ELSEVIER

network SECURITY

ISSN 1353-4858 June 2018

www.networksecuritynewsletter.com

Featured in this issue:

Are businesses getting complacent when it comes to DDoS mitigation?

The number of distributed denial of service (DDoS) attacks is growing, as is the likelihood of any given organisation being attacked.

There is now a growing realisation among businesses that no industry is safe: any type of business with an online presence is at risk. And yet still we hear the phrase 'it will never happen to me'. Too few organisations are taking note of the multiple warnings in the media and from the security industry, warns Chris Townsley of CDNetworks.

Full story on page 6…

Instilling a culture of data security throughout the organisation

While the threat of the bad guys infiltrating a modern organisation's network may be less than first thought, behaviour that can be just as damaging and expensive to businesses is happening all around us.

In fact, we may even be guilty of the contributing factors ourselves. There needs to be a shift in attitude. While implementing the right information security systems is important, organisations must also instil the right culture within the business so that employees understand and respect the importance of data security and don't put the organisation at risk, says Mike Simmonds of Axial Systems.

Full story on page 9…

How to build a secure API gateway

Most of the major technology trends of the past few decades have resulted in ever-greater numbers of connections to corporate IT assets.

At the heart of these connections are application programming interfaces (APIs) that underpin almost every interaction or process and these have quickly become a prime target for attackers. Yet despite their growing prominence, they have largely remained the sleeping giant of our technology-led world, attracting too little attention when it comes to security, explains Jason Macy of Forum Systems.

Full story on page 12…

Sharp rise in costs and damage from DNS-related attacks

Cyber-attacks that either target or exploit the Domain Name System (DNS) have risen steeply over the past year – as have the costs associated with them.

The '2018 Global DNS Threat Report' from EfficientIP claims that 77% of organisations were hit with a DNS-related attack in the past year, with an average of seven attacks per organisation. A third of organisations suffered data theft as a result of the attacks, which cost an average of $715,000, a rise of 57%.

"Worryingly, the frequency and financial consequences of DNS attacks have risen and businesses are late in implementing purpose-built security solutions

Continued on page 2…

Contents

NEWS

Sharp rise in costs and damage from DNS-related attacks 1

Healthcare under attack 2

FEATURES

Are businesses getting complacent when it comes to DDoS mitigation? 6

DDoS attacks continue to grab headlines as they become more prevalent and more crippling. There is now a realisation among businesses that no industry is safe. And yet still we hear the phrase 'it will never happen to me', warns Chris Townsley of CDNetworks.

Instilling a culture of data security throughout the organisation 9

The weakest part of a business's cyber-defences is likely to be its staff. There needs to be a shift in attitude. While implementing the right information security systems is important, organisations must also instil the right culture within the business so that employees understand and respect the importance of data, says Mike Simmonds of Axial Systems.

How to build a secure API gateway 12

Almost every application relies on communication to a server or database somewhere. At the heart of these connections are application programming interfaces (APIs), which have quickly become a prime target for attackers. Yet despite their growing prominence, they receive too little attention when it comes to security, explains Jason Macy of Forum Systems.

The need for continuous compliance 14

With the new EU General Data Protection Regulation (GDPR), the need for businesses to remain compliant with increasingly stringent industry regulations has once again come into focus. Compliance should no longer be thought of as a simple tick in a box. Nor is it something that should be considered complete the moment it has been achieved. Rather, it should be thought of as an amorphous organism that is continuously changing, argues Javid Khan of Pulsant.

Friendly fire: how penetration testing can reduce your risk 16

To get an accurate idea of how secure your systems are, you need to put them to the test. Yet even though penetration testing is a long-established means of doing this, it remains severely underused. In this interview, Dave Adamson of EACS explains some of the reasons for this and how organisations could exploit testing to reduce their risk.

Report Analysis 3

News in brief 4

Reviews 5

The Firewall 20

Events 20

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Bethan Keall

Editor: Steve Mansfield-Devine
E-mail: infosec@webvivant.com

Senior Editor: Sarah Gordon

Columnists: Tim Erridge, Karen Renaud, Colin Tankard

International Editoral Advisory Board:
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

…Continued from front page

to prevent, detect and mitigate attacks," David Williamson, CEO of EfficientIP, writes in the report.

The five most common DNS-based attacks are: DNS-based malware; phishing; DNS tunnelling; domain lock-up; and distributed denial of service (DDoS) attacks on DNS servers. Many of these completely bypass traditional security measures. The report details the most significant consequences as brand damage and the theft of intellectual property or customer information. More than a fifth (22%) suffered business losses due to DNS attacks, and in some cases the associated costs were over $5m.

The effects can be particularly severe when it comes to cloud services, the report claims, with two-fifths of organisations suffering downtime in these services as the result of a DNS-related attack.

DNS is both an attack vector and a target. Malware and hackers can exploit the DNS infrastructure to steal data, communicate with command and control servers, establish phishing and spam domains and so on. Alternatively, malicious actors may target DNS services directly, such as using DDoS attacks to effectively take domains offline by making DNS lookups impossible.

"The results of this survey are unsurprising and represent a serious issue for all Internet users," said Tim Helming, director of product management at DomainTools. "We have visibility to a multitude of websites which exploit the DNS infrastructure for malicious purposes, creating fake domains cybersquatting on legitimate brand or organisation names in order to distribute spam and malware, or engage in other malicious activities. What's more, with the new regulatory changes ushered in by the GDPR, the visibility of Whois data used to combat these malicious sites will be reduced, hindering researchers and in turn creating a safer environment for scammers and cyber-criminals and a more dangerous one for legitimate users of the Internet."

The report is available here: www.efficientip.com/resources/dns-security-survey-2018/.

Healthcare under attack

Cyber-criminals are increasingly focusing on the healthcare sector, particularly as targets for ransomware, according to two new reports.

While ransomware attacks have reduced to some extent, they remain a problem for healthcare organisations. And according to research by Proofpoint, other forms of attack mean that the healthcare industry is still under siege.

Its report says that cyber-attacks are exposing personal data, shutting down emergency rooms and defrauding partners, patients and staff. The firm logged more than 100 million ransomware emails sent to hospitals, clinics and health insurers over the course of a year. But, after peaking in the third quarter, ransomware traffic collapsed as attackers switched tactics, with business email compromise (BEC) becoming more prominent.

Nearly a fifth of emails purporting to be from a healthcare organisation were fraudulent the report claims.

There's more information here: http://bit.ly/2JI3tCi.

Imperva found that more than one in three healthcare organisations has suffered a cyber-attack within the past year, while almost one in 10 have paid a ransom or extortion fee. The firm surveyed healthcare IT professionals and found that 15% admitted their organisation's ability to handle a cyber-attack needed work.

Ransomware remains a major concern for a third of respondents. Attackers know that if a healthcare organisation does not have a mitigation strategy in place, they will likely opt to pay a ransom, rather than risk losing access to patient files entirely. However, research has shown that 50% of organisations never get their data back even.

Regarding insider threats, respondents were most concerned about careless users (51%). Additionally, 27% said a lack of tools to monitor employees and other insider activities makes detecting insider threats difficult. A third (32%) indicated that collecting information from diverse security tools is the most time-consuming task when investigating or responding to insider threats.

The report is here: bit.ly/2s2gYlq.

Report Analysis

Synopsis: Open Source Security and Risk Analysis

The open source movement has revolutionised the software world, from giving us powerful platforms such as operating systems and web servers down to the level of code snippets that solve specific problems. And leaving aside the debates around 'free' software, one of the promises of open source software (OSS) is the concept of 'many eyes' – that by being open to scrutiny by anyone, OSS leads to solutions that have fewer bugs. And that should mean fewer vulnerabilities, leading to fewer security issues.

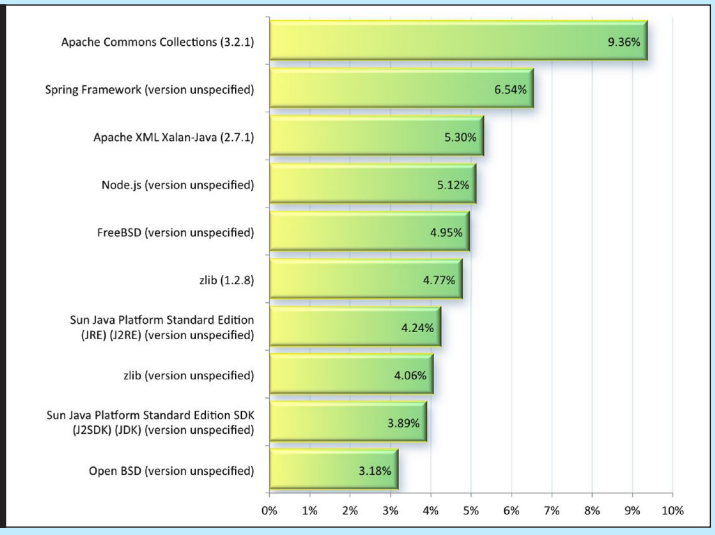
Nothing is ever that simple, of course. Organisations struggle to stay on top of what software they're running within their infrastructure even when they are paying hefty licence fees for it. With software that is free and available at the click of a download button, it can be even harder to keep track.

And the issues involve more than the big-name solutions: open source programming frameworks and libraries are in widespread use by development teams. Precisely what OSS components are in use in your organisation is often regarded as an implementation detail, of interest only to the coders working at the development coalface. And as the '2018 Open Source Security and Risk Analysis' report from Black Duck by Synopsys underlines, this attitude is a mistake. It's possible that OSS components are playing a critical and strategic role in the software on which your organisation depends. And when vulnerabilities become public knowledge, you need to find out if you're at risk because you're using the affected codebase – hackers will certainly be happy to discover if you're vulnerable.

"Since modern software and infrastructure depend heavily on open source technologies, having a clear view of components in use is a key part of corporate governance," said Tim Mackey, technical evangelist at Black Duck. "The report clearly demonstrates that with the growth in open source use, organisations need to ensure they have the tools to detect vulnerabilities in open source components and manage whatever licence compliance their use of open source may require."

There has been a timely reminder of this issue. As this issue was going to press, news broke of the 'Zip Slip' problem. Security firm Snyk revealed that certain libraries in common use that work with archive files could allow attackers to upload files to, say, websites that would overwrite existing files in arbitrary locations, thanks to a directory traversal flaw. There's more information here: http://bit.ly/2Js1JcM. The key issue here is that many organisations won't know they are vulnerable to this issue because a developer has simply downloaded a handy library or cut and pasted some code from StackOverflow and there's no record of the code being used.

Black Duck analysed more than 1,100 codebases in use in a variety of industries. It found a significant rise in OSS adoption, with 96% of the scanned applications having open source components – an average of 257 components per codebase (a 75% rise over the previous year). In fact, the applications use more OSS code than they do proprietary code.



The top 10 high-risk components found in the study (percentage of codebases). Source: Synopsys.

Alas, some of that code is vulnerable, and this applies to all the industry verticals studied. This was most marked in the Internet and software infrastructure sector, where 67% of applications contained high-risk open source vulnerabilities. The report notes that: "Ironically, 41% of the applications in the cyber-security industry were found to have high-risk open source vulnerabilities, putting that vertical at fourth-highest risk."

Where Apache Struts was present in the codebase, a third of instances also included the vulnerability that resulted in the massive Equifax breach.

"When Equifax was breached through the Apache Struts vulnerability, the need for open source security management became front page news," said Evan Klein, the Black Duck product marketing manager responsible for the OSSRA report. "Yet, even though it was disclosed in March 2017, many organisations apparently still have not checked their applications for the Struts vulnerability."

Some 74% of the codebases studied also contained components with licence conflicts, the report states, the most common of which were GPL licence violations. And the report warns of the difficulties that organisations can face with updating software. Patching in the OSS world tends to be somewhat patchier than with proprietary solutions with their built-in update mechanisms.

Not everyone is happy about some of the implications of the report. "The assertion that all open source software fails to automatically push out updates to users is inaccurate," said Jamie Bennett, VP of engineering, IoT and devices at Canonical, which produces the Ubuntu operating system. "The notion that open source software can go years with unpatched vulnerabilities is an issue, but not one that is contained in all open source software."

The report is available here: http://bit.ly/2Inp3Ix.

In brief

EU agencies fight dark web

Several European law enforcement agencies have joined forces to combat illegal activities on the dark web. The new Europol Dark Web Team includes representatives from the European Commission, Interpol and Eurojust as well as national and regional law enforcement agencies from 28 countries. It will be based at Europol's European Cybercrime Centre (C3). The move formalises ad hoc collaborations that have been successful in taking down a number of underground forums and marketplaces.

Google Groups leak data

Research by security firm Kenna Security has discovered that thousands of organisations are exposing potentially sensitive information as a result of using Google Groups. Many companies use Groups – which is included in the G Suite of tools and applications – to manage internal mailing lists and discussion forums. Kenna analysed 9,600 organisations with public Google Groups settings and found that 3,000 were exposing data. They included Fortune 500 corporations, hospitals, universities, media organisations and US Government agencies. At the heart of the problem is the misconfiguration of privacy settings that makes information that should be shared only among group members available to anyone who visits Google Groups. Journalist Brian Krebs followed up with his own examination and concluded: "In most cases, to find sensitive messages it's enough to load the company's public Google Groups page and start typing in key search terms, such as 'password,' 'account,' 'HR,' 'accounting,' 'user name' and 'http:.'." There's more information here: http://bit.ly/2sLTm5N.

Whalers seized

Police forces in several countries have arrested 74 people and seized more than $16m in funds in a joint operation targeting fraudsters who carry out so-called 'whaling' attacks, more properly known as business email compromise (BEC). In BEC attacks, people are fooled into making changes to the wiring address for invoices and contracts so that funds end up in the criminals' accounts. Operation WireWire, led by the FBI, resulted in 42 people being arrested in the US, 29 in Nigeria and three each in Canada, Mauritius and Poland. Many of those arrested are believed to be money mules, who launder funds by moving them around the world. The FBI said that several were also members of "international criminal organisations". There's more information here: http://bit.ly/2JJjvf5.

Mobile mining

Research by RiskIQ has revealed that cryptojacking is becoming a major problem on mobile platforms as well as desktop ones. For the 'Mobile Threat Landscape Q1 2018 Report', the firm analysed 120 mobile app stores and more than two billion daily scanned resources. It found a sharp rise in the number of apps that exploit a user's device to mine crypto-currencies, particularly Monero. In one case, Calendar 2, which appeared in the Apple App Store, the app disclosed this activity and offered the option for users to pay fees instead, or use the app with all advanced features disabled. However, the app developers set mining as the default option. The report also showed that malicious mobile apps continued to decline, despite the number of total apps observed by the company increasing over the past four quarters. In Q1, 21,948, or 1.4%, of the total of 1,508,825 newly observed apps were blacklisted by RiskIQ for being malicious, which is a lower percentage than in the previous four quarters. Google hosted 8,287 blacklisted apps in Q1, which is consistent with previous quarters and outpaces the next-most-blacklisted store, AndroidAPKDescargar, by 4,595. Although the Play Store consistently had high numbers of blacklisted apps between Q3 2017 and Q1 2018, its rate of blacklisted apps has hovered around a relatively modest 5%. There's more information here: http://bit.ly/2JJL481.

Paying ransoms

A third of organisations worldwide would try to cut costs by considering paying a ransom demand from a hacker rather than investing in information security, according to a report from NTT Security. In the UK, this figure drops to a fifth (21%). In the 2018 'Risk:Value Report', NTT claims that another 30% in the UK are not sure if they would pay or not, suggesting that only around half are prepared to invest in security to proactively protect the business. Levels of confidence about being vulnerable to attack also seem unrealistic, according to the report. Some 41% of firms in the UK claim that their organisation has not been affected by a data breach, compared to 47% globally. Of those in the UK, 10% expect to suffer a breach, but nearly a third (31%) do not expect to suffer a breach at all. More worrying is the 22% of UK respondents who are not sure if they have suffered a breach. Just 4% of respondents in the UK see poor information security as the greatest risk to the business while 14% put Brexit in that category. The estimated cost of recovery globally, on average, has increased to $1.52m, up from $1.35m in 2017, although UK estimates are lower at $1.33m this year. Globally, respondents anticipate it would take 57 days to recover from a breach, down from 74 days in 2017. However, in the UK, decision-makers are more optimistic, believing it would take just 47 days to recover, one of the lowest estimates for any country. The report is available here: http://bit.ly/2Mi6p7f.

Inadequate back-ups

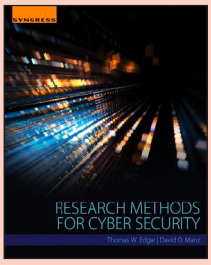
Almost a million UK businesses do not back up their company data and a further 2.8 million risk losing valuable information by storing electronic copies in the same location as the original data, according to new research from Beaming. The survey shows that although most (83%) of UK firms back up their data, half save it to servers or storage devices on the same premises. Nearly half (44%) of small businesses, 42% of medium sized firms and 34% of large organisations currently store backup information in the same location as it is generated, leaving them vulnerable to data loss through theft, fire or malware attack. Some 17% of businesses keep no data back-ups whatsoever and store information only on individual computers and employee devices. Sole traders and micro companies employing fewer than 10 people are the most likely to be guilty of not backing up their data. Only a third (35%) of UK businesses currently store their backup data to locations outside the office but less than a fifth (18%) back up their data to facilities located at least 30 miles from their own premises, the minimum distance recommended by business continuity experts to limit the IT impact of natural disasters. Most of the companies adhering to the '30 mile rule' are using cloud-based storage services and do not know precisely where their data is held.

Android devices ship with adware

Avast Threat Labs has found adware pre-installed on several hundred Android device models and versions, including devices from ZTE, Archos and myPhone. The majority of these devices are not certified by Google. The adware goes by the name 'Cosiloon' and creates an overlay to display an ad over a web page within the user's browser. Thousands of users are affected and in the past month alone, Avast has seen the latest version of the adware on around 18,000 devices belonging to users located in more than 100 countries including Russia, Italy, Germany and the UK, as well as some users in the US. The adware has been active for at least three years and is difficult to remove as it is installed at the firmware level and uses strong obfuscation. Avast contacted Google, which has taken steps to mitigate the malicious capabilities of many app variants on several device models, using internally developed techniques. Google Play Protect has been updated to ensure there is coverage for these apps in the future. However, as the apps come pre-installed with firmware, the problem is difficult to address.

Reviews

BOOK REVIEW



Research Methods for Cyber Security
Thomas Edgar and David Manz.
Published by Syngress.
ISBN: 9780128053492. Price: $89.95, 428pgs, paperback.
E-book edition also available.

Cyber-security is usually regarded as a very pragmatic, hands-on kind of activity. In fact, most of the more highly regarded certifications in the industry, such as CREST, place significant emphasis on testing practical ability.

A large proportion of hackers – of both the white- and black-hat variety – have learned their trade in a purely empirical manner. They have acquired and honed their skills by doing, albeit supported by the careful reading and understanding of protocols and processes. The purpose of cyber-security, after all, is to protect real-world systems.

Some aspects of cyber-security, of course, have their roots deep in theoretical concepts, with cryptography being perhaps the most obvious example. And the field draws on the wider discipline of computer science, which is heavily grounded in mathematics. But while something like, say, the Diffie-Hellman key exchange might be highly mathematical in conception, most cyber-security practitioners know it only from its application in software solutions. The scientific foundations of security rarely escape the confines of academia.

Part of the issue is the fast-changing nature of cyber-security. The technology we are trying to defend is constantly changing and becoming more complex, both in terms of individual devices or solutions and in the way they interact with each other. And the bad guys are innovative, too, frequently developing novel forms of attack. Much of the focus in cyber-security is on the practical needs of individuals and organisations to protect themselves.

That said, recent years have seen the growth of a corpus of literature – some of it in these pages – in which theoretical approaches play an increasingly important part. And the authors of this book attempt to take this a step further by exploring whether it's possible to provide a scientific definition for what security means and apply scientific methodologies and analyses to understand, objectively, the security of a system.

Coming from a background of an emerging 'science of security' community, the authors present scientific methods to help researchers establish a rigorous framework for studying cyber-security, encompassing theoretical, mathematical, observational, experimental and applied research.

According to the introduction: "This book seeks to borrow from the thousands of years of development of the scientific method in other disciplines, and to enhance the conduct of cyber-security research as a science in its own right. The intended outcome from using this book is research that is relevant, repeatable and documented such that colleagues can understand and critique the results and conclusions. The focus of this book is on the practical side of science, the research methods that can be used to perform your research."

"Coming from a background of an emerging 'science of security' community, the authors present scientific methods to help researchers establish a rigorous framework for studying cyber-security"

The book starts, perhaps surprisingly, with a fairly long exploration of what we mean by 'science' and an examination of the scientific method – just so that everyone is reading from the same page when these terms are bandied about. It then goes on to study how science relates to cyber-security – and where it often doesn't, not least because the latter is such a young discipline. It introduces many of the standard cyber-security concepts, such as what we mean by vulnerabilities, exploits, threat vectors and so on.

However, the meat of the book starts towards the end of the first section when the authors look at how to start planning your research. Subsequent sections cover observational research methods; mathematical research methods; experimental research methods; applied research methods; and a final part looking at instrumentation, dealing with adversarial situations and scientific ethics.

Inevitably, the book is primarily aimed at academic researchers and has been structured to be suitable for university coursework. However, it would also provide a solid foundation for any security practitioners looking to deepen their understanding of the field beyond reading CVEs and RFCs. The authors, then, intend that the book can be used in either of two ways – being read cover-to-cover as a course in the scientific foundations of cyber-security or as a resource whose chapters provide illumination for researchers studying specific topics.

While it might sound that this is a book that is going to be full of theory, its content is actually highly practical – if your practice is research. It is all about how to ensure your research is properly conducted and has a sound scientific basis so that your results are truly meaningful and can be shared easily and effectively with others. There is a strong emphasis on ensuring that the objectives of any research project are fully and rationally defined, that the conditions of any testing or experimentation (including simulations) are appropriate and realistic, and that the findings are presented in a way that is honest, useful and relevant.

In over 400 pages, the authors go into significant detail about how to achieve all of this. As a researcher, you could use this book as a template for a research proposal, and for mapping out how you will carry out your data gathering and analysis. How useful this will prove depends entirely on the nature of your work, of course. If you are studying malware in order to code better anti-virus software, then scientific rigour isn't necessarily an asset, especially if it comes at the cost of slowing things down because of the need to plan carefully and ensure all avenues are covered. If, on the other hand, you're trying to develop a deeper understanding of how malware operates, to uncover conceptual principles that might lead to novel mitigation methods, then the scientific approach is more appropriate.

Either way, it's encouraging that cyber-security is moving away from purely pragmatic firefighting into a realm of deeper understanding, and this book is both an indication of that development and a contribution to it.

There's more information here: http://bit.ly/2JCIPQE.

– SM-D

Are businesses getting complacent when it comes to DDoS mitigation?

Chris Townsley

Chris Townsley, CDNetworks

There is no doubt that the number of distributed denial of service (DDoS) attacks is growing, as is the likelihood of any given organisation being attacked. DDoS attacks continue to grab headlines as they become more prevalent and more crippling in their effect. There is now a growing realisation among businesses that no industry is safe: any type of business with an online presence is at risk.

Already this year, Dutch banks Rabobank and ING fell victim to an aggressive DDoS attack launched by a teenager in the Netherlands.[1] In a different industry entirely, news wire service Business Wire suffered a week-long attack by an anonymous attacker. And yet still we hear the phrase 'it will never happen to me'. Too few organisations are taking note of the multiple warnings in the media and from the security industry.

A recent report into DDoS protection, which evaluated businesses' ability to mitigate DDoS attacks, revealed that while the overwhelming majority (83%) of businesses believe they are adequately prepared to withstand an attack, 54% had suffered at least one successful DDoS attack in the 12 months prior to the survey.[2] These figures highlight the great confidence in DDoS mitigation strategy among IT teams. But businesses are losing the DDoS arms race, which raises the question, are they getting complacent?

Investment on the rise

With increased investment in DDoS protection, many businesses are feeling more confident in their ability to mitigate an attack. High profile attacks such as the Dyn attack that brought down Twitter and CNN in 2017 seem to have triggered substantial investment.[3] In fact, the most popular time to have invested in DDoS mitigation technology for the first time was within the last year. And nearly two-thirds (64%) of businesses claimed they plan to invest further in the next 12 months. Of the minority that haven't yet invested, almost all of them are planning to or are considering investment.

"The most popular time to have invested in DDoS mitigation technology for the first time was within the last year. And nearly two-thirds (64%) of businesses claimed they plan to invest further in the next 12 months"

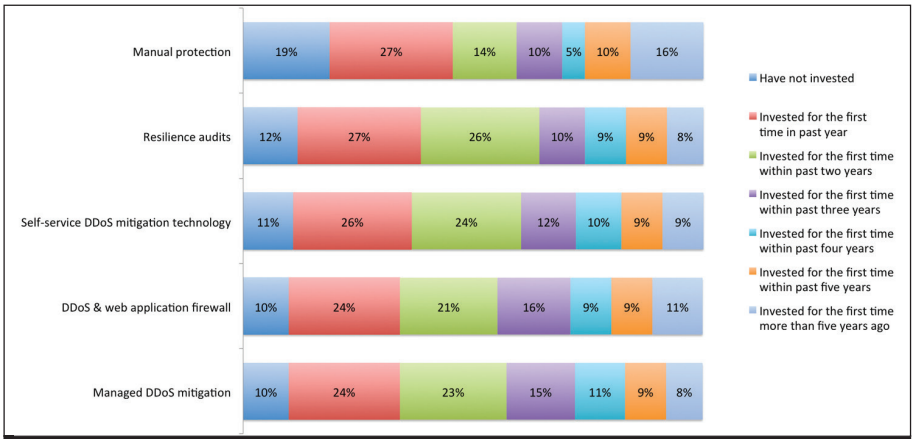
This is of course a step in the right direction. But while this investment is helping protect businesses, it is leading to overwhelming confidence in DDoS resilience. As seen from the number of successful attacks detected, this confidence is misplaced and is dangerous.

Justified confidence?

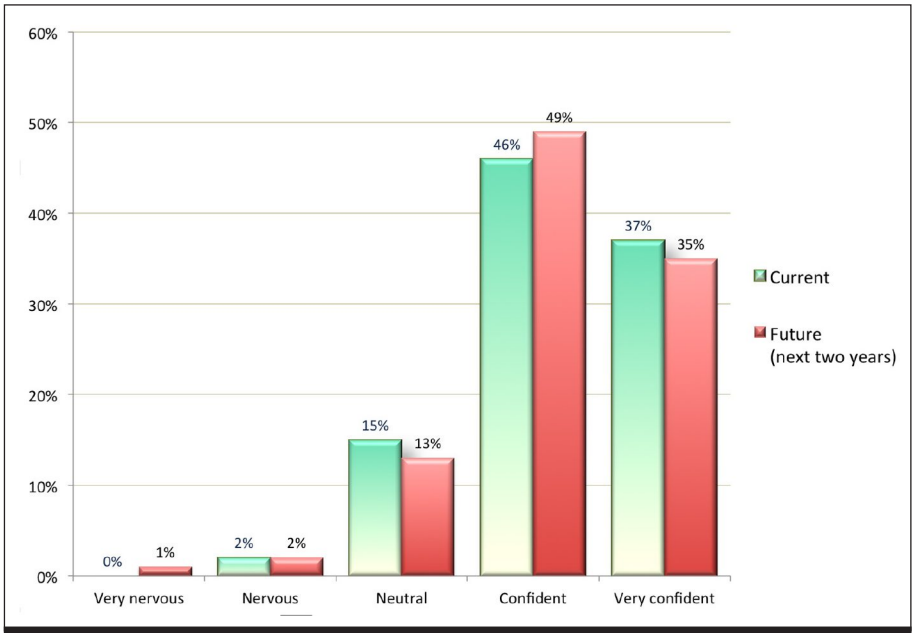
There would be some excuse for the overconfidence in DDoS mitigation if the victims of DDoS attacks were randomly selected. But this excuse doesn't stack up. In fact, nearly a third (31%) of victims were convinced that their successful attacks were intentional.

More and more, industrial sabotage is considered to be the reason behind DDoS attacks, with many businesses pointing the finger at rival firms that they believe are trying to gain a competitive advantage. A large-scale DDoS attack can be costly in both the interruption of service and subsequent loss of sales, as well as the long-term damage to a business's reputation. With the ability to set up a DDoS attack cheaply and easily, it is not difficult to believe that a competitor could launch such an attack.

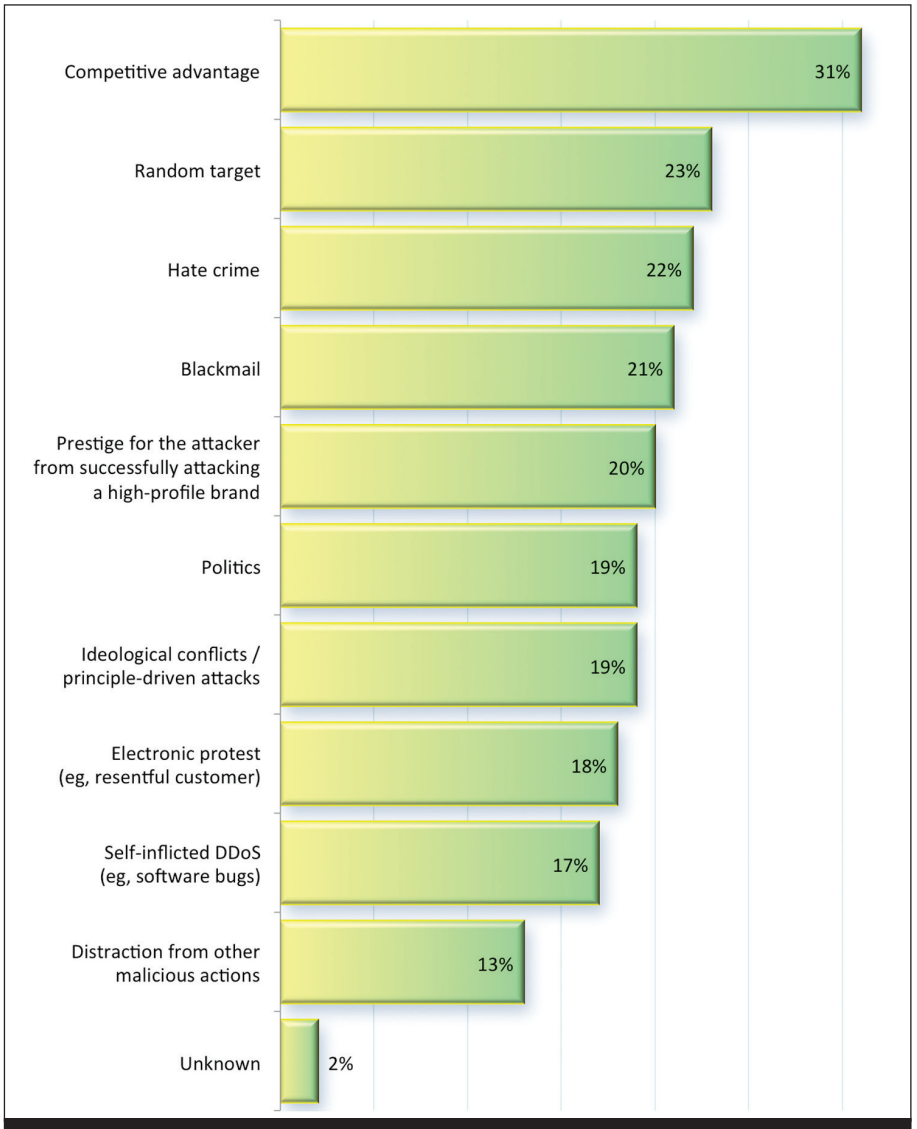
But it's not just rival firms that businesses are concerned about. There is a common belief among businesses that



Investment in DDoS mitigation. Source: CDNetworks.



How organisations rated their confidence in their current and future DDoS mitigation setups. Source: CDNetworks.



Reasons organisations believe they were attacked. Source: CDNetworks.

they have been the target of blackmail, hate crime or ideological conflicts.

They are aware of this threat and clearly have their suspicions. It is these deliberate motivations that make the IT teams' over-confidence and under preparation all the more striking. Businesses may be investing in DDoS technology, and feel confident in their DDoS resilience, but the reality is that they continue to fall victim to attacks.

"Increased budgets alone cannot protect a business. A fundamental change in mindset and more targeted technology investment are needed before a business can truly be confident"

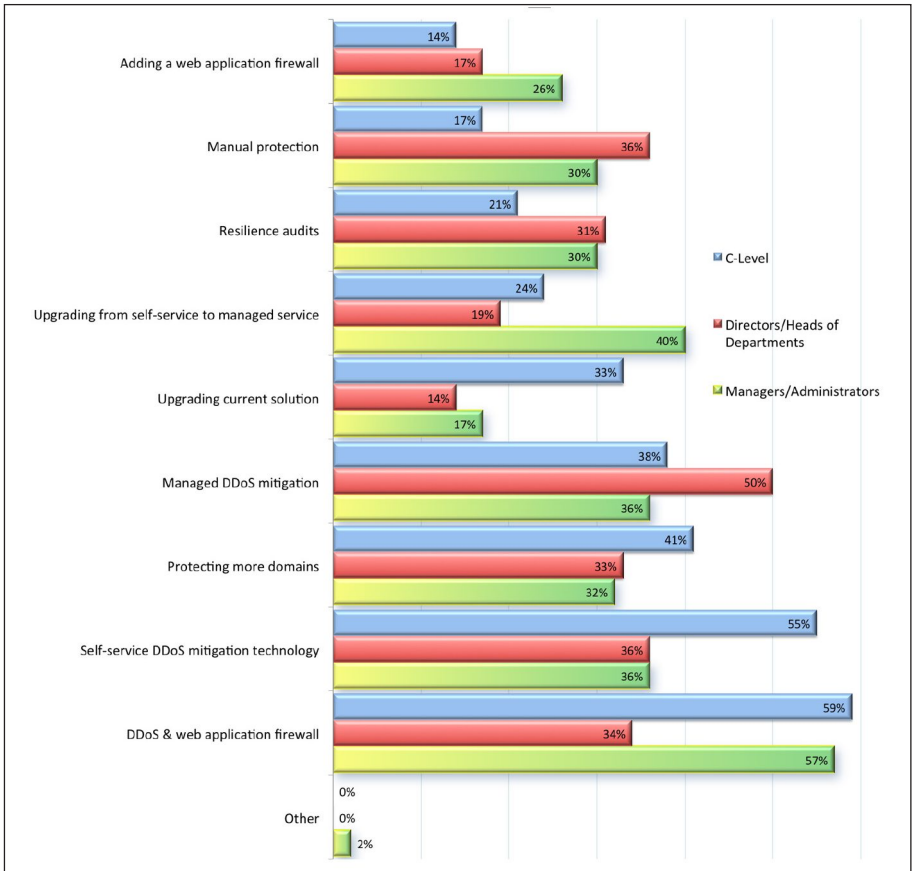
This is heightened when looking at how businesses see the severity of DDoS attacks – only 5% believe a DDoS attack would be catastrophic in its effect. Increased budgets alone cannot protect a business. A fundamental change in mindset and more targeted technology investment are needed before a business can truly be confident.

Targeted investment

There are a number of different people within a business who will be involved in deciding how best to protect against a DDoS attack. This naturally leads to internal disagreement about where additional investment should be directed.

For example, C-suite level executives tend to favour self-service DDoS mitigation technology, whereas IT managers favour upgrading from self-service to managed services. The C-suite has an inherently broader view and additional concerns, like customer data protection, which is why they lean towards a self-service technology. The IT managers' preference for managed services is a case of them being more aware of the workload that a DDoS attack creates and their focus is therefore on trying to mitigate it.

Ultimately, throwing money at DDoS technology will only get a business so far. With over half of businesses suffering successful DDoS attacks, they need to be smarter with their investment and understand the nature of the threat. As



Areas where companies that are currently underinvesting believe they should invest in the future. Source: CDNetworks.

such, businesses need to first determine if they have under-provisioned DDoS mitigation, and then take the appropriate steps to safeguard their business.

The first step therefore is to test the severity of the problem. Performing a vulnerability test can identify where the gaps lie in a system or network defences and how easily these can be exploited. Penetration testing can simulate an attack on the vulnerabilities from within and outside the network to determine if unauthorised access can be made to data. This is particularly important for industries at risk from a data breach, such as financial services or healthcare. While a DDoS attack itself does not expose an organisation to this threat, attacks can be used by cybercriminals to deliberately distract from a hack to the direct network, which could expose sensitive data.

It's clear that more targeted investment is needed, but there is disagreement on this within businesses. Only by testing can a business see where its vulnerabilities lie and determine which technologies or services are needed. With DDoS attacks evolving so quickly in their scope, it's crucial for businesses to keep up.

Where to invest

To do this, some businesses rely on specialist on-premise equipment and deploy hardware in datacentres in front of everyday servers and routers. But this is an expensive solution and requires regular updates to address the continued evolution of DDoS attacks. Failure to keep up with this extends the risk.

A network's weakness is its own capacity limit. So, if a DDoS attack breaches the threshold, the network fails. Opting for a cloud-based migration provider offers greater protection, as the capacity that cloud migration providers can consume on behalf of a business far exceeds that of any datacentre.

Resources such as the Open Web Application Security Project (OWASP) can help DDoS mitigation planning. OWASP ranks the top 10 most critical web application security risks by ease of exploitation, prevalence, detectability and impact.[4] When this is combined with advice from security partners, businesses can better plan their investment and truly begin to be confident in their defences.

Preparing for the worst

One of the dangers of overconfidence is that businesses that haven't yet suffered a successful attack can underestimate the impact it will have on them. However much of a risk a business believes DDoS to be, it's always best to prepare for the worst. Having a step-by-step guide, sometimes known as a 'runbook', assists IT employees and helps make sure there is a process in place should an attack strike. Without a process in place, a business can waste valuable time escalating an incident and deciding on the best response.

Another part of preparing for the worst is getting to know the 'likelihood calendar'. DDoS attacks have a habit of happening at the worst possible time and that's not always a coincidence. For example, an e-commerce website can find itself particularly vulnerable around big retail events such as Black Friday, as cyber-criminals want to attack at peak times when traffic will be higher than usual and the victim has more to lose. Understanding the likelihood calendar can help businesses anticipate when an attack may take place.

"Preparing for the worst is getting to know the 'likelihood calendar'. DDoS attacks have a habit of happening at the worst possible time and that's not always a coincidence"

It's also wise to have a policy on ransom notes. Blackmail attacks, including ransomware, can create panic throughout a business, but having an agreed policy in place ensures that the business can have an informed response. Paying is never recommended, as there is no guarantee that payment will stop the attack. A business that continues to pay out is more likely to become a repeat victim.

The best advice is to inform the legal team of an attack. In some cases, a note can be sent before the attack has even

begun and it remains unclear whether one was ever likely or even possible.

"There is more beyond investment that can be done to fully prepare should a DDoS attack strike. Only by understanding the risk can businesses start to gain true confidence in their resilience"

Many businesses devise a communications plan in the event of a DDoS attack, but fail to appreciate that some usual mechanisms, such as a blog or email, may not function as a result of the attack. Businesses should think about how they can use other methods of communication, such as Twitter, in order to inform employees, customers or even the media, of an attack.

Gaining confidence

Each of these processes and steps critically depends on a business being cautious and not overconfident or complacent. Businesses that recognise they are losing the DDoS arms race have re-evaluated the technology they have invested in, and considered the different processes they need to put in place to anticipate and plan for an attack. They have also taken out insurance policies to protect against an attack.

While a business can never have 100% confidence, there is more beyond investment that can be done to fully prepare should a DDoS attack strike. Only by understanding the risk can businesses start to gain true confidence in their resilience.

About the author

Chris Townsley is EMEA director at CDNetworks, a global content delivery provider. He has been in the CDN industry for the past 10 years and has over 25 years of international experience. Having worked across a large number of industries and companies, Townsley understands the challenges faced by companies looking to expand their online presence beyond domestic borders.

References

1. Pieters, Janene. 'Teen suspected of DDoS attacks on Dutch financial services wanted to prove a point'. NLTimes, 7 Feb 2018. Accessed May 2018. https://nltimes.nl/2018/02/07/teen-suspected-ddos-attacks-dutch-financial-services-wanted-prove-point.
2. 'Businesses are dangerously overconfident in the DDoS mitigation'. CDNetworks. Accessed May 2018. www.cdnetworks.com/uk/en/ddos-protection.
3. Woolf, Nicky. 'DDoS attack that disrupted Internet was largest of its kind in history, experts say'. The Guardian, 26 Oct 2016. Accessed May 2018. www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.
4. 'OWASP Top 10 – 2017'. OWASP. Accessed May 2018. www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Instilling a culture of data security throughout the organisation

Mike Simmonds

Mike Simmonds, Axial Systems

It has long been acknowledged that cyber-security is only as robust as its weakest link. While that could be an unpatched switch or a USB drive left in a company car park, one thing is generally consistent: the weakest part of a 21st Century business's cyber-defences is likely to be its staff.

There needs to be a shift in attitude. The attacks on the likes of Sony, TalkTalk and Yahoo have all made headline news throughout the globe, causing cyber-security awareness arguably to reach an all-time high. However, intentional criminal acts on the business community remain relatively rare considering how central sensitive data stores are to nearly every industry on earth. While the threat of the bad guys infiltrating a modern organisation's network may be less than first thought, behaviour that can be just as damaging and expensive to businesses is happening all around us. In fact, we may even be guilty of the contributing factors ourselves.

Human factors

The UK Government's Cyber Security Breach survey last year noted that: "Breaches are often linked to human factors, highlighting the importance of staff awareness and vigilance. However, few businesses currently provide staff with cyber-security training (20%) or have formal policies in this area (33%)."[1] This was also echoed in this year's report.[2]

The fact that some four out of five businesses don't provide staff with cyber-security training is simply staggering. After all, how many times in the past year has your organisation undertaken a fire drill? If you are like us, every few months there will likely be the shrill of the fire alarm, following by everyone obediently trudging down to an otherwise unused

corner of a car park that has been reserved for just such an occasion. The threat of a fire is quite rightly taken very seriously in businesses and is likely to be an integral part of every new staffer's induction. However, in 2018, shouldn't that induction now also include training for how to handle a cyber breach?

False sense of security

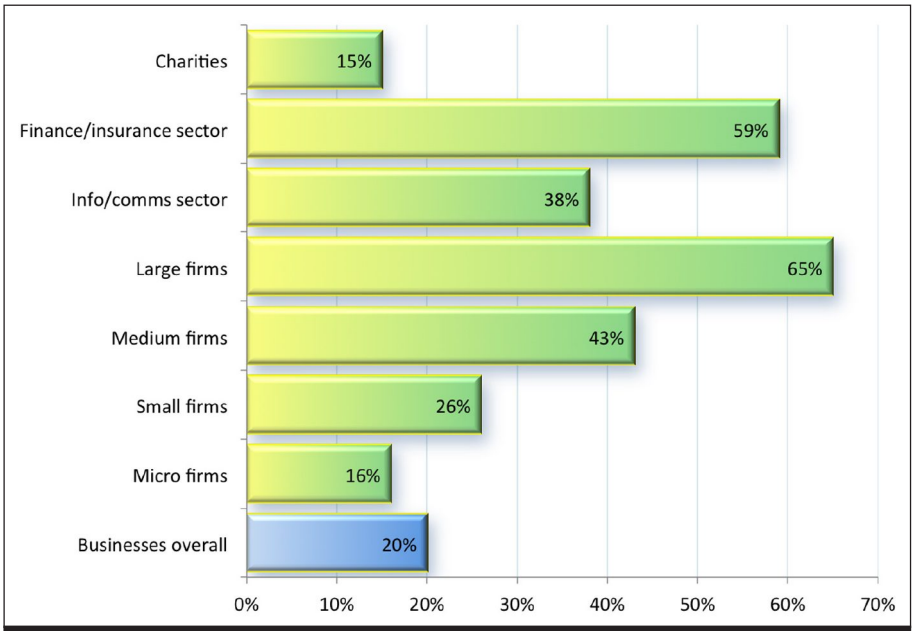
Firewalls and intrusion prevention solutions continue to keep pace with new and emerging cyberthreats to provide IT admins with a false sense of security. However, a Kaspersky Lab security risks survey found that three out of five (59%) of those polled believe that the most serious data breach they'd experienced was down to careless or uninformed employee actions.[3] It also revealed that the most frequent point of vulnerability was inappropriate usage or sharing data via mobile devices.

"Buoyed by speedier infrastructure and a greater culture of trust from employees, the trend for remote working shows no sign of abating"

Yes, those ticking time bombs in all our pockets. Since the start of the digital revolution, mobiles have grown to not just form part of the furniture of all our lives but have become almost an extension of our very selves. Today, there are more mobile phones on the planet than there are people and everyone from tech entrepreneurs to your grandparents will now probably own one. However, as they have become easier and more intuitive than ever before to use, leading us to be more connected to the information super highway than ever before, people have seemingly forgotten the inherent dangers that they present.

Blurred lines

With mobile phones being central to all our lives and the lines between personal and business use becoming increasingly blurred, the apps we have on our handsets have increasingly become a target for hackers, especially those apps that facilitate users to store personal details. knowingly or otherwise. It is therefore imperative that mobile phones are protected just as securely as any of the other endpoints you may have on a network rich with connected Internet of Things (IoT).



Percentage of organisations where staff have attended internal or external training, or seminars or conferences on cyber security in the past 12 months. Source: 'Cyber Security Breaches Survey 2018', UK Government.

Many people now work from home. Buoyed by speedier infrastructure and a greater culture of trust from employers, the trend for remote working shows no sign of abating. In fact, by 2020 over two thirds (70%) of organisations are likely to allow home working, according to the Work Foundation at Lancaster University.[4]

Today, many of us have become accustomed to being able to work from home and access all but the most confidential of company information. Employees of today – particularly those that have been brought up in an always-on, always-connected world – see remote working and the ability to access sensitive data, as a right and become frustrated if they are unable to do so.

Belt and braces

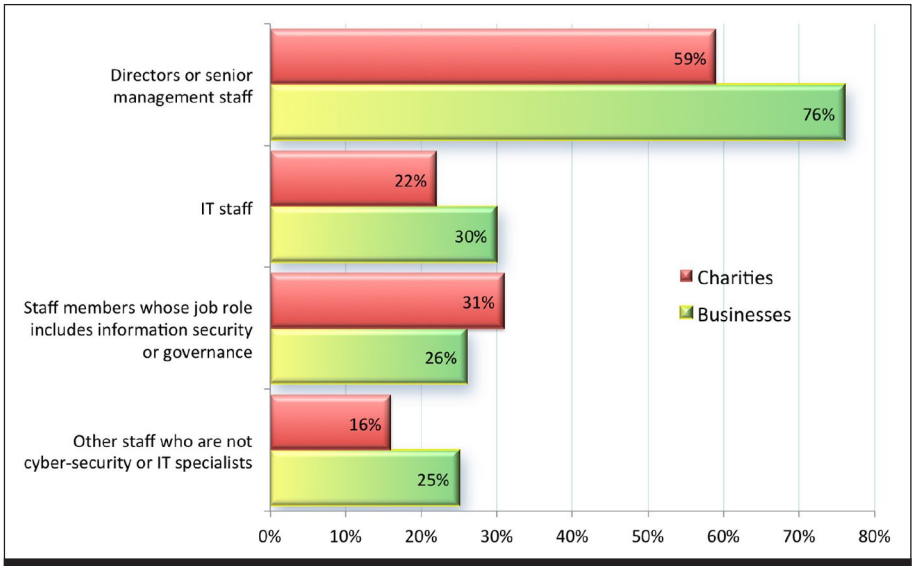
The problem is, remote workers can quickly become lackadaisical in the more relaxed surroundings of their home office. For example, they may need to give a presentation the following day and want to store it in an accessible place. They don't want to be in any uncomfortable situation of not being able to access the presentation in an unfamiliar office so take a 'belt and braces' approach by saving the slides in multiple locations: on a company laptop, on a file-sharing application and on a memory stick. The thinking being that if one fails on the day, the others can act as a back-up.

Such an approach creates its own problems. If the laptop is accidently left on a train it could become easy prey to anyone wanting to break in; the file sharing app could potentially be compromised or may be open as a searchable resource by nature of its terms and conditions; and we all know how frequently USB sticks are lost or shared without any thought as to their prior use.

In today's business landscape, the firewall is no longer the ultimate perimeter to the business. Simply by taking the data outside the corporate infrastructure, employees end up bypassing many of the expensive security measures that an organisation has in place and put potentially sensitive corporate data at risk.

Superheroes

Despite headlines telling us that names such as Uber and Deloitte have succumbed to major data breaches, many have the attitude that 'it won't happen



Which individuals in the organisation attended security training, seminars or conferences in the past year. Source: 'Cyber Security Breaches Survey 2018', UK Government.

to us'. This is particularly the case in the workplace where 'somebody else' is thought to be responsible for security. This is an outdated view that needs to change.

"There is an average of only 4.2 dedicated IT staff per organisation, which roughly equates to only one IT staffer per 100 employees"

Although many would view themselves as being on an equal footing with the superheroes they most admired from their youth, the reality is that even the most stellar IT teams are still only human. Breaches continue to occur because the latest security patches have not been applied and tested in a timely and regular manner, or a simple protective procedure has been ignored, perhaps through lack of time due to IT departments often being woefully understaffed.

Unfortunately, despite the digital transformation taking hold throughout the globe, and technology now being core to our modern civilisation, time continues to be a scant resource for the modern IT department. This is because the headcount allocated to IT departments in businesses has remained relatively constant, despite more responsibility being placed upon their shoulders. In fact, research from Spiceworks shows that there is an average of only 4.2 dedicated IT staff per organisation, which roughly equates to only one IT staffer per 100 employees for whom they are responsible. This is, alas, significantly smaller than the size of the equivalent marketing or finance departments for the size of organisation.

No more babysitting

The good news is that boards have finally begun to sit up and take notice of the dangers of a cyber breach to a modern organisation with IP and customer data at its core. However, driven mainly by the threat of huge fines from the likes of the new General Data Protection Regulation (GDPR) they are putting increased pressure on their IT departments to ensure that company networks are robust to a cyber-attack. This causes its own issues as while the growth in cyber-security awareness is now well established, the pool of skilled cyber-security talent has failed to grow alongside it

This dearth in cyber-security talent has placed the onus on everyone within the organisation to take responsibility and play their part in the overall cyber defence. Today, it is no longer possible for organisations to babysit the less technologically savvy within the business.

A combined approach

So, what's the solution for time-strapped IT departments wishing to better protect a data store that is more on the move than ever before? Yes, technology has to be a core component. Data leakage protection should be put in place, providing electronic tracking of files and putting systems in place that stop users arbitrarily dropping data out to cloud services. Adaptive authentication, in which risk-based multi-factor authentication helps ensure the protection of users accessing websites, portals, browsers or applications, also has an increasingly key role to play. All the above should happen while anti-virus and anti-malware software is kept up to date to protect against all the latest threats.

However, a combined approach is required. Information security measures need to be delivered in lock step with businesses ensuring that they hammer home the message to all employees that they must take a personally responsible approach to managing and protecting data in the modern world. They must be educated about and aware of the potential security threats and do all they can to mitigate them – from keeping secure and responsible care of devices they use at work to ensuring that their passwords are strong, unique and frequently changed.

"It's a case of getting employees on the side of the business and making them aware that what might make life easy for them can put the business at much more risk in the long run"

Making sure that every employee knows the consequences of non-compliance with regulations such as the GDPR is very important. If employees know that penalties can be as severe as €20m or up to 4% of total turnover – and consequently jobs could be at stake – the threat is no longer abstract but a real, personal concern. It's a case of getting employees on the side of the business and making them aware that what might make life easy for them can put the business much more at risk in the long run.

Sad but true

Data is the lifeblood of any organisation in the 21st century. Modern businesses

demand consistent access to network applications and data for their employees and partners. The move to more worker mobility and the drive towards fully cloud-based systems only adds complexity and increases the potential for breaches.

It's very easy to blame technology for many of today's problems but it's a particularly convenient scapegoat when it comes to a security breach. Rather, research shows that it continues to be a simple human lapse or lack of focus of some kind that makes a system vulnerable. Because of this, the attitude of your employees is as important a part of your security arsenal as the most expensive information security solutions that money can buy.

If a business had no staff, its security would be exemplary. While implementing the right information security systems is important, organisations must also instil the right culture within the business so that employees understand and respect the importance of data security and don't put the organisation at risk.

About the author

Mike Simmonds has dedicated his career to the communication and networking industry. Joining Axial Systems in 2007 as technical director he has been instrumental in developing its technology portfolio and providing customers with networking consultancy and advice. In March 2013 he was appointed managing director of the company.

References

1. 'Cyber Security Breaches Survey 2017'. Department for Culture, Media & Sport, Apr 2017. Accessed Jun 2018. www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.
2. 'Cyber Security Breaches Survey 2018'. Department for Culture, Media & Sport, Apr 2018. Accessed Jun 2018. www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.
3. 'The Threats from Within'. Kaspersky Lab. Accessed Jun 2018. http://go.kaspersky.com/rs/802-IJN-240/images/Threats-From-Within-EDU-Ebook%20FINAL.pdf.
4. 'Productivity, Technology & Working Anywhere'. The Work Foundation, 9 Jan 2018. Accessed Jun 2018. www.theworkfoundation.com/wf-reports/?prod-tech-work-anywhere/.

How to build a secure API gateway

Jason Macy

Jason Macy, Forum Systems

In this era of hyper-connectivity, where almost every app or application relies on communication to a server or database somewhere, it has become harder than ever to secure an organisation's systems, data and business-critical processes. Most of the major technology trends that have shaped IT over the past few decades – such as cloud computing, BYOD, IoT and even social media have resulted in more people and entities connecting to corporate IT assets than ever before.

At the heart of these connections are application programming interfaces (APIs) that underpin almost every interaction or process within this hyper-connected world and have quickly become a prime target for attackers.

Sleeping giant

APIs have quickly become the primary channel for business transactions in most modern enterprises due to the increasingly complex nature of their IT infrastructures, which often consist of a myriad of external partners, public cloud providers, mobile devices and virtualised datacentres. As APIs have become more prevalent, so too have API vulnerabilities. Yet despite their growing prominence, they have largely remained the sleeping giant of our technology-led world. They simply don't raise alarm bells in the same way as other threats and remain the most overlooked threat to information security today.

"IAM is fundamental to any cloud computing architecture because it allows the organisation to control who accesses the APIs and cloud services"

This is a mistake, but one which is beginning to be rectified. The challenge with API vulnerabilities is they are not always easy to spot and often require specialised technology for detection and prevention. In fact, if you looked at the latest version of the OWASP Top 10 (the highly respected, peer-reviewed list of the top vulnerabilities facing organisations today), nine of the top 10 vulnerabilities now include an API component of some kind.[1] This top 10 listing is derived from actual deployments and reported threats and thus clearly demonstrates the need to treat API risks as a critical aspect of a cybersecurity strategy.

Identity concerns

Taking into account the latest OWASP top 10, plus experience in processing over 10 billion transactions per day in mission-critical environments, we can say that there are two specific types of vulnerability that are particularly prevalent today, yet continue to be overlooked.

The first common vulnerability that has only recently begun to be significantly exploited is the weakness in Identity Access Management (IAM) products. IAM is fundamental to any cloud computing architecture because it allows the organisation to control who accesses the APIs and cloud services. Since most organisations are adopting the cloud as part of their digitisation efforts, IAM solutions have become prevalent in most corporate IT architectures.

The risks posed by IAM are being exacerbated further by the growing trend of deploying cloud-based, centralised IAM solutions. As cloud-based systems these solutions present a central point for attacking the architecture by compromising the IAM enforcement points, called PEPs (Policy Enforcement Points). The fundamental issue here is that IAM products are platforms, not cyber-security systems. They were never designed to be cyber-security hardened against attack.

In 2017, a major vulnerability given the highest classification of 'severe' was discovered on the Oracle Access Manager platform, where an attacker could take control of the entire system: it was deemed by NIST as a 10 out of 10 on the CVSS score. An attacked IAM could compromise any identity and impersonate any user. Building a secure IAM solution needs to be able to be done by first ensuring that the PEPs are secure. Without doing this, an IAM will become the weakest and most targeted hacking point into a firm's architecture.

API vulnerabilities

The next common API vulnerability that you won't find in any 'top 10' list is the API architecture components themselves. For example, the API gateway used to control API accesses must not become the target of compromise, yet since this technology centralises API access control and security, these components are the main targets of attack. To protect against attack and compromise, the product must be designed with secure architecture principles such as a locked-down, secure operating system, self-integrity health checks to detect and prevent compromise and independent security certifications that prove claims beyond just those stated by the vendor.

Consider the latest Spectre and Meltdown vulnerabilities that affected any system running potentially vulnerable third-party applications.[2] A locked down OS does not run third-party applications and is therefore not susceptible to this type of vulnerability or any other of its type. Does your API Gateway solution have a secure OS? Having security features in insecure API components is very different from having a cyber-secure API component.

"Unfortunately, as we have found over the past decade, most attacks and vulnerabilities are only discovered when they are widely publicised. But just because you haven't heard about a vulnerability doesn't mean it isn't out there"

As a security topic in its own right, API security and API vulnerabilities are still relatively unknown to most organisations and even many security professionals. Unfortunately, as we have found over the past decade, most attacks and vulnerabilities are only discovered when they are widely publicised. But just because you haven't heard about a vulnerability doesn't mean it isn't out there, it only means the hackers currently don't know about it yet (or worse still, they do know but you haven't detected the breach in your system yet).

Security gateway

API security gateways represent cyber-secure API product technologies which enable the benefits of APIs without exposing them to the risks of API vulnerabilities. API security gateways typically provide three layers of protection:

1. **A secure PEP** to allow secure enforcement of authentication and authorisation of users within any identity management ecosystem. The secure PEP prevents threats and compromise to the most critical aspect of identity management – the actual enforcement of the policies. An API security gateway can interoperate with any identity management infrastructure solution, so it also presents a simple solution to securing identities without requiring rip-and-replace strategies and without disrupting existing business systems.
2. **Real-time protection and monitoring** to proactively monitor and enforce compliant traffic to applications and services and take protective measures if threats are detected. Also, API security gateways can capture advanced heuristics and integrate with machine learning, artificial intelligence and big data analytics to add even more depth and intelligence to your security position.
3. **Cloud and mobile integration** to integrate seamlessly with the broadest possible spectrum of client and server technologies. This is especially beneficial for integrating legacy systems and securing hybrid-computing models where internal systems communicate with cloud systems and mobile devices.

API security gateway technology is heavily deployed in government and commercial enterprises around the world, ranging from telecoms to energy, healthcare, finance, manufacturing, robotics, etc. In most cases, you don't actually know the technology is there because it is meant to be seamless and silently protect and enforce the API communications.

Building blocks

Building a secure API gateway is very different from providing a platform. It requires attention to several layers of the architecture, as described below:

- **The operating system**: The underlying operating system on which the API gateway is running must be security hardened as the first layer of architecture design. This means ensuring no root access, no ability to add third-party software and integrity checks both at start-up and while running to ensure that the system modules have not been compromised.
- **The product architecture**: The architecture of the solution must be security-focused to ensure that administration, policy storage and

sensitive security artefacts such as PKI keys, passwords, etc are encrypted not only when stored locally but also when transmitted to other product instances for policy sharing.
- **Mission-critical stability**: Security and stability must go hand-in-hand and the integrity of a system must be able to sustain high-volume performance and penetration attacks in order to ensure that the system itself is not a target for compromise. This includes hardening of the code paths, hardening of the protocol stack and hardening of the message parsers such as XML parser and JSON parser so that these components are not susceptible to message-based attacks.

In a well-planned architecture, APIs can dramatically accelerate application development, create new revenue opportunities and reduce costs in the modern IT environment.

Proactive checks

But APIs can only deliver these benefits without compromise when this same IT infrastructure employs centralised identity control, security enforcement and proactive business transaction monitoring. Without these checks in place, APIs risk exposing sensitive information or providing unscrupulous actors with unrestricted access to applications and systems. An IT infrastructure built on APIs is extremely vulnerable if security is not embedded throughout the network.

"Leveraging secure product technologies such as API security gateways that are cyber-hardened will dramatically reduce exposure to common and emerging threats"

Given the threats highlighted in this article and the recent examples of the Spectre and Meltdown vulnerabilities, it is important to secure your API architecture using secure API components that are purpose-built to prevent such vulnerabilities.

Security is not easy to build and using solutions that are not secure leaves your infrastructure vulnerable to attack at the very points that you put in place to provide security. Leveraging secure product technologies such as API security gateways that are cyber-hardened will dramatically reduce exposure to common and emerging threats that continue to plague the ecosystems built on platform-based, developer-centric solutions.

About the author

Jason Macy is chief technical officer at Forum Systems (www.forumsys.com), responsible for innovation and product strategy for global operations. He is deeply involved in enterprise architecture design and the deployment of API identity and security technology, with hundreds of deployments worldwide.

References

1. 'OWASP Top Ten 2017 Project'. OWASP. Accessed May 2018. www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project.
2. 'Meltdown and Spectre'. Home page. Accessed May 2018. https://meltdownattack.com.

The need for continuous compliance

Javid Khan, Pulsant

Javid Khan

Compliance isn't a new challenge to business. In fact, it is something that organisations have been grappling with for some time, particularly those in highly regulated industries such as insurance and financial services. However, with the new EU General Data Protection Regulation (GDPR), the need for businesses to remain compliant with increasingly stringent industry regulations has once again come into focus.

Time has now run out. Since May 25, any business that falls foul of a data breach could face a potential fine of €20m, or 4% of annual turnover fines (whichever is greater). Yet recent research by Censuswide, looking at current IT compliance attitudes and practices in the UK, highlighted several areas of concern.[1] Most worrying was that there appears to be a distinct lack of alignment within UK businesses when it comes to managing and maintaining compliance, with almost one in three not knowing which regulatory frameworks they need to align to.

This seems a very laissez-faire attitude. In today's global climate, compliance is a challenge that nearly every business faces. It should no longer be thought of as a simple tick in a box. Nor is it something that should be considered complete the moment it has been achieved. Rather, it should be thought of as an amorphous organism that is continuously changing, and should underpin all business processes.

Change is coming

There needs to be a change of approach when it comes to maintaining compliance, whether that means better tools, more automation or working with a trusted partner to manage the entire process. The good news is that there is overwhelming acceptance that this is the case. The research showed that 83% of IT decision-makers admit there is room for improvement when it comes to the tools and technologies used in managing compliance. The most-cited desired features include real-time alerts, better reporting,

open integration with other compliance tools, and more comprehensive monitoring capabilities.

Achieving compliance should be considered a badge of honour for organisations: after all, it is imperative to the general health and wellbeing of a 21st century business. Being compliant demonstrates to customers, partners, investors and other stakeholders that the business is committed to implementing best practices, whether that is around security, safeguarding data or ensuring privacy. Conversely, the consequences of non-compliance are severe fines and untold reputational damage that translates into loss of revenue.

The simple truth is that becoming compliant is perceived to be a costly exercise that is time and resource intensive as well as highly complex. Achieving compliance and maintaining it may be viewed as two sides of the same coin, but they are actually very different. Moving beyond simply achieving compliance and making sure an organisation remains compliant is a challenge that's discussed in boardrooms throughout the country. Within these fast-moving, digitally transformative times, compliance needs to keep up with shifting market dynamics so that industry innovation can be effectively fostered and new products can be brought to market.

Specialised tools

Due to constantly shifting regulations, businesses today are having to audit their IT compliance requirements on average four and a half times per year, according to our research. Now more than ever, the act of adhering to regulatory requirements requires an ongoing commitment. It also increasingly needs to rely on the use of specialised tools and human expertise to make it more effective and accurate.

While businesses may feel they have the tools and skills to help them deal with compliance, there is room for improvement. Unfortunately, full-time compliance people are costly, as well as difficult to recruit and retain, given the growing skills gap in compliance and cyber-security in the UK market. To plug this gap, businesses often need to look outside of their own four walls and turn to third-party partners to assist them.

The tools, too, need to be fit for purpose. Given that compliance is such a complex and time-intensive task, automating some of the processes can make realising compliance on a continuous basis easier to achieve. It can also reduce the potential for human error and make the entire process more accurate and more efficient.

"Being compliant demonstrates to customers, partners, investors and other stakeholders that the business is committed to implementing best practices"

As digital transformation has continued to take hold across multiple industries, businesses have grown to contain a whole host of data that is siloed across different departments, with no coherent 360-degree unified view. Today, the big data mountain is understood to have reached five zettabytes and the volume of data shows no sign of slowing, especially with the Internet of Things (IoT) becoming more ubiquitous than ever. With the sheer amount of data being produced, it is becoming difficult to see the forest for the trees. This makes obtaining the information required to become and remain compliant a far from streamlined exercise and opens up the potential for mistakes.

Becoming agile

Compliance is critical for businesses. A lack of compliance affects the bottom line, stakeholder trust and, in some industries, can stop an organisation from operating altogether. As a result, it is a task that many, if not all, organisations are tackling.

Only when businesses change their mindset to one of attaining compliance on a continuous basis can they capitalise on all the benefits that cloud and new technologies actually deliver. Continuous compliance leads to a level of agility that enables a business to be able to compete effectively within marketplaces that continue to shift faster and more frequently than ever before.

Easing the strain

While many organisations are not sure what regulations they need to adhere to, at least there is a shift towards wanting to ensure they do remain compliant and avoid potentially crippling fines. Yes, managing and maintaining IT compliance can be time-intensive and complex, but by using the correct tools and technologies to automate at least part of the process and leaning on third party experts, the strain can be somewhat eased.

This emerging regulatory technology (RegTech) sector is playing an increasingly important role in supplying organisations with the advanced solutions needed to meet their fast-growing compliance needs. While focused largely on the financial services market, RegTech has the potential to become a much needed helping hand for any business, especially as the regulatory world becomes more crowded and complex with the likes of the GDPR.

As there is a move towards continuous compliance, there is a definite need for the process of both achieving and maintaining compliance to be optimised, streamlined and made more effective. The use of smarter and more intuitive tools and technologies, along with automating processes, will enable organisations to gain the benefits they are seeking, such as real-time alerts, better reporting and bringing all data sources together. Going forward, there will be increased demand for this type of technology that can optimise the compliance process, both from a management and maintenance point of view.

About the author

Javid Khan is CTP of Pulsant (www.pulsant.com) where he uses his experience of building multiple global private clouds and delivery of several £50m-plus infrastructure implementations to bring enterprise best practice to the organisation's delivery capability.

Reference

1. 'The State of IT Compliance – exploring the attitudes and approaches to the compliance challenge'. Pulsant. Accessed Jun 2018. www.pulsant.com/knowledge-hub/report/the-state-of-it-compliance-exploring-the-attitudes-and-approaches-to-the-compliance-challenge/.

Friendly fire: how penetration testing can reduce your risk

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, Network Security

To get an accurate idea of how secure your systems are, you need to put them to the test. Yet even though penetration testing is a long-established means of doing this and is even mandated in many industry sectors, it remains severely underused. In this interview, Dave Adamson, head of technology at EACS, explains some of the reasons for this and how organisations could exploit testing to reduce their risk.

Part of the problem, Adamson believes, is a slightly negative image that some people have of pen-testing. "It still is something that's viewed as almost a necessary evil for ticking boxes around compliance and governance processes, in demonstrating that businesses have done the right thing because they have to, rather than necessarily having it embedded within the DNA of their multi-layered security strategy," he says. It's treated as a kind of 'fire and forget' exercise, he adds, with organisations thinking: "We're required to do a test in whatever time period – maybe once a year – so we do it, we deal with the actions from it, and we forget about it for 12 months, until it comes around again."

Dave Adamson is head of technology for EACS (www.eacs.com), bringing more than a decade of technical experience as an IT professional to the position. Over the course of his career, he has acquired expertise in a wide range of disciplines, holding accredited qualifications in technology platforms including Microsoft, VMware, Nutanix, Citrix and Sophos. Adamson joined the EACS team in 2015 as a solutions architect and pre-sales team leader before progressing to head of technology in 2017. Before beginning at EACS, he held IT and management roles at several companies including Norwich Union, Itim Group and Blue Chip.

Minimum effort

Most penetration testers will tell you that it's not uncommon for clients to ask for a pen-test only for it to emerge during discussions that what they actually want is a much less probing vulnerability scan. Sometimes this is because the company is only interested in – as Adamson put it – 'ticking boxes' to fulfil its compliance requirements. And sometimes it's because it is scared of messing with the IT on which the business depends. But Adamson thinks these attitudes are starting to shift.

"The rise of security events that target the individual as well as the infrastructure – so things like phishing and whaling and those types of attacks – and more identity and application-focused threats, is starting to cause a bit of a shift in our customer base," he says. "They are starting to take it a bit more seriously, not just take the easiest option."

Adamson would suggest – and clients are becoming more receptive to – a blended approach to IT infrastructure, including applications, networks and people. Sometimes the discussion starts with the client wanting the bare minimum, says Adamson, but as the organisation's understanding of the issues matures, so does the approach to pen-testing.

The mention of 'people' in the mix is interesting, given the frequency with which social engineering attacks such as phishing turn up in breaches. Often, the first step in a targeted attack is a phishing email designed to lure an employee into giving up credentials. This has led to a rise in testing services in which simulated phishing attacks play an important role. However, Adamson doesn't see much in the way of really targeted phishing attacks – spear-phishing or whaling – taking place among the organisations with which he engages.

"It's more around mass attempts at credential harvesting from infected emails, and hoping to strike lucky," he says. If there is a directed attack against individuals, he adds, "we tend to find that comes as a secondary phase after the initial breach has occurred, and the attackers have gathered a bunch of information from a wide-ranging attack. They then identify an interesting target from it and then go around a second time to do a more targeted approach for some of the more high-profile people in the organisation."

Technical exercise

It's inevitable that many people regard securing technology as itself a purely technical exercise. But this can be a mistake.

"People are the weakest link," says Adamson. "But people see attacking the problem as a technical solution rather than a people solution. It's the path of least resistance. So we see a rise in people taking up technical solutions to help arm them against social engineering or identity-type issues, but they do those in preference, rather than necessarily as a complementary strategy, to educating the end user. We do have a number of customers who are more mature in their outlook and do take that more holistic approach to security, but it's not the de facto option by any stretch."

Rather than seeing pen-testing and security training as separate issues, Adamson believes there is much to be gained from linking them.

"IT security around infrastructure was always a slightly ethereal thing that the technical guys in the organisation knew was something they should do, but they struggled to sell it upwards"

"The fact that people are the weakest link and the rise of phishing and similar types of attacks in recent years have allowed senior leaders in organisations to ascribe direct commercial value to the risk," says Adamson. "IT security around infrastructure was always a slightly ethereal thing that the technical guys in the organisation knew was something they should do, but they struggled to sell it upwards, to release the budget into IT for focusing specifically on security. But as you start to see CFOs, CEOs, senior leaders in organisations being targeted with highly reported breaches and directly relatable incidents that they can understand, there is starting to be more money made available to look at the cultural and social impact, to educate the user community. However, it's a big shift to turn around, particularly in longstanding, privately run organisations, rather than those who are perhaps publicly listed and need a more publicly defensible posture around security."

Driving uptake

More and more businesses are finding themselves subject to regulations or demands by B2B customers that require them to undertake pen-testing on a regular basis. However, even outside that group, Adamson says he is seeing an uptake, albeit slight, of pen-testing services and he puts this down to the constant flow of data breach stories in the headlines.

"We are now seeing breaches being reported on the front pages of newspapers, and in headline articles on the TV news, so even for those who aren't going looking for IT security information, it's starting to permeate into the consciousness a bit," he says. "And perhaps it's making people look at whether they should be doing a bit better than they are today."

While this might help sell business executives on the idea of spending on security, how do you convince them that penetration testing is an essential part of that? A bright, shiny box, such as a firewall or IDS system, looks like an investment. A pen-test can feel more like an administrative overhead.

If the EU's General Data Protection Regulation (GDPR) results in the kinds of fines people are expecting, that could act as a spur too, reckons Adamson. But in any case it has got some people thinking about their attitudes to security.

"It's about at least obtaining a defensible position," he says, "so that if you do get breached, you can demonstrate to the regulatory bodies that you were taking reasonable steps and that you're able to report breaches in a timely manner and so on. Penetration testing is one of the tools in the armoury, to show that you're at least taking IT security seriously."

That said, there are still many organisations – particularly in the small and medium-size enterprise (SME) sector – that aren't aware that penetration testing is even available.

"They don't have dedicated security heads and perhaps they're in certain industries that aren't that technical in nature," he says. "I don't think people really understand what penetration testing is – that it can be multi-layered and multi-faceted in its approach. It probably still has a reputation as being about poking around in firewalls, seeing if you can get in from the outside, and checking firmware revisions and so on, rather than anything at the application layer or the people layer, or even the physical security of the environment."

Expectations

Once people know what a penetration test is and have come to the conclusion that they need one, what expectations do they have? Larger organisations tend to have a clearer idea of what's involved and what they can get out of it, But further down the size scale, the picture isn't so clear.

"In SME land, they probably don't understand vulnerability scanning, wouldn't understand necessarily what a CVE is and those kind of things," says Adamson. "I don't want to unfairly tarnish SMEs, as we've got some very security-conscious ones, particularly those that are small businesses but high value. But I think an understanding of what's available is patchy, frankly."

There's also the question of what to test. For example, it's not uncommon for certain operational systems to be off-limits simply because the business can't risk having something bad happen to them. But there are more nuanced questions to ask about what really needs to be examined.

"As with most IT matters, there's the fitting-to-budget element, so it tends to be quite a consultative process," says Adamson. "It'll start with somebody making contact to ask if they can have a conversation with you about security. They either know they need to do a penetration test because they're being told they need to do one, or they've heard about it and want some guidance."

The requirements are different for every organisation and every industry, he adds: "There are many organisations that need or wish to do the bare minimum, tick the box and get away with it, through to those who want to be quite rigorous."

The consultation includes finding out where the organisation perceives its greatest risks are – and perhaps challenging those perceptions. For example, having experience of penetration testing

Common issues

Inevitably, penetration testing organisations encounter the same issues time and again. One of the most common is patching.

"Manufacturers have their own cadences for releasing patches that mitigate against vulnerabilities that are discovered," says Dave Adamson. "There are not that many organisations running a 100% tight ship on that front, for whatever reason. And in some situations there are organisations that are prepared to take the risk on a particular technology – the much-derided Java, for example and its well-known ability to only work with in-house applications at certain levels. If there's a vulnerability in that Java version, that could expose you to something with a degree of risk. But the cost to the business of redeveloping applications to work with later versions is disproportionate to that risk."

If an organisation is smart – or if it is compelled by regulation or contractual terms – it will repeat the pen-test at regular intervals. And pretty much every pen-tester will tell you that they will find the same problems on the next test that they reported in the last one. This suggests that organisations are often failing to act on the warnings they are being given – failing, in fact, to reap the benefit of the pen-test. But the situation is sometimes a little more complicated than that, says Adamson.

"It depends what vulnerabilities have been discovered," he explains. "There are those that are very easy to mitigate and typically they are simple for an organisation to either carry out themselves or to find a small amount of IT budget on an operational basis to deal with those issues. Those that are much larger in scope, in terms of the remediation activity, tend to be a little bit harder to see through for people. So we do come back and find the same thing year on year. And in some organisations, there's an attitude that if it hasn't caused a problem for the past 12 months, why should it cause a problem in the next 12 months?"

with other organisations in the same area, Adamson says it's not uncommon to be able to alert customers to vulnerabilities they may never have considered. The engagements also vary in terms of how the penetration testers go about their work – from complete black box tests where the testers have no inside knowledge of the organisation and have to approach it in much the same way that a hacker might, through to organisations that are already quite confident about their security and will share details so that the pen-testers can independently assess the quality of the security.

This might mean testing specific parts of the IT environment. A classic case is an organisation where the networks are split into back-office IT and operational technology (OT). The OT side might be off-limits because the organisation is already confident in its robustness and only the IT side is in need of scrutiny.

Alternatively, an organisation might want to test its 'crown jewels' systems – those that are most critical to generating revenue, such as an e-commerce system that is an intrinsic part of the brand. Less critical systems are deemed unworthy of the expense and potential disruption of a penetration test.

Testing the limits

It's important to be realistic about what penetration testing can achieve. For a start, the testing itself is going to come up against some limitations.

"There are the technical and risk-based limitations around the ability to provide authenticated versus unauthenticated testing," explains Adamson. "Clearly you're going to get different results if you enter into an infrastructure as a privileged user as opposed to an unprivileged user."

Some of the biggest barriers Adamson encounters are operational ones. For example, in an engagement where the customer wants an authenticated attack, obtaining the information necessary to do this isn't always easy. Similarly, when targeting specific systems, and where the test might carry some risk to the system's uptime, obtaining the necessary maintenance window in which to perform the test can be tricky.

Relating to risk

It's rare for pen-testers not to find an issue of some kind – Dave Adamson couldn't think of an example – although not every problem carries a high risk. But that does raise the issue of assessing risk: how do you relate vulnerabilities or issues discovered during the pen-testing process to risks to the business? Is this the job of the pen-tester or is it down to the organisation itself, because it will depend on its precise nature? Adamson thinks it's a bit of both.

"What they look for in a penetration testing partner is a consultative and advisory approach that helps them interpret the risk, particularly if it's a non-technical audience, or an organisation that's used to running IT outsourcing and doesn't have an internal IT function to interpret the results," he explains. "They need to have trust in the people who are providing their results, to help them make sensible and informed decisions about any remediation."

Even if everyone is on board and the necessary co-operation is forthcoming, a penetration test isn't necessarily going to tell you everything about your security.

"Setting expectations in terms of what can be achieved is important at the beginning of the process," says Adamson. "Also, it's very important that people don't come away from the penetration test thinking 'job done'."

This is a crucial point in this era of fast-changing, agile IT – much of it cloud-based. An organisation that is exploiting the flexibility of infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS) solution will find that its IT environment is constantly changing, often in ways that are beyond its control.

"It's a dangerous game to assume that a point-in-time test is going to guarantee your safety one month, three months, six months down the line," says Adamson.

This also means that there are areas of IT that you simply can't test. For example, while IaaS solution providers may

allow you to pen-test (with notice) the virtual machines you have spun up in the cloud, this only applies to the infrastructure to which you have direct access.

"Any attempt to penetration test the lower layers and you come up against the defence teams of that organisation and will be shut down as a consequence," explains Adamson. "That brings with it the risk that your workloads are shut down which, if they are revenue-generating or customer-facing, is not something you should enter into lightly. For those who are living in the public cloud world, the importance of penetration testing shifts a little bit away from infrastructure and up into the application layer. If you're an organisation spinning out applications and workloads in a much less controlled manner than has traditionally been the case, then the danger of leaving things lying around, of unsecured APIs, of developers not understanding the network layer and so on, brings its own fresh set of dangers. Looking at technologies that can help test and indeed mitigate against the exposure of APIs and public networks in public cloud and software as a service offerings is something that we'll see quite a big shift towards in the coming years."

Making the most

Given that penetration testing has so much to offer an organisation in terms of improving its security, is it being underused? Adamson certainly thinks so.

"I would encourage people to make use of penetration testing not as the only tool in the kitbag in terms of IT security but also to assess what their exposure and risk level are, and indeed their risk appetite as an organisation," he says. "If you look simply at the differences between internal and external penetration testing, if you're an organisation that doesn't have much of a public presence when it comes to network or Internet-type activities and you only elect for an external penetration test on your firewall, then you're probably not going to identify the areas of highest risk in your organisation. If the firewall is locked down and there's nothing of interest inside it, but the front door's open and you can litter USB sticks in the car park and unleash malware that way, then that's probably not making the best use of the penetration-testing strategy."

"Having a skilled and educated IT team, particularly one with a security focus, and perhaps even an internal security team, is a really good thing for organisations to do. That being said, there's nothing quite like somebody else marking your homework"

There are many organisations, particularly SMEs, that still don't have formal IT security strategies. So would a penetration test be a good way of establishing a baseline concerning vulnerabilities and act as a starting point for developing security policies?

"It's a good point-in-time snapshot, a sort of current state assessment, if you like," says Adamson. "But if an organisation is heading off on that IT security journey, I would encourage them to not necessarily start with a penetration test but to seek some advice and guidance from a security partner, to help them develop a security strategy and perhaps a strategy towards remediation. It's highly likely that a penetration test will be a great way of finding an initial set of information about areas to prioritise first. But I think there's a danger that doing that in isolation allows you to ignore other areas."

Another potential application is when an organisation is developing, say, a new line of business or has established a new department. Would a pen-test be a useful part of the development activity?

"It should form part of the strategy when undertaking that business development or product development," says Adamson, "for two reasons: one, to make sure that what you're building is secure by design and two if that new venture or new function links back to an existing function in some fashion. It may be that your new development introduces vulnerabilities that didn't exist previously. If you connect two organisations together and punch some holes in some firewalls to do so, you're perhaps generating a new attack vector that wasn't there previously. So as part of that product development or business development cadence, I think that's an excellent idea."

And what about those organisations that, having concluded they need to perform penetration tests – or at least vulnerability scans – decide on the 'do it yourself' approach rather than hiring specialists?

"Having a skilled and educated IT team, particularly one with a security focus, and perhaps even an internal security team, is a really good thing for organisations to do, assuming it fits with their overall organisational structure," says Adamson. "That being said, there's nothing quite like somebody else marking your homework."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security and its sister publication Computer Fraud & Security.

The Firewall

Streamlining data discovery

Colin Tankard, Digital Pathways

Understanding what unstructured data exists in the enterprise is not easy. Massive volumes of documents, spreadsheets, presentations and emails are typically scattered about the organisation.

With no real tools to manage it based on business value, it accumulates with no end in sight. The easy option is to buy more storage but that doesn't fix the problem. Continue and you have hundreds of terabytes or petabytes of unstructured user content, with no way to classify and manage the data according to its value. But by breaking it down into multiple iterative steps, starting high and working down to a level of detail to satisfy all stakeholders, order can be achieved.

Unstructured files are 'chock full' of valuable metadata that sheds light on content, providing a level of knowledge lacking on enterprise storage platforms. Even if your storage vendor provides a tool to make sense of the data, it wouldn't have the ability to provide knowledge across such a large scale of disparate storage platforms. This is where different techniques are required to analyse the metadata, file by file, and separate it into categories.

Categories can be based on a wide range of criteria and can use standard dictionaries as well as custom language to meet even highly specialist data sets such as those used in the medical profession. Very quickly, after the process starts, a deeper understanding is gained of what is stored and this level of insight can be used to generate comprehensive reports and analysis, modify the search categories and sift data further.

Using metadata, when combined with Active Directory classifications, you can easily gain deeper knowledge of what exists on the network and classify it by department or down to individual owner. It is important to understand that these metadata fields can be queried and reported on using a dynamic and iterative process.

Once data is classified and managed using policies, it can be managed and migrated depending on business needs. Based on an organisation's policy, specific files or emails can be archived and preserved, even adding custom retention policies on data, to support the organisation's governance initiative.

As disposition of the data is performed, logs are maintained detailing the date and disposition, including the user who executed the disposition, enabling secure execution of defensible deletion, migration and archiving policies.

It is important to link other actions to the discovery of the data to add protection and allow time for deeper research to be undertaken. A first step is to move the sensitive data to a location that can automatically encrypt the data.

Furthermore, this data can be automatically scanned to understand the content wording and appropriate classification added. For instance, company IP data could be classified 'top secret', controlling who can access the data and what can be done with it. A benefit is that such data can be controlled if it is to be emailed, as the classification will prevent such data from going to non-company email accounts and, also, only to users of the correct level of authority.

Discovering data is always a huge task, often resulting in further work. By using an integrated approach to discovering, classifying and protecting data, based on automated tools, the workload can be greatly reduced. It can streamline the process, allowing for the final decisions on what to do with the data to be given to a wider audience, thus relieving the burden for IT and legal departments.

EVENTS CALENDAR

1–4 July 2018
International Conference on Cybercrime and Forensics
Penang, Malaysia
www.apatas.org/icccf-2018/

2–6 July 2018
OWASP AppSec EU
London, UK
https://2018.appsec.eu/

5 July 2018
Applied Cryptography and Network Security
Leuven, Belgium
www.cosic.esat.kuleuven.be/events/acns2018/

7 July 2018
Steelcon
Sheffield,UK
www.steelcon.info

19 July – 23 August 2018
IEEE Cyber 2018
Tianjin, China
http://ieee-cyber.org/2018/

20–22 July 2018
Hackers on Planet Earth (HOPE)
New York, NY, US
https://hope.net

25–27 July 2018
RSA Asia Pacific & Japan
Marina Bay Sands, Singapore
www.rsaconference.com/events/ap18

1–3 August 2018
IEEE International Workshop on Cloud Security and Forensics
New York, NY, US
http://bit.ly/2JuhQq7

4–9 August 2018
Black Hat USA
Las Vegas, US
www.blackhat.com