as possible, if you would like to be involved, so I can allocate space, as this will be strictly limited.

If you are interested in contributing editorially to any of these features, contact:

Brian Wall
Editor of Computing Security magazine
Email: brian.p.wall@btc.co.uk