ELSEVIER

network
SECURITY

ISSN 1353-4858 June 2017
www.networksecuritynewsletter.com

Featured in this issue:

Fighting application threats with cloud-based WAFs

Companies that conduct business online must ensure that their web applications and APIs are protected from attack. However, defending an online operation is no mean feat.

Whichever route a company takes to protect itself, what is clear is that any web application firewall (WAF) must itself be constantly evolving and gather the intelligence needed to protect against application layer and DDoS attacks – and to do it with great speed and scale, says Daniel Shugrue of Akamai Technologies.

Full story on page 5…

GDPR: a milestone in convergence for cyber-security and compliance

One of the greatest misconceptions in business today is that compliance equates to good business practice – particularly with regard to security.

Cybercrime is evolving at an exceedingly rapid pace, meaning it is often difficult for regulations and legislation to keep up with a changing security landscape. The EU's General Data Protection Regulation (GDPR) presents an opportunity to level the scales and drive greater convergence between cyber-security and compliance – two areas often seen as disparate by business leaders, explains Jesper Zerlang of LogPoint.

Full story on page 8…

How automating data collection can improve cyber-security

The fallout from a data breach can be catastrophic. And hackers have become better at developing smarter, better targeted and more automated tools that help them fly 'under the radar'.

Security analysts need tools and processes that enable them to work much more efficiently, especially for real-time analysis. And the storing of alert-related packets allows specialists to look for so-far undetected breaches. The security industry needs to develop automated processes that automatically collect relevant 'suspicious' packet data and make it readily available for analysis, explains Jay Botelho of Savvius.

Full story on page 11…

NSA leak shows Russian attack on US electoral system

A document leaked from the US National Security Agency (NSA) shows that Russian hackers had some success in attacking 122 election officials and a vendor of voting software prior to the 2016 presidential election.

Rumours about Russian attacks started circulating in September 2016. But even the one publication to fully report on them – *The Intercept* online magazine which regularly runs material from whistleblowers – said it had not previously seen the NSA documents. (It has since published a story based on them, available here: http://bit.ly/2skBHUc.)

Continued on page 2…

Contents

NEWS

FEATURES

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: smd@contrarisk.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

The NSA report squarely points the finger for the attacks at Russian military intelligence, particularly the General Staff Main Intelligence Directorate (GRU), and that the hackers were members of a team with a "cyber-espionage mandate specifically directed at US and foreign elections".

According to excerpts from the document published by *The Intercept*: "Russian General Staff Main Intelligence Directorate actors … executed cyber-espionage operations against a named US company in August 2016, evidently to obtain information on elections-related software and hardware solutions. … The actors likely used data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting US local government organisations."

The attackers first targeted an e-voting system vendor. The company is not named in the NSA document but there are other references to Florida-based VR Systems whose voting solutions are used in eight states. The attack used a Microsoft Word document containing malware.

The spear-phishing campaign against local government employees involved sending emails purportedly coming from the e-voting system vendor and containing links to a fake Google page.

The NSA document was allegedly leaked by Reality Winner who had served in the US Air Force before joining a company that works for the NSA as a contractor and who has now been charged with offences that could result in a 10-year jail term. She had already served at the NSA's headquarters in Fort Meade as a cryptologic language analyst. It's alleged she printed a copy of the NSA document and that the agency's printer logs helped identify her.

Attacks on industry

Although the majority of industrial organisations believe they are well-prepared for cyber-security incidents, around half of firms using industrial control system (ICS) technology experienced between one and five incidents last year, according to research by Kaspersky Lab, and 4% experienced more than six. Meanwhile, a major new threat has emerged.

On average, ineffective cyber-security costs industrial organisations up to $497,000 a year. Companies are struggling with the challenges raised by the convergence of IT and operational technology (OT) and the availability of industrial control networks to external providers. Despite high awareness about new threats such as targeted attacks and ransomware, the biggest pain point for the majority (56%) of ICS organisations is still conventional malware.

There is a mismatch surrounding employee errors and unintentional actions, which are far more threatening to ICS organisations than actors from the supply chain and partners, and sabotage and physical damage by external actors. Yet it's the external actors that are in the top three of what ICS organisations worry about the most.

On the positive side, the security strategies adopted by ICS practitioners look quite solid. The majority of companies have already given up on using air gaps as a security measure, and are adopting comprehensive cyber-security solutions. In the next 12 months, the surveyed firms plan to implement industrial anomaly detection tools (42%) and security awareness training for staff.

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

Researchers at ESET who have examined a piece of malware they have dubbed 'Industroyer' say it is capable of attacks such as the one that brought down part of Ukraine's power grid in December 2016. In fact, it's possible that attack was a large-scale test of the malware.

According to ESET: "Industroyer is a particularly dangerous threat, since it is capable of controlling electricity substation switches and circuit breakers directly. To do so, it uses industrial communication protocols used worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure systems (such as water and gas)."

In addition, the malware is capable of data wiping and its modular design means it can be repurposed for a wide range of attacks against critical national infrastructure. There is more information here: http://bit.ly/2rq4Ng0.

In brief

WannaCry payments

According to Elliptic, a company that monitors the use of Bitcoin in illicit activities, by 12 June 2017 the WannaCry ransomware campaign had made just over $142,000 for the criminals running it. Most of the payments had been made by mid-May. While WannaCry hit organisations and individuals around the world and attracted huge press attention, the malware turned out to be flawed – not least because it contained a 'kill switch' option that was triggered when a security researcher registered a domain name hard-coded into the software. The malware also contains a number of other coding errors that make file recovery possible in some circumstances. There's more information at SecureList here: http://bit.ly/2s5wMDq.

Healthcare breaches

The healthcare sector accounts for just under half (43%) of all data breaches in the UK, according to figures obtained from the Information Commissioner's Office (ICO) by security firm Egress. Between January 2013 and December 2016, healthcare organisations suffered 2,447 incidents and consistently led all other sectors in the number of breaches. And the number of incidents rose year on year, with a 20% increase, from 184 incidents in the last quarter of 2014 to 221 in the last quarter of 2016. However, most of the data leaks were the result of accidents and incompetence rather than external threats. Taking the 221 breaches that occurred between October and December 2016, the top-ranking incident types included: theft or loss of paperwork (24%); data faxed or posted to incorrect recipient (19%); data sent by email to incorrect recipient (9%); and failure to redact data (5%). However, Egress warns that while healthcare had the highest volume of incidents, other sectors are increasing more rapidly. Across all sectors, the total number of security incidents reported has increased by almost one-third (32%) since 2014. The courts and justice sector has experienced the most significant increase in incidents – a 290% hike since 2014, placing it in the top five worst affected industries by the last quarter of 2016. Other significant increases can be seen in the central government and finance sectors, with 33% and 44% increases, respectively. The human element, where internal staff made mistakes, accounted for almost half of total data breach incidents, ranging from 44% to 49% in the period studied. And data shared accidentally is the single highest contributor to breaches resulting from human error, causing roughly one-third of incidents.

Swift profits down after hack

The Swift interbanking network has seen its profits drop by nearly a third as a result of a major breach in early 2016 in which nearly $82m was stolen. Using a combination of malware and a knowledge of Swift processes, the criminals were only just prevented from stealing close to $1bn from the Bank of Bangladesh. Most of the money they did steal was never recovered. There were other attempts in 2016 using similar techniques which led to the Bank of England launching a review of the system. Greater investments in security by Swift are a large part of the reason for pre-tax profits (which are disbursed as rebates to owner-members) falling 31% to €47m.

IoT security standards

The EU's information security organisation ENISA is urging the tech industry to develop and adopt security standards for Internet of Things (IoT) devices. A report, produced in collaboration with semiconductor firms Infineon Technologies, NXP Semiconductor and STMicroelectronics, highlights the failure of industry so far to harden IoT products against hacking and malware. With malware campaigns, such as Mirai, now targeting unprotected IoT hardware, this could lead to an erosion of trust in the market as well as allowing for further outbreaks of ransomware, denial of service attacks and other forms of criminal activity that could harm consumers. ENISA says that standards are required so that devices can come with a 'trust label', helping to steer customers to secure products and raise confidence. The report is available here: http://bit.ly/2rdlw6N.

FBI dark web probe in danger

Large amounts of evidence gained during an investigation into child abuse imagery shared via the dark web may become inadmissible in court following a judge's ruling that the FBI misused a warrant. The agency took over a dark website called Playpen which then acted as a honeypot and placed tracking software (acting much like malware) on any PCs connecting to it. During the 13 days of its control by the agency, Playpen recorded the IP addresses and other data belonging to more than 8,000 computers. This led to the arrests of nearly 900 people worldwide. However, in one of these cases – that of Terry Lee Carlson from Minnesota – a federal magistrate judge in Minneapolis said that evidence seized in Carlson's home, including data on hard drives, should be suppressed. This is because the warrant that allowed the FBI to gain access to information on computers visiting Playpen doesn't have jurisdiction outside of Virginia, where it was issued. Magistrate Judge Franklin Noel also ruled that the warrant doesn't allow for the seizing of data and described the FBI operation as "misconduct".

Worst year ever

If the current trend in data breaches keeps up, 2017 is on track to be the worst year ever. The first three months have set records, with more than 1,250 breaches resulting in the exposure of 3.4 billion records. The figures come from the 'Q1 2017 Data Breach QuickView Report' from RiskBased Security. One particular trend noted by the report is cyber-criminals using data stolen via phishing attacks to fraudulently file W-2 tax forms in the US to claim rebates. Business email compromise (BEC) has also seen a sharp rise. And there has been an increase in the sale of large datasets of stolen information on underground markets. The report is available here: http://bit.ly/2s6i4fD.

Vulnerability disclosure

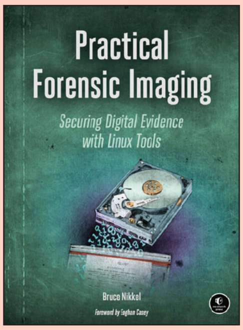
Threat intelligence company Recorded Future says that three-quarters of software vulnerabilities are publicly disclosed – on blogs, social media, code-sharing sites and underground forums – before they make it into NIST's centralised National Vulnerability Database (NVD). This is based on the firm's study of over 12,500 Common Vulnerabilities and Exposures (CVEs). This is making organisations vulnerable to exploits that leverage these vulnerabilities if the firms rely on just the standard published sources to assess their exposure. Additionally, the vulnerability content available on the dark web illustrates that the criminal community is actively monitoring and acting on the broad set of sources where vulnerability information is initially released, says Recorded Future. The median lag between public disclosure and publication on the NVD was seven days. This time lag also significantly differs between vendor announcements and NVD publishing, with the fastest vendor having an average delay of one day and the slowest 172 days. Some 5% of vulnerabilities are detailed on the dark web prior to NVD release and these have the highest severity levels. There's more information here: http://bit.ly/2sx7noP.

Mac ransomware

Ransomware is now available for Apple's macOS platform, although the standard doesn't appear to match the many varieties found on Windows. Security firm Fortinet said it has seen MacRansom being offered as 'ransomware as a service' so that would-be cyber-criminals can simply sign up via an online portal stating the ransom they want to extort from victims and the time and date they want the malware to take effect. The creators will provide samples and even offer a demonstration video. There's more information here: http://bit.ly/2rWiLtv.

Reviews

BOOK REVIEW



Practical Forensic Imaging

Bruce Nikkel.
Published by No Starch Press.
ISBN: 978-1-59327-793-2.
Price: $49.95, 320pgs, paperback.
E-book edition also available.

Digital forensics have come a long way. But then so has technology, meaning that forensic examiners face ever-more complex environments in which digital evidence must be preserved and analysed.

This used to be so much easier. There was a time when police officers, say, could haul away a suspect's floppy disks and examine them at their leisure. (Although I know of one instance in which said officers seized a suspect's twin-floppy PC but left the disks behind.)

Today, forensic practitioners are faced with devices that are rarely switched off. And the complex operating systems they run are constantly making invisible changes – reading and writing data in the background, updating parameters and refreshing state. And this presents a challenge for the forensic examiner who wants to make a copy of the target machine's data and be able to say – in court, if necessary – that the copy is a true representation of the condition of the machine and the data on it at the time of seizure.

One of the key steps in digital forensics is acquiring an image of the machine's persistent storage – hard disks, solid-state drives, memory sticks and optical storage – as a means of preserving evidence. (Copying the contents of memory is also, and increasingly, a critical step but beyond the scope of this book.) Tools for achieving this have been with us for a long time but most of them – such as the EnCase range – are typically very expensive, proprietary solutions.

As is so often the case, open source software provides a low-cost alternative, and that's Bruce Nikkel's focus here. He explains how to use the Linux platform and a range of readily available tools to acquire and secure digital evidence. As the title suggests, it's a hands-on procedural guide – a 'how to' manual, if you like – with pretty much all of the action taking place on the command line.

If working only with command-line tools makes you think that the techniques described here might be limited in scope, think again. For one thing, as Nikkel points out, many of the platforms that investigators face today are embedded or single-board systems such as the Raspberry Pi, where working on the command line is the only option available. The book also tackles many of the latest interfaces and technologies, such as NVME and Sata Express, Thunderbolt, hybrid SSDs and more.

As is usual with this kind of book, it starts with describing how to set up your platform with all the necessary tools and how to go about planning and preparing for a forensic examination. From that point on, though, it's possible to treat this as a workshop manual, dipping into the bits you need to perform specific tasks.

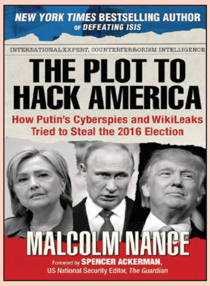
There's plenty that isn't covered here – enterprise-class storage, proprietary devices, cloud data and so on. But the book does cover the most common platforms and in a very accessible way. That approach and the fact that the books revolves around low-cost tools, is significant because the need to acquire forensic data now extends beyond law enforcement agencies and the forensic specialists that support them. For example, security practitioners within enterprises now find themselves having to do far more forensic investigation (if they ever did any in the first place) as a result of the sheer number of attacks and breaches that are occurring. While Nikkel has partly aimed the book at existing forensic practitioners who want to hone their Linux command-line skills, he had also targeted systems administrators and incident response teams who may not previously have carried out this kind of work.

It's commonly said, these days, that you should assume the bad guys have already breached your networks. The ability to carry out forensic examinations is one of the key skills you'll need to respond to that. This book is a solid introduction to acquiring those skills.

For more information, go to: http://bit.ly/2sT6t3o.

– SM-D

BOOK REVIEW


NEW YORK TIMES BESTSELLING AUTHOR OF DEFEATING ISIS
THE PLOT TO HACK AMERICA
How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election
MALCOLM NANCE

The Plot to Hack America

Malcolm Nance. Published by Skyhorse Publishing. ISBN: 9781510723320.
Price: $18.99, 216pgs, paperback.
E-book editions also available.

Any doubts about whether Russia really did attempt to meddle in the 2016 US presidential election are rapidly evaporating. Although attribution for actions in cyberspace is tricky, the evidence is being piled high. So Malcolm Nance's book is a useful summation of what was known at the time he wrote it.

But there's a problem with this type of book. It was rapidly rendered out of date. The main part of the book was written before the result of the election was known. And there have been several important developments since, such as the leaks by Reality Winner and the ongoing congressional investigation.

This book has all the hallmarks of something dashed out to exploit public interest in a hot topic. It's not just that there are frequent typos and repetitions, with the same information often being restated within just a few paragraphs; the book also fails to frame the issues in a coherent way. Nance is an intelligence community insider and so presumably has a good grasp of the concepts (although his explanations of some things, such as waterhole attacks, are dubious at best and suggest that even he doesn't understand them fully). However, in rushing through the story, the author often fails to convey the full significance of some aspects.

In the end, this book lacks depth and real analysis. It's already well behind this constantly unfolding story. And the structure is somewhat chaotic. It does, nonetheless, offer a handy précis of the situation up to a point in time and manages the occasional insight, particularly in terms of how the Russian intelligence services operate.

For more information, go to: http://bit.ly/2rgOQNQ.

– SM-D

Fighting application threats with cloud-based WAFs

Daniel Shugrue

Daniel Shugrue, Akamai Technologies

Companies that conduct business online must ensure that their websites, web applications and APIs are protected from attack. They understand that any vulnerabilities, however small, could render not only their site, but also their applications unavailable for use by customers, staff or partners. They also understand that vulnerabilities provide a doorway for hackers that can lead to the exposure and loss of sensitive data, such as personal information entrusted to the company by customers, or confidential documents.

As we have seen in the media, this can lead to reputational damage, loss of brand confidence and millions of pounds of lost revenue or regulatory fines. At the time of writing, financial services company Wonga has become the latest UK victim, with a reported 270,000 customer details stolen. When TalkTalk was hacked in 2015 to the tune of 150,000-plus customer records, it later received a fine of £400,000 from the Information Commissioner's Officer (ICO), but the company admitted the breach has cost it over £42m.[1]

However, protecting an online operation is no mean feat, regardless of its size, market or location. There are three main reasons for this: first, the availability of automated tools and knowledge among the hacking community means that it is easier, quicker and cheaper than ever before to launch an application layer (or other) attack against an organisation. Second, the ubiquity of bitcoin has made 'cashing out', formerly the most difficult part of an online fraud operation, relatively easy.

The other significant change is the way in which companies utilise their online presence. We no longer live in a world of static web pages delivered to desktop computers: content is dynamic and responsive and capable of being delivered to many different devices. Equally, applications rely on the web to communicate, whether with other business applications, to provide services to customers, or to share data with business partners. These points, coupled with the need to 'connect from anywhere', mean that the attack surface is vast and vectors varied.

Application security

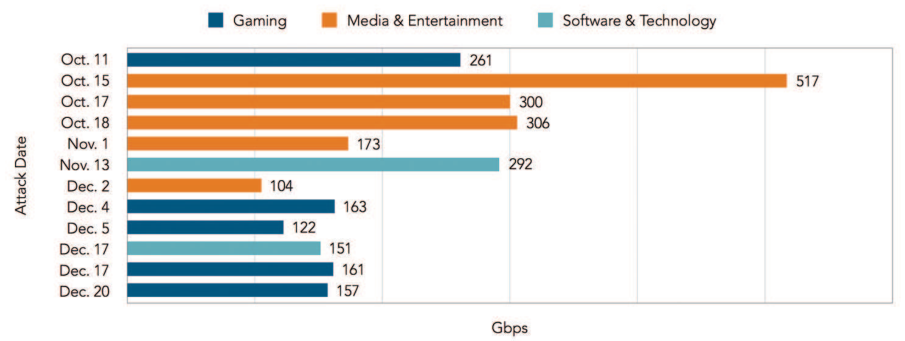
The attacks that often grab the headlines are distributed denial of service (DDoS) attacks and it would be easy to be tricked into thinking that they are the 'most critical' threat, especially when data from Q4 2016 showed that the size of DDoS continued to grow and the number of attacks sized at over 100Gbps increased by 140% compared to the previous year.[2] The largest attack measured an astonishing 623Gbps.

Application attacks happen 'behind the scenes' and thus don't grab as many headlines as DDoS attacks do. While a successful DDoS attack will take a website offline, a successful application attack is sneaky in that when data is exposed or stolen there are often no tracks left behind to the casual observer or even the security practitioner.

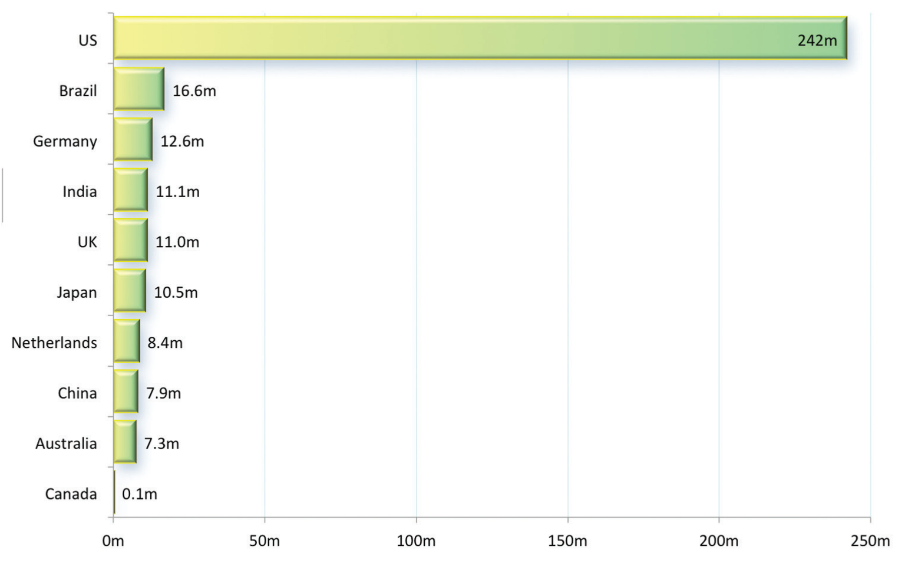
Make no mistake, application layer attacks in all their forms are a major threat to businesses, potentially leading to the theft or destruction of customer or corporate data, creating significant difficulties for the business. Even enterprises that believe they have deployed sufficient security solutions can inadvertently expose themselves through poorly coded application programming interfaces (APIs), resulting in DDoS and parameter-based attacks. Total web application attacks increased 27% in Q4 2016, compared to Q3 and a 33% increase in SQLi attacks was observed. For UK companies, it's notable that the UK remains one of the top five countries targeted in this way.

Considering APIs

It's worth considering APIs more specifically, mostly because for the past few years, APIs have been growing in influence, enabling companies to extend



Attacks of over 100Gbps seen in Q4 2016. Source: Akamai.

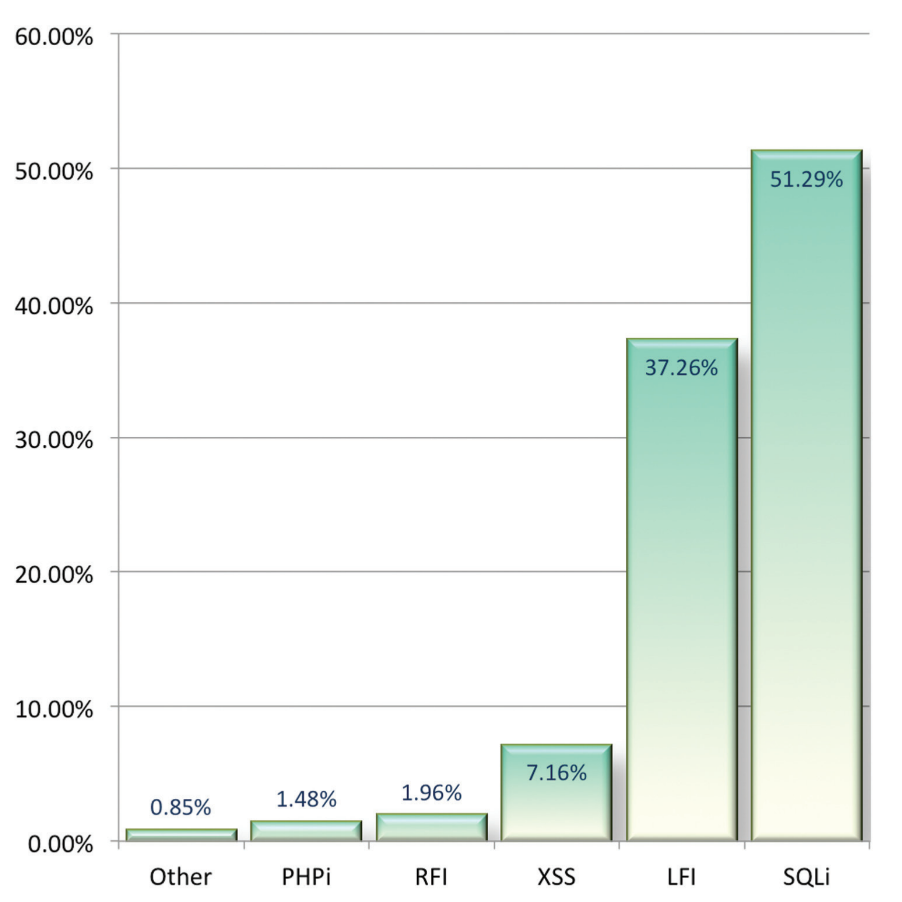


Top 10 target countries for web application attacks, Q4 2016, with numbers of attacks in millions. Source: Akamai.

their core assets and services and add new revenue streams. As a result, they now comprise over 25% of the Internet traffic that Akamai sees and they have become a popular component for delivering native mobile applications.

However, their rapid evolution has meant that security companies are now having to come up with new solutions to provide appropriate protection and companies need to be aware of the specific weaknesses when it comes to deploying their APIs. The exploits of known vulnerabilities such as SQL injection, as well as denial of service by an excessive rate of calls and slow POSTs, require APIs to have an additional layer of protection, ideally with a positive security model that is designed to easily identify and block any abnormal requests or calls that may be attempting to exfiltrate data or otherwise cause harm or havoc.

In addition to updating for new vulnerabilities, a web application firewall (WAF) solution needs to be continuously updated to reflect changes in the applications that it protects. This requires continuously scanning new web applications as they are first deployed as well as existing applications when they are updated, identifying new vulnerabilities and configuring rules to address those vulnerabilities. Web applications are constantly changing and most organisations do not have the resources or expertise necessary to manage a WAF solution over time.



SQLi and LFI combined accounted for 88% of observed web application attacks in Q4 2016. Source: Akamai.

Barriers to implementing firewalls

There is a common theme that runs through the challenges we have raised above – scale, whether it is the threat landscape, traffic volumes or the ability of staff to scale to a point where an internal team can gather the intelligence needed to manage a WAF effectively. With an on-premise WAF, scale is a big issue from a technology perspective. It is not hard to hit a datacentre with a big enough volumetric attack (application or network layer) that will either bring a network down completely, or seriously hinder network performance. Ultimately the pipe connecting the business to the rest of the web will be blocked. Even if staff can respond quickly enough to patch a hole, the traffic continues to block the pipe.

This scale issue is why the traditional WAF, with its very specific role, is no longer up to the job. The cloud is the answer to this challenge, where scale is not only not a problem, it provides an overwhelming benefit. A cloud-based WAF benefits from the intelligence gained by a dedicated security team and often some form of data analysis engine, while enabling a level of automation that can outmanoeuvre the most agile in-house team. It also has the benefit of being able to absorb attacks in the cloud, rather than blocking the pipes serving the datacentre, so availability is not impacted. And cloud-based WAFs usually cache content at the edge of the Internet and thus have the benefit of improving performance. Finally, every customer of that WAF provider feeds the firewall, making it stronger and more intelligent, to the advantage of every customer.

> ***"A cloud-based WAF benefits from the intelligence gained by a dedicated security team and often some form of data analysis engine, while enabling a level of automation that can outmanoeuvre the most agile in-house team"***

Of course, the idea of handing over the care of something so critically important as security to a third party fills some people with fear and this is understandable. We're IT people – we like control! But keeping control in-house has issues as well: problems, including DDoS outages, latency and excessive warnings and alerts, put a huge strain on staff resources. The decision to be made requires balancing of risks. Is the risk of handing responsibility for DDoS and application security to a third party outweighed by the risk of leaving those controls on the inside of the upstream pipe to your ISP?

There are other benefits too, such as adding additional services including in-cloud DDoS mitigation, caching or site fail over. A tightly integrated cloud-based WAF will allow you to do a lot more than simply monitor Layer 7 traffic.

The bots are always hunting

Most web attacks are opportunistic, with bots searching sites at random to look for vulnerabilities. Too many enterprises are aware of the risk they are putting themselves in but simply cross their fingers that it won't be their website that comes onto the bot radar next.

A cloud-based web application firewall, driven by a data analysis engine, can automatically respond to pre-determined threats, matching the pace of the hacker tools looking for cracks in the armour. But allowing that level of automation requires a company to have confidence in the solution and the actions it would take in certain situations.

For those firms that have partnered with a cloud provider – and this is a sensible option, particularly for sites with very heavy traffic – there is the necessity to take into account – and act on – the findings of that partner's intelligence. There is little point in simply using the WAF rule set to 'alert' or running them in listen mode, rather than taking action. In the same way that hackers are using bots to constantly identify weak points, new targets and adapting their attacks, companies must take advantage of the intelligence available to them.

Making a real difference

For those with responsibility for ensuring that their websites and APIs are fully protected, there are a number of 'must haves' when assessing vendors to ensure they can stand nose to nose with the threat. It is worth giving particular consideration to four specific requirements for any successful cloud-based security solution:

1. **Application layer protection:** regularly and automatically updated application firewall 'protection groups' that eliminate the need for companies to manage individual rules. The addition of new protection capabilities without requiring configuration changes. Core protections against SQLi, XSS, RFI, LFI and CMDi attacks.
2. **DDoS protection:** the facility to implement a reverse web-proxy that will automatically drop all non-HTTP and HTTPS traffic regardless of volume. Additional application layer rate controls, slow POST protection and DoS protection group controls round out the DDoS protection capabilities.
3. **Custom rules:** the ability to deploy multiple custom rules, providing the flexibility to address any application-specific issues that can benefit from cloud-based protections.
4. **Self-service management:** it should be possible to easily and fully manage the deployment and ongoing protection of websites and APIs without any dedicated third-party resources.

Constant change

The security landscape changes constantly and it is imperative that enterprises that rely on the web to communicate with, or sell to, their customers are in a position to adjust quickly and with agility. For example, the threat posed by Internet of Things (IoT) devices is serious and should not be dismissed as just a problem for homeowners with smart TVs. The vulnerability of IoT devices has already been exposed with devastating effect and yet there is still a lack of urgency among manufacturers to implement appropriate security for each individual connected device.

While this remains unresolved, companies need to be focused on reducing the downtime, defacement and data theft risks, staying ahead of threats through automatic rule deployments. Unless an organisation is already in the business of developing cyber-security solutions, it will not have visibility into new vulnerabilities and attacks that are constantly evolving. An organisation can choose to implement and manage its own WAF to block DDoS and web application attacks, but aside from the lack of visibility can it afford the investment required in terms of hardware and skilled security professionals? There is an economy of scale achieved by working with specialist partners, where the perceived loss of control is greatly outweighed by the skill and speed with which they can react to the most challenging attacks.

Whichever route a company takes to protect itself, what is clear is that any WAF must itself be constantly evolving and gather the intelligence needed to protect against the known and unknown from application layer and DDoS attacks – and to do it with great speed and scale.

The problem is not going away: the scale of a company's internal defences is starting to become irrelevant – if there is a crack, however fine, it will be found. As historian C Northcote Parkinson put it "Delay is the deadliest form of denial".

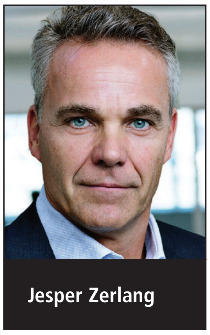
About the author

Daniel Shugrue is a director of product marketing at Akamai. He has 15 years of experience working in telecom and security technology. Prior to working at Akamai, he was principal product marketing manager for RSA, the security division of EMC. Shugrue now drives the marketing activities for Akamai Cloud Security Solutions, which provide cloud-based website protection services for many of the world's largest companies.

References

1. Monaghan, Angela. 'TalkTalk profits halve after cyber-attack'. The Guardian, 12 May 2016. Accessed Jun 2017. www.theguardian.com/business/2016/may/12/talktalk-profits-halve-hack-cyber-attack.
2. 'State of the Internet/Security: Report for Q4 2016'. Akamai. Accessed Jun 2017. https://content.akamai.com/pg7969-q4-soti-security-report-uk.html.

GDPR: a milestone in convergence for cyber-security and compliance



Jesper Zerlang

Jesper Zerlang, LogPoint

One of the greatest misconceptions in business today is that compliance equates to good business practice – particularly with regard to security. In reality, compliance ensures a base level of security to which companies must adhere in order to 'tick the box'. Cybercrime, however, is evolving at an exceedingly rapid pace, meaning it is often difficult for regulations and legislation to keep up with a changing security landscape. The result is outdated requirements that are often unfit for purpose.

The General Data Protection Regulation's (GDPR) predecessor, the European Data Protection Directive, was adopted in 1995. While ensuring compliance with this Directive was not mandatory, it did help to ensure industry-wide best practice. But since its implementation over 20 years ago, the digital landscape has changed drastically. From a proliferation of data, to increasingly interconnected technologies and a growing amount of processing power, it had become clear that the EU Data Protection Directive was in urgent need of modernisation.

Businesses have been reaping the rewards from this new digital landscape, utilising the increased amounts of data created each day to inform high-level decision-making. What has not kept up with this shift, however, are the regulations and security essentials that coincide with its use. While the majority of organisations do *attempt* to ensure data security in the modern economy, the baseline set forth by the Data Protection Directive has fallen short as time has progressed. The GDPR presents an opportunity to level the scales and drive greater convergence between cyber-security and compliance – two areas often seen as disparate by business leaders.

Impact on modern business

One of the biggest benefits of the new GDPR is the open wording. The regulation is designed with the future in mind, specifying the minimum security baseline to which data will be subject, as opposed to the minimum requirement to secure it. The focus is far more broad than its predecessor, motivating companies to secure their systems to avoid data breaches where possible and effectively reporting on them when mitigation has failed. This means that in a continuously evolving digital landscape, the regulation should remain relevant to modern business practices for some years to come. A key result of this shift will be the adoption of cyber-resilience, a change in perception that acknowledges that cyber-attacks *will* occur. Under GDPR it is now the responsibility of each business to proactively prepare for and mitigate the damage caused by an attack, getting back to business-as-usual as soon as possible.

At its core, GDPR's primary objective is to strengthen and harmonise data protection for individuals as well as to simplify regulatory environments for organisations. GDPR contains several new requirements regarding how all organisations should process, store and safeguard personally identifiable information (PII), with financial penalties to ensure they are implemented. Data breaches must now be reported to relevant authorities within 72 hours; Data Protection Officers must be employed; and Subject Access Requests must be met.

Failure to comply with GDPR legislation could result in fines of up to €20m, or in the case of an undertaking defined as a 'business grouping', 4% of annual worldwide group turnover – whichever is higher.

In theory, this regulation has been in force since its introduction in April 2016. As of May 2018, however, GDPR will be fully enforced, giving companies just over a year to make the necessary changes and ensure compliance. At its core, GDPR is a regulation that encourages digital transformation. By requiring greater categorisation and reporting standards on data held, data becomes far easier to find within an organisation – both for the organisation and – unfortunately – hackers. In case of an attack, the final security hold-out, security through obscurity, is now broken down. With all data mapped and accounted for, GDPR turns security from a consideration into a necessity. In meeting these requirements, organisations are presented with the opportunity to go beyond compliance, integrating modern cyber-security practices to drive operational efficiency.

Connected landscape

The business landscape has changed since the implementation of the first Data Protection Directive. It has taken a number of years, but businesses are now being incentivised to shift with it through GDPR. In 2011, the amount of data created reached 1.8 zettabytes per year; currently, 90% of the total data in existence has been created within the past two years alone.[1,2] By 2025, the amount of data created yearly is predicted to rise to a staggering 44 zettabytes. This will in turn put greater security pressures on organisations in the public and private sectors.[3] This will be particularly apparent within healthcare organisations, which are especially vulnerable to phishing and social engineering attacks, where valuable stolen data is sold at a premium online.[4,5]

Following the financial crisis of 2007 and 2008, new technologies were almost exclusively focused on compliance – looking at who is doing what with data and which people are accessing it within individual departments. During this period, organisations were invariably working in silos – different departments with disparate capabilities and data storage methods. While far from an ideal scenario, the smaller amount of data created meant that a siloed approach was feasible. This practice was influenced by the regulations and directives at the time, with organisations following guidelines and maintaining compliance.

> ***"By requiring greater categorisation and reporting standards on data held, data becomes far easier to find within an organisation – both for the organisation and – unfortunately – hackers"***

Should this siloed approach be utilised today, however, companies would very quickly find themselves falling victim to data breaches. For example, the recent TalkTalk hack resulted in the company losing over 100,000 customers and enduring costs of £60m.[6] This hack was revealed to be the work of a single teenager, who exploited the organisation's failure to implement basic security measures.[7] Notably, the company experienced £20m in lost revenue due to the reputational damage and a reduced customer base in its fourth quarter in 2016.[8]

Whereas in previous years, the challenge posed by cyberthreats would be met solely by the department against which the attack was perpetrated, the appointment of a Data Protection Officer represents a recognition that data is now central to an organisation's success. As a facet of GDPR compliance, this new role will go a long way towards providing a holistic overview of the technologies required and data possessed by a company: driving towards analytics and big data utilisation, as well as ensuring cyber-resilience. This overview will be essential to ensuring the security of data across an entire business, as opposed to individual, disparate departments. The challenge, however, will come from implementing this shift in organisations which solely look to meet compliance – with the added requirement of breaking down silos in the process.

Meeting the challenge

When exponential data growth is combined with outdated regulations, the outcome is a staggering level of cyber-risk. Further than the inherent reputational damage, the rising amount of data with which organisations must now work also correlates with greater levels of compliance failings and security risks. The fault for this by no means rests with businesses alone.

The rising amount of data created and used within the private and public sector has created the perfect environment for a new breed of cyber-attacker. In recent months, the use of ransomware has increased exponentially – particularly against large-scale institutions such as hospitals, where one target recently paid $17,000 to recover files.[9] When increasing cyber capabilities are combined with a greater financial motivation to attack companies, the result is a pressing requirement for businesses to ensure security.

> ***"While the majority of organisations do attempt to ensure data security in the modern economy, the baseline set forth by the Data Protection Directive has fallen short as time has progressed"***

In meeting the challenges posed by GDPR, organisations will be required to vastly increase the security of their data, systems and processes with modern technologies such as security information and event management (SIEM) acting as an enabler. While GDPR adherence may be a costly process for organisations focusing solely on 'ticking the box', the process can go beyond compliance. Instead, businesses can take advantage of the digitalisation process that GDPR encourages, utilising advanced tools to analyse the big data on offer.

Beyond compliance

Notably, in light of GDPR integration and compliance, cyber-security spending across EMEA is expected to grow to $15.9bn by 2020.[10] The benefits of integrating GDPR across a business are clear, however the drive to digital transformation will require significant planning and review around the people, systems and processes necessary to secure it. Once this has been achieved, the convergence between the once separate practices of cyber-security and compliance will become clear.

Within the financial sector, for example, compliance is becoming increasingly complex – due not only to the amount of data to process but also the increasing requirements to keep it secure. This complexity is exacerbated by the rising number of cyber-attacks in the sector. In 2016 alone, 80 million cyber-attacks were detected against financial services – netting an estimated £8bn in fraudulent transactions.[11]

Cyber-attacks therefore pose a direct threat not only to businesses, but also to the data they hold, which is frequently personally identifiable in nature. Despite holding a wealth of personal information and a greater motivation to ensure its security, just one in five organisations is confident it could detect a data breach.[12]

Budgetary limitations

What poses extreme difficulty in the public sector is the consistent theme of fixed budgets, which are invariably set in advance. When ensuring cyber-security within an organisation to meet compliance, this budgetary system can be ineffective. Should a business fall under attack, a yearly budget may be quickly drained in restoring server status, reporting on any data that has been lost and upgrading defences to ensure that the threat is mitigated in future. This allows no further in-budget scope for proactive network defence, leaving businesses open to social engineering attacks such as CEO fraud.

Due to budgetary constraints, organisations have in the past chosen to secure only the most mission-critical elements of their business. In today's digital landscape, there exists a greater number of threat actors, methodologies and entry points. Any device an employee uses within the office represents a potential threat. Internet of Things devices, which are hacked an average of 360 seconds after going online, provide backdoor access into otherwise secured networks.[13] With so many threats and a myriad of entry methods, single, unsecured elements of a firm can act as a staging ground for much broader attacks.

When cyberthreats are able to hit any element of a network, the solutions must be equally as all-encompassing. Air-gapping a network, as recently attempted by the Singaporean Government, is only a viable solution until an employee plugs an infected USB into a port.[14] To adhere to GDPR going forward, businesses must shift towards digitalisation, ensuring a holistic overview of all data held within a company and an all-encompassing security focus on that basis. Once this is achieved, the onus can shift away from damage control and towards mitigation and cyber-resilience.

Proactive security

Data normalisation is fast becoming an essential for modern business under GDPR, with SIEM technology playing a key role. Often, the data held is stored in different formats, meaning that a huge amount of time is required to manually detect a breach or event. Once this data is normalised, however, searching for anomalies and identifying threats is a much more streamlined process, allowing rapid response times, preventing or minimising the quantity of data stolen and avoiding fines from delayed reporting.

Further to this, one of the key elements of GDPR compliance is meeting Subject Access Requests (SAR). The process of normalisation not only allows for a greater level of proactive security, but the easy access to available data means that once a SAR is received, the recipient can accurately access every piece of information held on them.

Once normalisation is in place, intelligent technology is essential to maximise its potential through big data. Network monitoring and analytics, enabled through this normalisation process, can go further than compliance. Ransomware attacks, for example, are one of the most prolific attacks affecting business globally. These are identified through high frequency file changes on a computer or network, changes which happen at speeds impossible for a human to make or detect. If a file is not catalogued correctly, the baseline of monitored data is muddied, with attacks going un-noticed until the damage is already done. However, should a qualifying number of files be changed in a short period of time, alerts can be sent to relevant stakeholders and damage can be mitigated.

GDPR represents a demand for effective data management practices, with cyber-security fast becoming synonymous with compliance. Where data threats may have not previously been identified due to disparate, non-communicative systems, the rapid response allowed by technology-enabled normalisation can assist with proactive cyber-security.

With under one year until GDPR comes into force, many businesses are yet to fully implement an effective digitalisation strategy – not only risking non-compliance, but missing out on the business benefits inherent in a data-driven organisation. Beyond compliance, GDPR represents an opportunity for companies to shift towards a digital future, effectively utilising big data to make informed business and security decisions. It is now the responsibility of each individual organisation to ensure that they benefit from this shift through innovative technologies, instead of falling foul of GDPR fines.

About the author

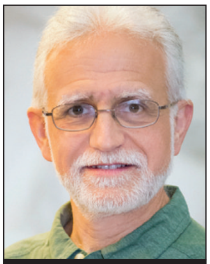
Jesper Zerlang, CEO at LogPoint (www.logpoint.com), has a background in larger corporates such as Telia, Dell, HP and AP Moller Maersk – always with a strong customer focus. His entrepreneurial interests have driven him to smaller organisations to spark innovation and growth – with experience in businesses such as private equity, IP telephony, IT hardware technologies and IT security. Zerlang serves on the board of directors of other high-potential software companies and has supplemented his academic background with executive management programmes from Harvard Business School.

References

1. Mearian, Lucas. 'World's data will grow by 50x in next decade, IDC study predicts'. ComputerWorld.com, 28 Jun 2011. Accessed Mar

2017. www.computerworld.com/article/2509588/data-centre/world-s-data-will-grow-by-50x-in-next-decade – idc-study-predicts.html.
2. Wall, Matthew. 'Big Data: Are you ready for blast-off'. BBC.co.uk, 4 Mar 2014. Accessed Mar 2017. www.bbc.co.uk/news/business-26383058.
3. Turner, Vernon. 'The Digital Universe of Opportunities'. IDC, Apr 2014. Accessed Mar 2017. www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.
4. Whittaker, Zack. 'A hacker is advertising millions of stolen health records on the dark web'. ZDNet.com, 27 Jun 2016. Accessed Mar 2017. www.zdnet.com/article/hacker-advertising-huge-health-insurance-database/.
5. Donnelly, Laura. 'Largest NHS trust hit by cyber-attack. Telegraph.co.uk, 13 Jan 2017. Accessed Mar 2017. www.telegraph.co.uk/news/2017/01/13/largest-nhs-trust-hit-cyber-attack/.
6. Farrell, Sean. 'TalkTalk counts costs of cyber-attack'. The Guardian, 2 Feb 2016. Accessed Mar 2017. www.theguardian.com/business/2016/feb/02/talktalk-cyber-attack-costs-customers-leave.
7. Jones, Sam; Thomas, Daniel. 'Experts say TalkTalk had 11 serious website vulnerabilities'. FT.com, 30 Oct 2015. Accessed Mar 2017. www.ft.com/content/e5eead0c-7f0b-11e5-98fb-5a6d4728f74e.
8. Hall, Kat. 'TalkTalk admits losing £50m and 101,000 customers after THAT hack'. The Register, 2 Feb 2016. Accessed Mar 2017. www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/.
9. 'Three US hospitals hit by ransomware'. BBC News, 23 Mar 2016. Accessed Mar 2017. www.bbc.co.uk/news/technology-35880610.
10. 'New Regulations Impact EMEA Cyber-security Market in 2016, IHS Says'. IHS, 11 May 2016. Accessed Mar 2017. https://technology.ihs.com/578184/new-regulations-impact-emea-cyber-security-market-in-2016-ihs-says.
11. Ashford, Warwick. 'Cyber-criminals net £8bn from financial services in 2016'. ComputerWeekly.com, 27 Feb 2017. Accessed Mar 2017. www.computerweekly.com/news/450413850/Cyber-criminals-net-8bn-from-financial-services-in-2016.
12. Coumaros, Jean; Chemin, Marc. 'The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure'. Capgemini Consulting, 2 Feb 2017. Accessed Mar 2017. www.capgemini-consulting.com/resources/data-privacy-and-cyber-security-in-banking-and-insurance.
13. Leyden, John. 'Sweet, vulnerable IoT devices compromised 6 min after going online'. The Register, 17 Oct 2016. Accessed Mar 2017. www.theregister.co.uk/2016/10/17/iot_device_exploitation/.
14. Wagstaff, Jeremy; Aravindan, Aradhana. 'Mind the air-gap: Singapore's web cut-off balances security, inconvenience'. Reuters.com, 24 Aug 2016. Accessed Mar 2017. http://uk.reuters.com/article/us-singapore-Internet-idUKKCN10Y2F1.

How automating data collection can improve cyber-security



Jay Botelho

Jay Botelho, Savvius

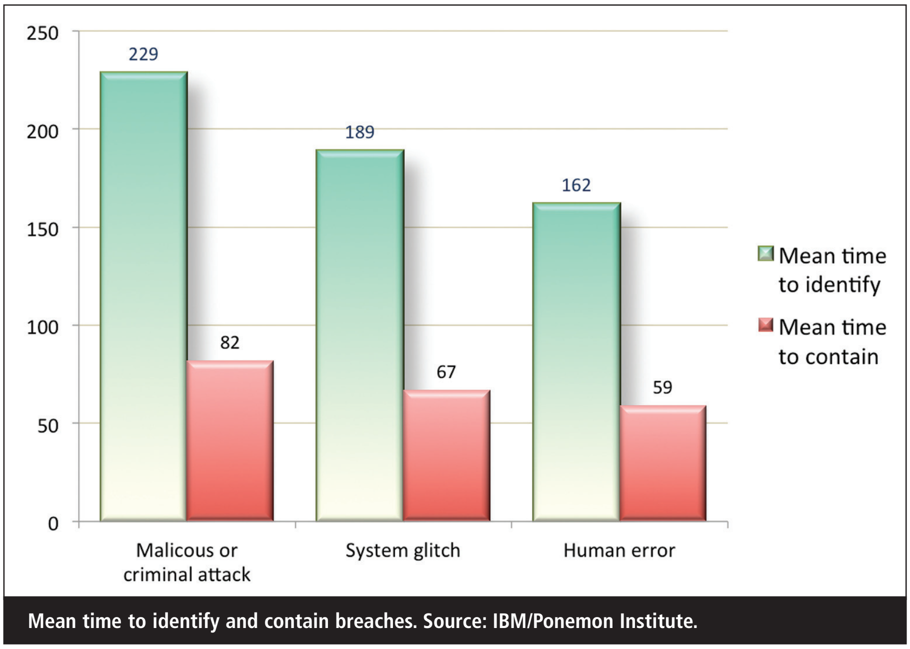
The fallout from a data breach can be catastrophic. We have yet to understand the full impact of the massive Yahoo breach, but that doesn't mean that smaller and equally damaging breaches aren't taking place every single day.

The scale of Yahoo's breach may be unparalleled, but the problems are not. The simple fact is that it takes way too long to discover and resolve breaches. And something has to be done about it.

Security drivers

According to a report by the SANS Institute, the majority of companies already spend up to 12% of their annual IT budget on security.[1] The reasons behind this kind of spend include a variety of business drivers, including the need to protect sensitive data, improve incident response, and of course to comply with legal requirements as defined by the General Data Protection Regulation.[2]

Security technologies have evolved as a means to defend against hackers, while cyber-criminals have a clear motive to make money by stealing data. To illustrate how lucrative cybercrime can be, we need only look at the Darknet. This seedy underbelly of the Internet is a haven for an incredible volume of hidden criminal commerce. In congressional testimony in September 2015, FBI director James Comey referred to the darknet as: "A world full of criminals, which is why investigators for the FBI and our partners spend a whole lot of time there." Putting a dollar figure on



Mean time to identify and contain breaches. Source: IBM/Ponemon Institute.

their activity is difficult, but according to the United Nations Office on Drugs and Crime, cybercrime was estimated to rake in $600bn in 2017, more than any other form of crime, even exceeding the value of the drug trade.

So we know that there is money in cybercrime. A logical question to ask, then, is whether security methods can keep up.

Under the radar

In the past, traditional security methodology relied almost exclusively on incremental improvements and updated signatures in firewalls; intrusion detection and prevention technologies (IDS/IPS); and security information and event management (SIEM) devices. Without being disparaging about these devices – because they are fantastic at what they do – they are far from perfect. In recent years, hackers have become much better at developing (and sharing) smarter, better targeted and more automated tools that help them fly ‘under the radar’ without having to bombard an enterprise security system (unless their goal is a distributed denial of service attack). Attackers understand how IDS/IPS/SIEMs work, so they have become much more adept at avoiding those known detection techniques.

One of the most common methods used by hackers today is social engineering. These attacks are not only becoming more common against enterprises and SMBs, but they're also increasingly sophisticated. A common way for a hacker to gain a foothold in a network is to use email or other forms of communication that cause a victim to reveal sensitive information, click on a malicious link, or open a file with a malicious attachment. These emails are often disguised to look like legitimate messages from someone inside the organisation. With hackers deploying increasingly realistic ways to fool employees and individuals into handing over valuable company data or passwords, enterprises need to be significantly more diligent if they want to get ahead of cyber-criminals.

Contrary to what we see in movies, most successful hacks are generally not the result of bad actors trying to exploit technical flaws or zero day vulnerabilities. Rather, they target people who accidently give them access to a network. Symantec claims that only about 3% of the malware it encounters is an attempt to exploit a technical vulnerability. The other 97% is aimed at tricking users through some kind of social engineering scheme. The most common of these is a phishing or spear-phishing attack, which may rely on things such as fake court notices or IRS refund ransomware to prompt an individual to respond.

Ultimately, it takes just one chink in an enterprise's security armour for a hacker to quietly gain access to an enterprise network and sit there undetected for many months while looking around and preparing to exfiltrate valuable data.

Overwhelmed analysts

We know that organisations are in a constant arms race with hackers and we shouldn't expect this to change any time soon. In fact, it will probably get worse. The latest IBM and Ponemon 2016 Cost of Data Breach Study found that malicious and criminal attacks took an average of 229 days to discover and an additional 82 days to resolve.[3] Why so long? This is a complex issue, but a lot of the blame lies in the fact that security analysts are overwhelmed with data. As more and more alerts are generated by an enterprise's IDS/IPS devices, analysts can only investigate a handful each day.

> ***"A common way for a hacker to gain a foothold in a network is to use email or other forms of communication that cause a victim to reveal sensitive information, click on a malicious link, or open a file with a malicious attachment"***

Turning again to recent well-known incidents helps to illustrate this problem. An obvious one is the breach that took place at big-box retailer Target. Security expert and blogger Brian Krebs was the first to break the news of the Target breach, in which the card data of 40 million cardholders and the phone numbers and email addresses of 70 million customers were compromised during the 2013 holiday shopping period.[4] He described the Target incident as an APT, or advanced persistent threat, in which hackers were able to access Target's network via one of the company's third-party vendors. The hackers then remained undetected for months, waiting for an advantageous time to strike.

More recently, Yahoo's massive breach went undetected for years, ultimately compromising hundreds of millions of users' data and damaging Yahoo's reputation and value. Even after being alerted to the breach, it took Yahoo months to announce the true extent of the damage. The fact is that sophisticated hackers will use any means they can to gain access to an enterprise network and they often won't be detected for many months.

Two-part solution

So what's the solution? The answer is twofold. First, for those who continue to subscribe to the theory of real-time detection and prevention, security analysts need tools and processes that enable them to work much more efficiently. It's amazing that companies deploy security solutions to produce all these alerts, but they don't have the bandwidth to analyse them. The most logical reasons are that security analysts don't have access to the right data and they cannot access it quickly enough. This is a huge problem. Current solutions require a multistep process where security analysts go to multiple systems for aggregated yet uncorrelated data, then to specific computers for detailed information, and then must correlate all the data manually. The very best data is in the network packets, but none of it is indexed to the alert, and access to such data is typically a network function, not a security function. And if the alert is older than a few days, then the original packet data have probably been discarded. Security engineers need access to all of the packets related to an alert right at their fingertips, at the click of a button.

"It takes just one chink in an enterprise's security armour for a hacker to quietly gain access to an enterprise network and sit there undetected for many months"

But second, and even more importantly, while there is still a widely-held mythology that rapid response to hacker attacks is possible, all of the evidence indicates that there is little chance of catching a bad actor 'on the fly'. Better models assume the hacker is already present and focus efforts on finding and removing his outposts(s) and determining the compromised resource and the extent of the damage.

In practice, this means two things; being able to discover and remove infiltrations faster and having the best data available to unequivocally determine the damage done. This is not the time for the kind of imprecision we've seen over and over again - first report: two million records were compromised; after a bit more research, it turns out to be really 20 million; and in the final analysis, the real damage was 80 million records compromised. For both a security professional and a victim, this is unacceptable.

"Critical network packet data can be stored for months, allowing security analysts to work on the premise that the hacker is already present and has been for a while"

Just as in the real-time case, the best data to address the imprecision we see today in security forensics is network packet data. As alerts are received from a security system, a computer should parse them, storing only the network packet data that correlates with the source of the alert. By doing so, critical network packet data can be stored for months, allowing security analysts to work on the premise that the hacker is already present and has been for a while. Security-relevant packet data, along with log data from a SIEM, can be pulled together in the background, automatically, making it easier for an analyst to access the data with a single click and evaluate whether an issue needs further investigation. If, for example, the log and packet data don't match, then a deeper look may be warranted.

Automating data collection

Automating alert-related data collection will allow that data to be stored in a central location, but that one place doesn't exist yet. Currently, analysts typically go to something like a SIEM dashboard and log into a host machine or other UI, switching between multiple software applications or devices to access information. This is ridiculously time consuming and inefficient.

The security industry needs to develop automated processes that automatically collect relevant 'suspicious' packet data and make it readily available for analysts. This will make their jobs more efficient, while helping them to investigate more alerts each day. If that can happen, I think it's reasonable to expect analysts' productivity to increase significantly, whether searching for bad actors on the fly, or retracing their steps long after they've gained access.

About the author

Jay Botelho is director of products at Savvius (www.savvius.com), which offers packet intelligence solutions for network performance management and security investigations. He holds an MSEE and is an industry veteran with more than 25 years of experience in product management, product marketing, programme management and complex analysis. From the first mobile computers developed by GRiD Systems to modern day network infrastructure systems, Botelho has been instrumental in setting corporate direction and specifying requirements for hardware and software products. He is based at Savvius' headquarters in Walnut Creek, California.

References

1. 'IT Security Spending Trends'. SANS Institute. Accessed Jun 2017. www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697.
2. EU GDPR Portal, home page. Accessed Jun 2017. www.eugdpr.org/.
3. '2016 Ponemon Cost of Data Breach Study: Global Analysis'. IBM/Ponemon Institute. Accessed Jun 2017. https://www.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542.
4. Krebs, Brian. 'Sources: Target investigating data breach'. Krebs on Security, home page. Accessed Jun 2017. https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

Leaks and ransoms – the key threats to healthcare organisations

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

Of all the personally identifiable information (PII) that could be leaked, healthcare data is arguably the most intimate and worrying. You would think that healthcare organisations would try their hardest to protect that information and yet they are constantly in the headlines following leaks and successful cyber-attacks. In this interview, Niall MacLeod, sales engineering manager EMEA at Anomali, explains how healthcare organisations are getting better at managing information security, but that the road ahead isn't easy.

"Healthcare organisations globally are facing the same challenges," he says. "We're seeing data breaches across sectors increasing everywhere. The Information Commissioner's Office [ICO] says there were 239 data security breaches from June to October last year, covering the NHS and other UK healthcare providers and cyber breaches accounted for about 74 of those. We're seeing, within the UK, breaches of health providers probably account for most of those reported to the Information Commissioner's Office. Partially that's to do with the NHS's mandatory reporting requirements, but as a generalisation, I think that attacks focused on healthcare providers are on the increase globally and definitely within the UK."

Accidents and malice

Not all data breaches are the result of malicious attacks. Many are the result of carelessness resulting in the accidental loss of data. MacLeod mentions the incident in Orkney in 2014 when patient notes were left on the pavement outside Balfour Hospital.[1] And in February 2017 it was discovered that a company responsible for delivering correspondence from National Health Service (NHS) services – including hospitals, clinics and GPs – had instead stored many of the letters and reports in a warehouse.[2] Around 500,000 pieces of correspondence, which included test results and treatment plans, were mishandled by NHS Shared Business Services (NHS SBS), a private company co-owned by the Department of Health and French firm Sopra Steria that provided document delivery services for NHS England. Following the discovery, NHS England set up a team to address the problem, but did so in secret, leading to accusations of a cover-up.

However, while there is certainly the potential for harm with such accidental exposure, it's often difficult to point to concrete examples of damage caused by the breach of information *per se*. (In the case of the NHS SBS incident, the harm is most likely to have arisen from the non-delivery of the documents.)

"We're looking at attacks focused on electronic health records. We're looking at traditional hacking. This could get quite serious, with the proliferation of medical devices that are out there"

The same cannot be said where data breaches are the result of malicious activity.

"We're looking at attacks focused on personally identifiable information, maybe details of NHS employees themselves," says MacLeod. "We're looking at attacks focused on electronic health records. We're looking at traditional hacking. This could get quite serious, with the proliferation of medical devices that are out there. We've got a lot of critical systems within hospitals that are Internet connected these days – on a network and possibly vulnerable, running on legacy systems."

Ransom demands

Notoriously, the healthcare sector has also been heavily targeted in ransomware attacks. Some of the first victims to be identified in the recent WannaCry (aka WannaCrypt0r 2.0) spree were UK healthcare organisations, leading to the mistaken assumption – at least early in the campaign – that the attackers behind WannaCry were specifically targeting the NHS.[3]

However, just because the WannaCry campaign turned out to be rather more catholic in its taste for victims, the fact that healthcare organisations were hit – and were among the first – is not without significance. That's because WannaCry was unusual. The vast majority of ransomware campaigns have used spamming and mass phishing attacks to achieve their infections. WannaCry, however, is now known to have employed both carefully targeted spear-phishing in the initial phases as well as the direct compromising of Internet-connected devices with weaknesses – specifically, the use of outdated SMB protocols – that could be remotely detected. As we'll see, many healthcare organisations are particularly vulnerable here.

WannaCry was far from being the first ransomware campaign to hit healthcare organisations. In fact, they

Niall MacLeod, sales engineering manager EMEA at Anomali, has been involved in cyber-security since the early 2000s, working across sales engineering, consulting and architecture. His first SIEM installation was back in 2004 and other roles have covered securing web-facing infrastructure for government; evaluating disaster recovery plans for an investment bank; and PCI audits of retail organisations. MacLeod joined Anomali in 2016, where he works with platforms addressing threat intelligence. He holds CISA and CISSP certifications and was previously a PCI QSA.

were among the earliest targets when cyber-criminals decided to switch the focus of ransomware campaigns from individuals to businesses. Early in 2016, the Hollywood Presbyterian Medical Centre, a large hospital in Los Angeles, fell victim and ended up paying the attackers.[4] Other hospitals soon followed, both in the US and Europe. By October 2016, 14 hospitals had been attacked in the US alone.[5]

It can be difficult to get exact figures to judge the scale of the problem. Security firms have used Freedom of Information requests in the UK in an attempt to get NHS Trusts to reveal if they have been affected by ransomware attacks, but the results are incomplete. One such survey, by the NCC Group, queried 60 NHS Trusts, of which 31 refused to respond, citing patient confidentiality.[6] Worryingly, of the 29 that did reply, all but one said they had been hit by ransomware in the past year. And that one admitted it had also been affected – just not in the preceding 12 months.

A subsequent survey by SentinalOne obtained responses from 94 out of 129 trusts contacted. This found that a third (30%) admitted to having been hit by ransomware.[7] One of the organisations – Imperial College Healthcare – had 19 attacks in one year. And of the 15 organisations that were able to offer additional information on the nature of the attacks, 87% said that a networked NHS device was compromised and 80% said the attack involved phishing.

These attacks can be devastating. "The very big one reported last year was North Lincolnshire & Goole NHS Foundation," says MacLeod.[8] "They were hit by a large ransomware attack – a piece of malware called Globe 2, which is fairly sophisticated. It uses the Bluetooth-encryption algorithm. That attack caused a four-day IT shutdown and 2,800 appointments or procedures were cancelled and many patients, including high-risk patients such as women in labour, were sent to neighbouring hospitals. That was a serious cyber-attack."

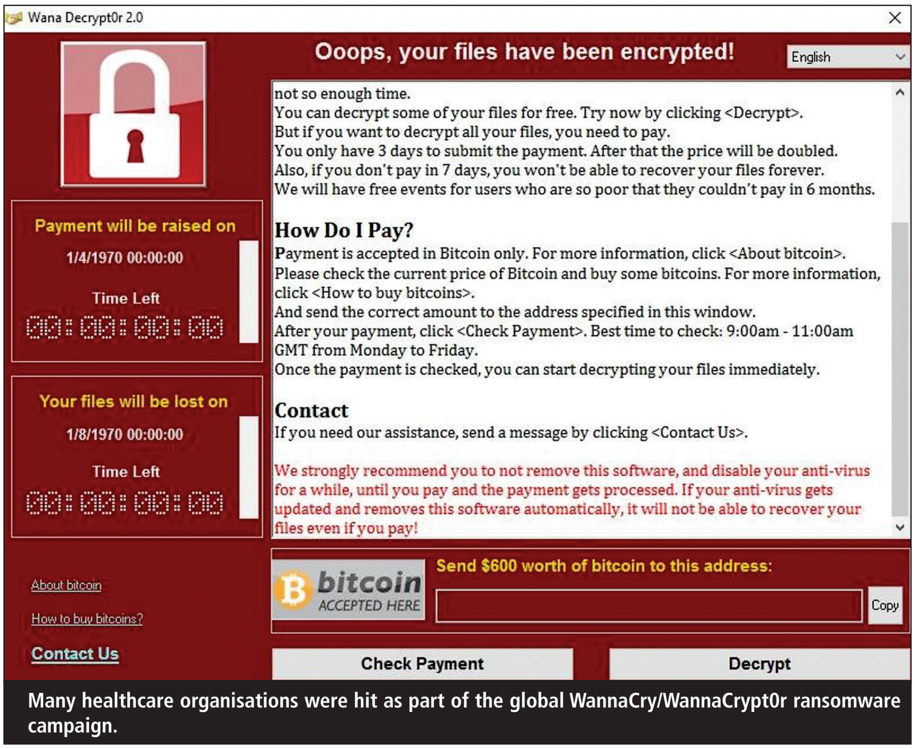
Value of data

Strangely, the targeting of hospitals with ransomware is partly a response, MacLeod believes, to massive breaches in the past that have flooded the underground markets with PII. The cybercrime world is a free market and this has had an effect on the value of that data.

"At one stage, an electronic health record with a lot of PII information was actually worth something, it actually had a monetary value," he says. "It was probably worth about 10 times the amount that a credit card detail was worth. But there have now been many large-scale breaches in the US, including the Anthem attack back in early 2015, where they lost almost 80 million records – this is larger than the population of the UK. There are just too many [records] out there, so the price of PII coming through from hospitals has dropped dramatically in value. Things that people were advertising for $75 or $100 back in 2015 are now going for $20 to $50."

> ***"Think how this sort of information could be used against you: you have all of your medical history available, but if that was given to your employers, that could be harmful to you"***

That still makes the information worth having, from an attacker's point of view. But the criminals who are acquiring healthcare PII are not necessarily doing anything with it themselves.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking <Contact Us>.

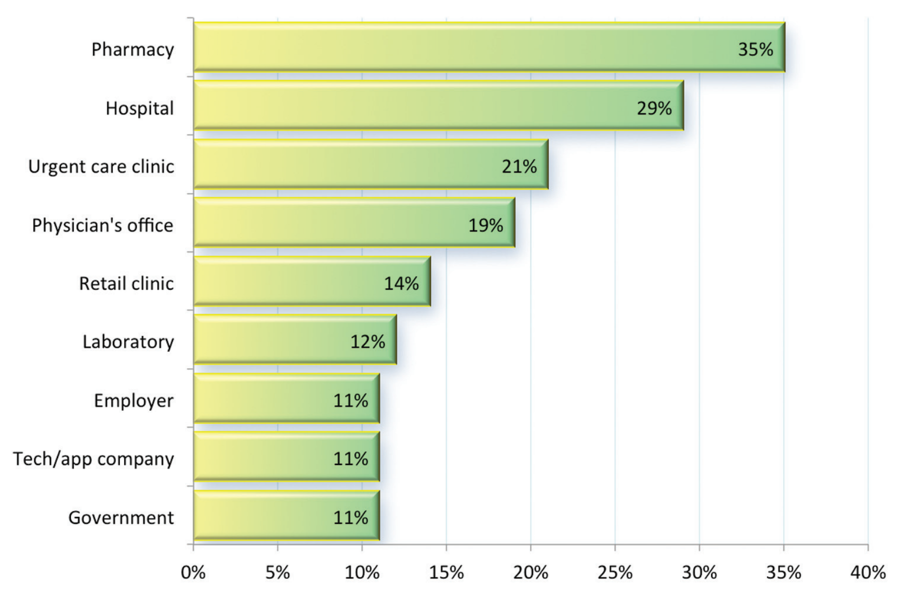
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

Send $600 worth of bitcoin to this address:

Many healthcare organisations were hit as part of the global WannaCry/WannaCrypt0r ransomware campaign.



Where digital healthcare breaches occur. Source: Accenture (see box).

"We track a lot of threat actors out there," says MacLeod. "One of the famous ones in the US is an organisation called the Dark Overlord. Very often, they just look at this as an asset and they're not looking to monetise it themselves. They're just looking to sell that information on to the highest bidder.

"What the highest bidder does with it then is up to them. It might just be identity fraud – to use medical information as background information to allow [them] to open bank accounts. But the implications for medical data are quite incredible. There have been reports of things like prescription medication being ordered through false profiles. In the US, we've seen fraudulent insurance claims being launched. Think how this sort of information could be used against you: you have all of your medical history available, but if that was given to your employers, that could be harmful to you. It could contain your sexual history; it could contain your drug use, illegal or not; information to be used by life assurers. There are a number of different ways that this information could be used."

He gives the example of the Chelsea & Westminster NHS Trust, which was fined £180,000 by the ICO.[9] The trust sent an email to around 780 recipients, all of whose email addresses were included in the To: header of the message, instead of the Bcc: field, making them readable by all recipients. Most (730) of the addresses also included the recipients' full names. To make matters worse, the people listed were all patients of 56 Dean Street, a Soho-based sexual health clinic, who had signed up for an HIV newsletter. This is not the kind of information you want going to the wrong place.

Nonetheless, it still takes a lot of effort to exploit this kind of data. And if the people mounting the cyber-attacks can't get a good return for their efforts, then it may be better to try something else.

"What's happening now is that the hackers are looking for other ways to monetise their skills," says MacLeod, "and ransomware definitely seems to be the flavour of the moment. Targeting a hospital means you're targeting somewhere that cannot do without computer systems. There could be life-or-death decisions being based on uptime of certain systems. And if hackers can get into and disable those, there's a very good chance that they will get their ransom paid."

Uniquely vulnerable

It's believed that several healthcare organisations, having fallen victim to a ransomware attack, have paid up. Given that the most effective solution to ransomware is to have good back-ups, does this suggest that some of these organisations are ill-prepared for an attack? Or do they have unique vulnerabilities?

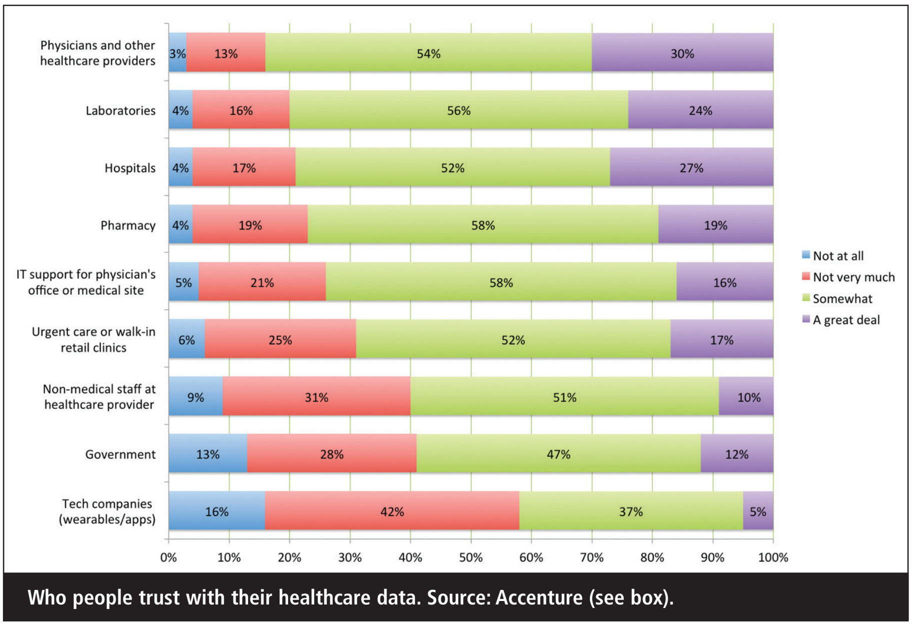
"A lot of them do have very good backup systems, to be honest," says MacLeod. "And there have been a lot of cases in the UK where the hospitals and trusts have managed to avoid paying ransoms altogether. The problem isn't really the financial loss, it's just the disruption. If we look at that previous example – four days of computers being offline, while they were restored from back ups and cleaned, 2,800 appointments and procedures cancelled – just think of how much that costs. In that sort of case, paying a ransom may even have been cheaper! So it's not the case that organisations cannot recover from these attacks – it's whether they have the time to do it."

The idea that outdated systems, resulting from a lack of investment, made NHS organisations highly vulnerable gained a lot of traction in the press and social media. Much of the speculation turned out to be unfounded. But are healthcare organisations struggling with legacy equipment?

"The legacy systems out there are quite incredible – 15% of workstations still use Windows XP. That hasn't been supported since about 2014"

"Healthcare organisations are really jacking up their cyber-security efforts," says MacLeod, "but you'll probably find that they've fallen a bit behind the curve. They're probably behind places like financial services organisations, so there is a lot of spending, a lot of work they have to do around cyber-security."

He adds: "The legacy systems out there are quite incredible – 15% of workstations still use Windows XP. That hasn't been supported since about 2014. You have a lot of very specialised equipment – this could be x-ray machines and other scanners – and very often these are connected to the suppliers, sometimes via the Internet, sometimes via VPNs. But very often they've been installed and set up with default passwords, so that's another area that hackers could look to exploit. They are a great target for ransomware-style attacks, because of the time criticality of the data that they hold."



Who people trust with their healthcare data. Source: Accenture (see box).

Inappropriate sharing

There are other ways that data can be abused. Recently, a deal between the NHS and Google's DeepMind operation has come under attack.[10] The deal was made in 2015 and provides DeepMind with anonymised patient records for use in its Streams app. This monitors for signs of kidney problems and is used in the Royal Free London NHS Foundation Trust and other hospitals. However, there are now strong concerns over the legal basis of the deal and whether the use of the 1.6 million patient records is appropriate.

"The data that was provided to DeepMind went with certain caveats in place," explains MacLeod, "but it appears that those caveats were probably legally unenforceable and the scope of how that data was used by DeepMind went a lot further than the original intention of the trust."

Data is a two-edged sword. It's obviously valuable, both in terms of utility and commercial worth, but can cause great damage when leaked or used in the wrong way. That latter point is important because we increasingly acquire and store data without having a clear-enough idea of why we are doing that and whether it's necessary. MacLeod points to a system in use in 2,700 medical practitioners' practices around the UK where a single click decides whether a particular record can be included in 'advanced data sharing'. "But by simply switching that button, you open up the potential to expose confidential data to people with no need to have it," says MacLeod, "and that would be a breach of the Data Protection Act."

"That information is being shared, whether we like it or not. It has to be stored somewhere. The problem is mainly around how comfortable we are with that data being shared and who has access to it"

This is a critical issue not just because the volumes of data being collected are increasing but because many healthcare organisations are becoming dependent on it for developing their services and products. And it's now common for patient records to be passed around – for example, from a GP to a hospital or a consultant – in order to ensure that all practitioners have access to the fullest and most accurate information. But it's easy to see how that movement of data can introduce vulnerabilities.

"That information is being shared, whether we like it or not," says MacLeod. "It has to be stored somewhere. The problem is mainly around how comfortable we are with it being shared and who has access to it. We're covered by various legalities and things like the Data Protection Act. GDPR [the EU General Data Protection Regulation] will cover this as well."

However, there is a history of how things can go wrong, says MacLeod. He points to the NHS England Care.data scheme, which was pronounced dead in the middle of 2016.[11] The intention was to store anonymised patient data in a central repository to be managed by the Health and Social Care Information Centre (HSCIC). The plan was paused several times because of concerns over patient confidentiality and the clumsy and chaotic approach to patient opt-outs.

"People were uncomfortable with the amount of sharing," says MacLeod, "and the amount of people with no [valid] reason that may have access to that data."

The NHS does have a data-sharing system, known as Spine, used by health and social care professionals.[12] It manages summary care records, electronic prescriptions and referrals. However, as fast as healthcare service providers push for greater use of technology, it seems members of the public and privacy professionals push back – which is what led to the demise of Care.data.

Across the pond

The picture in the US is different, MacLeod points out – perhaps ironically because the healthcare system there is much more disjointed.

"They have numerous independent organisations, mostly run on a commercial basis," he says. "You also have a number of healthcare plan providers – insurance people. They've a whole commercial organisation behind healthcare in the US that we don't have here, so a lot of information is shared between people like healthcare plan providers, hospitals, etc."

With any disjointed system tied together with IT there is usually a lot of scope for security issues to creep in. Does this mean that the UK, with its more homogenous environment is in a better position to make itself secure?

"You would think so," says MacLeod. However, it's not quite as simple as that. He points out that even in the UK there are 20,000 organisations involved in the NHS. While the number in the US is

Data breaches and consumer confidence

A recent survey by Accenture found that 13% of consumers in England have had personal medical information stolen via some form of technology. Perhaps surprisingly, more than a third (35%) of these breaches occurred in pharmacies, followed by hospitals (29%), urgent care clinics (21%), physician's offices (19%) and retail clinics (14%). Also, more than one-third (36%) discovered the breach themselves or learned about it by noting an error on their health records or credit card statement. Only a fifth (20%) were alerted to the breach by the organisation where it occurred and even fewer (14%) were alerted by a government agency.

Nevertheless, most consumers still trust their healthcare providers (84%), labs (80%) and hospitals (79%) to keep their healthcare data secure, although the level of trust isn't so good for the government (59%) or health technology companies (42%) to do so.

In response to a breach, nearly all (95%) of the consumers who were data-breach victims reported that the company holding their data took some type of action. Some organisations explained how they fixed the problem causing the breach (cited by 29%), explained how they would prevent future breaches (23%) or explained the consequences of the breach (22%).

There's more information available here: https://accntu.re/2sgOi7k

greater – and many of them are in direct commercial competition with each other – they have actually seen the advantage of collaboration when it comes to sharing security information.

"If a hospital in one state sees a particular spear-phishing attack, it would be good for them to share that information with a wider community so that the next hospital to receive a similar attack might recognise it," he says. "If I'm hit with a piece of malware, I might want to share that file hash out to the wider community, so that other organisations, other hospitals, can proactively scan their networks to see if it has infected them already."

Much of this sharing is enabled by the HITRUST Alliance, a not-for-profit organisation founded in 2007.[13] As well as threat intelligence sharing, it also develops risk and compliance management frameworks. And it provides a portal through which healthcare organisations can share information directly between themselves, "almost like an information sharing analysis centre [ISAC] type of community," says MacLeod. Organisations can share data such as IP or email addresses used in attacks, file hashes for malware and so on.

"They can also collaborate to build up more strategic intelligence," MacLeod adds.

There's nothing quite like this in the UK yet, although NHS Digital did launch CareCERT, which provides an emergency response team security assessment, awareness training and other information security services to the health service.[14] With the prevalence of phishing in attacks targeted at healthcare organisations, that security awareness training could be one of the most effective tools.

"The easiest vector into a hospital is via spear-phishing," says MacLeod. "If we haven't educated the people who are receiving those emails – what to look out for, how to spot a fraudulent email, how not to click on attachments if you're unsure what they are – a lot of the other things, like perimeter security devices, can be got around."

In the US, MacLeod believes healthcare organisations are doing quite well in terms of carrying out vulnerability assessments and penetration testing, exploiting the benefits of next-generation firewalls and implementing defences against distributed denial of service attacks. And they are leveraging cyberthreat intelligence.

"Within the UK, everything's a top-down approach," he says. "I would hope to see some sort of initiative from NHS Digital through the CareCERT programme – maybe having them act as a central point for cyberthreat intelligence. But it really takes the involvement of each and every organisation, NHS trust and hospital to use that data and to contribute to it, to make sure that everyone is aware of what threats are affecting them."

Moving forward

This sounds like healthcare organisations are at least making efforts. The question is, is it enough?

"Organisations may have to look at the next attacks that are coming through. Those could be things like large-scale denial of service attacks. It could get a lot more sinister, though"

"They're on the right track," says MacLeod. "Budgets are always an issue, but it really is a case of bolstering your defences as much as possible. There's a lot of work that's come up through the Care Quality Commission, that speaks about addressing legacy systems within organisations. [UK Health Secretary] Jeremy Hunt last year announced a £4bn investment in NHS technology over the next five years.[15] And of that, about £1bn was earmarked for infrastructure, data consent and cyber-security. So it's a great time to start putting plans in place in terms of what defences need to be bolstered, to start looking at getting rid of machines within an organisation that are no longer supportable – those Windows XP boxes – and to evaluate relationships with third-party suppliers, such as how they connect up remotely to systems, whether they have done due diligence in disabling default passwords and securing those boxes themselves."

He adds: "Security awareness is still very important: teaching the staff how to recognise phishing emails, recognising what to do with them and then tying that into a cyberthreat intelligence package where they have the ability to take those spear-phishing emails and forward them directly to the platform.”

Using such solutions, staff can play a part in building up incident reports and identifying indicators of compromise. In the US, with systems such as HITRUST, these can then be shared with other participants. “I’d love to see something similar in the UK,” says MacLeod.

When it comes to what we can expect next in this sector and the challenges that are on the horizon, MacLeod believes that it all depends on how we respond to what’s happening now. The switch in focus from stealing and selling patient data to ransomware is all about monetisation.

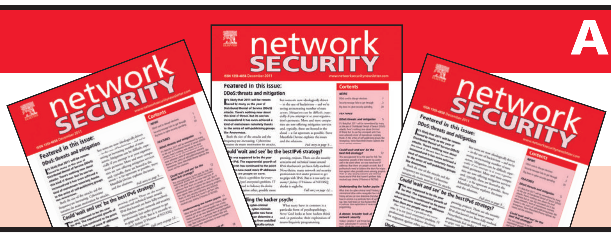
“Everything has moved across to ransomware attacks and the way we respond to those will probably dictate how attackers treat us next,” says MacLeod. “If they’re able to monetise ransomware attacks, they will continue to happen. But if we start defending ourselves against them, hospitals and healthcare organisations may have to look at the next attacks that are coming through. Those could be things like large-scale denial of service attacks. It could get a lot more sinister, though. A lot of serious medical equipment is connected up to the Internet and is potentially vulnerable. People hacking into those systems, changing settings, could have the ability to cause loss of life.”

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. *He also blogs and podcasts on information security issues at Contrarisk.com.*

References

1. ‘Probe after NHS Orkney patient records found on pavement’. BBC News, 15 Jul 2014. Accessed May 2017. www.bbc.com/news/uk-scotland-north-east-orkney-shetland-28314887.
2. Campbell, Denis; Duncan, Pamela. ‘NHS accused of covering up huge data loss that put thousands at risk’. The Guardian, 27 Feb 2017. Accessed May 2017. www.theguardian.com/society/2017/feb/26/nhs-accused-of-covering-up-huge-data-loss-that-put-thousands-at-risk.
3. Gayle, D; Topping, A; Sample, I; March, S; Dodd, V. ‘NHS seeks to recover from global cyber-attack as security concerns resurface’. The Guardian, 13 May 2017. Accessed May 2017. www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack.
4. ‘California Hospital Pays $17,000 To Hackers In ‘Ransomware’ Attack’. CBS, 18 Feb 2016. Accessed May 2017. http://sanfrancisco.cbslocal.com/2016/02/18/california-hospital-ransomware-attack-hackers/.
5. Davis, Jessica. ‘Ransomware: See the 14 hospitals attacked so far in 2016’. Healthcare IT News, 5 Oct 2016. Accessed May 2017. www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016.
6. ‘47% of NHS Trusts in England admit to falling victim to ransomware’. NCC Group, 24 Aug 2016. Accessed May 2017. www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2016/august/47-of-nhs-trusts-in-england-admit-to-falling-victim-to-ransomware/.
7. Leyden, John. ‘Ransomware brutes smacked 1 in 3 NHS trusts last year’. The Register, 17 Jan 2017. Accessed May 2017. www.theregister.co.uk/2017/01/17/nhs_ransomware/.
8. Burton, Graeme. ‘Globe2 ransomware blamed for Lincolnshire NHS trust cyber-attack’. Computing, 5 Dec 2016. Accessed May 2017. www.computing.co.uk/ctg/news/2479109/globe2-ransomware-blamed-for-lincolnshire-nhs-trust-cyber-attack.
9. ‘London NHS trust fined for HIV newsletter data breach’. Information Commissioner’s Office, 9 May 2016. Accessed May 2017. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/05/london-nhs-trust-fined-for-hiv-newsletter-data-breach/.
10. Burgess, Matt. ‘DeepMind accused of accessing NHS data on an “inappropriate legal basis”’. Wired, 17 May 2017. Accessed May 2017. www.wired.co.uk/article/deepmind-nhs-data-sharing-privacy-concerns.
11. Evenstad, Lis. ‘NHS England scraps controversial Care.data programme’. ComputerWeekly, 6 Jul 2016. Accessed May 2017. www.computerweekly.com/news/450299728/Caldicott-review-recommends-eight-point-consent-model-for-patient-data-sharing.
12. Spine, home page. NHS Digital. Accessed May 2017. https://digital.nhs.uk/spine.
13. HITRUST Alliance, home page. Accessed May 2017. https://hitrustalliance.net.
14. Hoeksma, Jon. ‘NHS Digital to roll out new CareCERT cyber-security services’. DigitalHealth, 15 Sep 2016. Accessed May 2017. www.digitalhealth.net/2016/09/nhs-digital-to-roll-out-new-carecert-cyber-security-services/.
15. Metzger, Max. ‘£4bn investment for NHS digital transformation’. SC Magazine, 8 Feb 2016. Accessed May 2017. www.scmagazineuk.com/4bn-investment-for-nhs-digital-transformation/article/531430/.



The Firewall

Securing emails

Colin Tankard, Digital Pathways

Of all the millions of emails sent each day, how many senders even think about whether their messages are secure? Traditional email has the confidentiality level of a postcard – anyone involved in its transport can easily read it. Lack of care becomes even more of a problem when the sender is attaching confidential or sensitive data. Is it being sent to the correct person? Should the attachment be allowed? Even if it is all right to send, how do you know it was received, when was it read and has it been forwarded? Current system notification is not good enough.

With General Data Protection Regulation (GDPR) fines looming, now is the time to gain control of emails.

With a secure email system, correspondence is protected and verified, giving information on the date opened, etc. It gives you peace of mind. The flaw in many of these secure email systems is that they are on a one-to-one basis – ie, a company to an individual or a company to a company – which means no collaboration outside of these groups.

What is required is a way to transform your email into a confidential and auditable electronic letter that can collaborate with any email box, enabling one single credential accessible to all. Such systems are emerging but the key to their success will be ease of use, level of encryption and the other complementary services they offer, such as secure collaborative storage.

One system available works by using your existing email address and prevents any third party accessing or storing the content of your email. After registering, you can read and write secure emails on the web portal or you can use client software. This service allows companies to share sensitive data in-house or to external clients/partners through a highly secure process of user identification, authorisation and secure delivery without the need to replace any existing systems. Furthermore, if the recipient likes the solution they can adopt it and use their credentials to invite others to join. This is something you can’t do with other secure email systems.

Secure storage is often advertised, but who holds the key is rarely discussed, as it is complicated to set up a system that enables the data owner to hold the key and even more complicated to share the key, to enable collaboration.

The creator of an individual securebox electronically invites other members and assigns user rights. Upon acceptance of an invitation, the user will be admitted to this securebox and will also receive online web access. The user may also choose to automatically replicate parts, or all, of the securebox onto their own infrastructure, from smartphone to server.

One of the most criticised facts about cloud services is the lack of security of stored data. In order to make sure that your securebox data is always secured, all encryption and decryption is done ‘on the fly,’ so that even the provider who hosts the data is not able to peek into your files.

The way email and the sharing of documents is handled needs to be rethought, especially with GDPR and its requirement to track and disclose sensitive data. The excuse that an email went astray will no longer be tolerated. It is now time to implement secure services so that, come May 2018, all electronic communications will be secure and auditable.

EVENTS CALENDAR

4 July 2017
Cyber Security Summit
London, UK
http://www.cybersecurityconference.co.uk/

8 July 2017
Steelcon
Sheffield,UK
http://bit.ly/2oj2h9X

11–13 July 2017
International Conference on Digital Security and Forensics
Kuala Lumpur, Malaysia
http://bit.ly/2n6jPGd

22–27 July 2017
Black Hat USA
Las Vegas, US
www.blackhat.com

27–30 July 2017
DefCon
Las Vegas, US
www.defcon.org

31 July–7 August 2017
IEEE Cyber 2017
Hawaii, US
http://ieee-cyber.org/2017/

4–8 August 2017
SHA2017
Amsterdam, Netherlands
https://sha2017.org/

8 August 2017
Cyber Security Summit Chicago
Chicago, Illinois, US
https://cybersummitusa.com/2017-chicago/

12 August 2017
3rd International Conference on Cyber Security
Kota, India
www.iccs2017.iaasse.org