ELSEVIER

network SECURITY

ISSN 1353-4858 March 2017

www.networksecuritynewsletter.com

Featured in this issue:

Encryption as the cornerstone of big data security

Big data programmes benefit organisations in many ways, driving competitiveness and innovation. But they can also increase security risks owing to the vast amount of sensitive information they hold.

Big data sets harness information from multiple sources such as databases, data warehouses, log and event files, security controls such as intrusion prevention systems and user-generated data from sources such as emails and social media posts. So data security is a must for any organisation, and encryption needs to be a key part of that, says Colin Tankard of Digital Pathways.

Full story on page 5…

National infrastructure – the next step for seasoned hackers

Due to the advancing capabilities of hackers and the ever-decreasing adequacy of traditional perimeter security solutions, national infrastructure operators must turn towards innovation to solve major cyber-security gaps.

These issues will only grow more significant over time. Any change is fraught with challenges, but cyber-security needs to be tackled head-on if the organisations responsible for supplying our clean water, electricity and fuel can be trusted as proactively tackling this complicated problem, says Lewis Henderson of Glasswall Solutions.

Full story on page 8…

Software vulnerability management: how intelligence helps reduce the risk

Every year, thousands of software vulnerabilities are discovered in thousands of products, and the exploitation of these vulnerabilities can cause extensive damage.

The proactive nature of software vulnerability management presupposes that it is less costly to avoid attacks than to fix the problem afterwards. Therefore, organisations need to understand what IT assets exist within their environments that could be the target of attack. A thorough programme founded upon vulnerability intelligence will help minimise the attack surface, says Vincent Smyth of Flexera Software.

Full story on page 10…

Financial institutions become more confident about cyber-security but weaknesses remain

Research carried out by Accenture, the professional services firm, shows that 78% of banks and financial institutions are confident about their overall cyber-security strategy. And about half have "high confidence" in their organisation's ability to identify the cause of a breach, measure its impact and manage the associated financial risk.

However, other statistics somewhat undermine this rosy picture. For one

Continued on page 2…

Contents

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: 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

thing, more than half (52%) of those questioned said they weren't confident their organisations could detect a breach via internal monitoring. And nearly half (48%) recognised that internal breaches have a greater impact than external threats. This is in an environment where organisations report an average of 85 serious breach attempts a year with more than a third (36%) of those being successful (defined as the attackers obtaining some information). And 59% of the affected banks admitted it took months for them to detect the attacks.

"Banks have traditionally prioritised their cyber-security investment around building higher, more secure walls," said Chris Thompson, senior managing director and head of financial services cyber-security and resilience, Accenture Security. "But this has often been to the detriment of their internal capabilities. While defending the perimeter is crucial, it's often the people inside the walls that present the biggest risk."

Part of the problem may lay in poor code. A study by software firm CAST, analysing more than a billion lines of code across 1,850 applications, concludes that the drive to add functionality to corporate systems is resulting in sub-standard code and that this issue is particularly acute in financial solutions. There's more information here: http://bit.ly/2ndo0QW.

These issues may be offset by the fact that financial institutions are ramping up their security spend. According to the 'Financial Institutions Security Risks' research from Kaspersky Lab and B2B International, security investment is a high priority for banks and financial institutions. Retail banks spend three times as much on IT security as comparably sized non-financial institutions. Moreover, 64% of banks say that they will invest in improving their IT security regardless of the return-on-investment.

Emerging risks related to mobile banking are highlighted in the report as a trend that can expose banks to new cyberthreats. Some 42% of banks predict that an overwhelming majority of their customers will use mobile banking within three years, but admit that users are too careless in their online behaviour.

There's more information here: http://bit.ly/2m7BFaz.

Zero-days last for years

A new study from the RAND Corporation, based on data about zero-day vulnerabilities, concludes that the average life expectancy for one of these bugs before it is publicly disclosed and patched is 6.9 years. Only a quarter of them survive for less than 18 months.

This comes at a time when CIA documents leaked by Wikileaks suggest that the agency has been stockpiling zero-days, contrary to stated US policy. The common consensus is that not alerting software vendors about zero-days makes everyone vulnerable. But the RAND research found that the likelihood of two people finding the same vulnerability is low. For a given stockpile of zero-days, only around 5.7% will be discovered by an outside entity in the span of a year.

The dataset studied by RAND covered 200 zero-days spanning 14 years, around half of which have still not been publicly disclosed. There's more information available here: http://bit.ly/2n7eF0w.

"The findings of the study are indeed aligned with the work we have done in vulnerability research, and I dare say that the problem is much larger than the recent CIA exposure and the RAND indicate," said Mike Ahmadi, global director of critical systems security at Synopsys. "We regularly find multiple zero-day vulnerabilities when testing systems, and hundreds if not thousands of known vulnerabilities, which are, in reality, a much bigger problem, due to the frequent presence of known exploits for such vulnerabilities. Because the user is rarely aware of known vulnerabilities, and often does not patch, it has the same effect as a zero-day, with the additional issue of scale."

John Cloonan, director of product at malware detection firm Lastline, said: "The notion of vulnerabilities being stockpiled and reused is not new. There have been a few companies whose business model has been finding and weaponising zero-days. To some extent, the process does leave the general user base at increased risk, however as the research shows there is a low probability of multiple researchers identifying the same vulnerability."

In brief

Toy users' details breached

The CloudPets range of toy animals has leaked the personal details of around 820,000 users. The toys allow parents and children to send and receive messages via a cloud platform. Starting last December, the manufacturer received several warnings that the database driving the service was vulnerable. Like many databases running on the MongoDB platform, it was accessible across the Internet with no password protection. At the beginning of January, someone stole the database, deleted the original and left behind a ransom note. Passwords in the database were hashed with bcrypt. However, the service allowed users to set passwords as short as a single character. Researcher Troy Hunt, who obtained a copy of the database, said he was able to crack a large number of the passwords in a short time. The breach may also have exposed around 2.2 million voice recordings.

ICO probes Brexit campaign

The Information Commissioner's Office (ICO) is investigating whether the Leave.eu campaign illegally used UK citizens' data ahead of the Brexit vote. A report in *The Observer* detailed how the campaign used the services of US-based analytics company Cambridge Analytica. This may have involved the exploitation of personal data in an effort to sway the opinion of voters. Cambridge Analytica is owned by billionaire Robert Mercer who is also part-owner of the right-wing Breitbart News Network, a major donor to Donald Trump's election campaign and a personal friend of Nigel Farage. According to *The Observer*: "Cambridge Analytica, an offshoot of a British company, SCL Group, which has 25 years' experience in military disinformation campaigns and 'election management', claims to use cutting-edge technology to build intimate psychometric profiles of voters to find and target their emotional triggers." The ICO commented: "We are conducting a wide assessment of the data-protection risks arising from the use of data analytics, including for political purposes, and will be contacting a range of organisations. We intend to publicise our findings later this year." There's more information here: http://bit.ly/2mbjXnr.

DoJ drops case to protect Tor hack

The US Department of Justice (DoJ) has dropped a child pornography prosecution in order to protect an exploit it used against the Tor network. Jay Michaud was arrested in 2015 and charged with visiting the Playpen website, a child pornography site hosted on the dark web. Previously, the FBI had seized servers belonging to Playpen but continued to operate them from its own premises for 13 days, spying on visitors to the site. Michaud was one of 137 people indicted as a result. He had used the Tor browser, but it's believed the FBI used malware to eliminate the privacy normally provided by Tor and obtain IP addresses, MAC addresses and other private data belonging to visitors. However, the exact tools and methods used are classified, and it's in order to avoid breaching the secrecy surrounding the FBI's operations that the DoJ has asked the judge to dismiss the case against Michaud 'without prejudice'.

VoIP backdoor

Pretty much all devices made by Chinese VoIP specialist DBL Technology seem to have backdoors in them, probably intended as a debugging feature, according to researchers at Trustwave. A telnet server running on the devices provides limited information to remote users through accounts named 'ctlcmd' and 'limitsh', which both require the user-set administrator password. However, there's also an undocumented 'dbladm' account that gives root-level shell access and uses a challenge/response authentication method. Anyone with knowledge of the protocol can therefore take control of the device. When advised of the issue, the manufacturer made the authentication a little more complex, but not enough to defeat a determined attacker.

Europol warns of rise in criminal gangs

The number of criminal gangs operating in Europe has surged to 5,000, says Europol, with many of them engaged in ransomware attacks. While people smuggling is arguably the most serious of the gang-related activities, the law enforcement agency warned that technology has become the "primary facilitator" for illegal activities, much of which have been enabled by the darknet. There has been a rapid rise in criminal 'entrepreneurs', many of whom carry out illicit trade, such as drug dealing, from their homes over the Internet.

Ransomware worms its way through networks

The threat from ransomware has stepped up a notch. Javelin Networks has reported finding a variant it's called Samas RansomWorm because of its ability to spread through a network. Most ransomware simply infects the machine on which it's initially installed. But the new variant steals domain credentials, identifies potential targets on the network via Active Directory and then spreads, potentially infecting all workstations, servers and even back-ups in a domain. There's more information here: http://bit.ly/2ndXZkB.

BEC nets $3bn in West Africa

Criminals operating out of West Africa have netted around $3bn in three years using business email compromise (BEC) schemes against targets worldwide, according to research carried out by Interpol and Trend Micro. Also known (less accurately) as 'CEO fraud', BEC tricks firms into transferring funds to the attackers' accounts through the use of fake invoices or spoofed messages from executives within the target organisations. There's more information here: http://bit.ly/2n7NDG5.

Spammer breached

A database of 1.4 billion email addresses used by an alleged spamming operation was openly available on the Internet. MacKeeper security researcher Chris Vickery found a number of files that were accessible and unprotected belonging to an organisation called River City Media (RCM). Although it styled itself as a marketing agency, RCM has been accused of spamming and all of its infrastructure is now blacklisted by RBL operator Spamhaus. As well as email addresses, some of the files also contained IP and even physical addresses.

Unpatched software

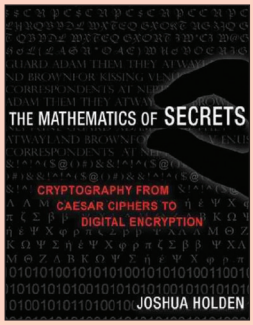
The average private user in the UK has 72 programs installed on their PC, and 6.7% of them are end-of-life programs that are no longer patched by the vendor. Such packages are popular attack vectors for hackers because they are so widespread. These figures come from reports for 12 countries published by Secunia Research at Flexera Software. The research also found that 7.2% of users had unpatched Windows operating systems in Q4 2016, up from 6.4% in the previous quarter but down from 8% in the same quarter in 2015. The top three most exposed programmes for Q4 2016 were Apple iTunes 12.x (53% unpatched, 29 vulnerabilities), Oracle Java JRE 1.8.x/8.x (45% unpatched, 39 vulnerabilities) and VLC Media Player 2.x (36% unpatched, five vulnerabilities). There's more information here: http://bit.ly/2mrOxdk.

DDoS victims blame rivals

Worldwide, nearly half (43%) of the victims of distributed denial of service (DDoS) attacks believe that their business rivals are to blame, according to research by Kaspersky Labs. Only 38% put the blame on cyber-criminals. When it comes to why they were attacked, the vast majority of firms put it down to industrial espionage, with disgruntled former employees and politically motivated attacks coming much further down the list. There are some regional differences: in the Asia Pacific region, business rivals were blamed by 56% of victims, with 33% suspecting former staff and 28% pointing the finger at foreign governments. In Western Europe, competitors were blamed by only 37% of firms, and foreign governments attracted far less suspicion, being accused in only 17% of cases. There's more information here: http://bit.ly/2mJIDXq.

Reviews

BOOK REVIEW



The Mathematics of Secrets
Joshua Holden. Published by Princeton University Press. ISBN: 9780691141756. Price: $29.95, 392pgs, hardback. E-book edition also available.

Encryption is a fundamental component of information security, yet it is also frequently misunderstood and misused. And while strong encryption is readily available to anyone who wants to use it (to the chagrin of law enforcement and intelligence agencies), it's easy to make mistakes that undermine the secrecy that it is meant to provide.

One of the problems with encryption is that it is a profoundly technical field, requiring a high-level grasp of mathematics. Weaknesses in encryption algorithms come from corner cases and (to most people) incomprehensible convolutions of logic.

There is a reason there's a saying in the software development world: 'Never roll your own crypto'. Even if you're a highly skilled and experienced coder, none of that counts for much in the crypto world. So while you may think your encryption method is strong and clever, a cryptanalyst will know of all manner of ways of attacking it that are simply unimaginable to you.

Sadly, too many software developers will continue to devise their own novel schemes for protecting information that will continue to be broken. And others will use existing crypto libraries and algorithms that, while strong in themselves, are rendered vulnerable by their misapplication.

Those developers need to read this book, for a couple of reasons. First, it should convince them that encryption is the realm of mathematicians, not people with Python or even C coding skills. It's arcane and it's complex. If you find any part of *The Mathematics of Secrets* a stretch when it comes to comprehension, you should not be attempting crypto by yourself. Second, the historical overview provided by the book demonstrates a sad but important truth about encryption methods – they all end up broken eventually.

We've seen this just recently. Hashing algorithms lie at the heart of much cryptography. And one of the critical features of such algorithms is that the output should be unique to a given input. Years ago, the once mighty MD5 algorithm was demonstrated to suffer from 'collisions', where two different inputs produce the same output. Now, after a couple of years of speculation and theoretical work, the same has been shown, by a couple of Google researchers, to be true of SHA-1. They produced two different PDF documents that encoded as the same hash.

"The historical overview provided by the book demonstrates a sad but important truth about encryption methods – they all end up broken eventually"

This is so important to the security of our data that steps have been taken to protect us. For example, Google's Chrome browser will throw up warnings about SSL certificates that have been signed using SHA-1 hashes. And Microsoft has just released a tool for programmers that warns about the use of, for example, MD5 or SHA-1 functions to create hashes.

It's important for developers and information security practitioners to stay current with regard to best practices around which crypto libraries and algorithms to use, and there are guidelines for that. Where books like *The Mathematics of Secrets* can play a role is not in the practical aspects of employing cryptography but in understanding what lies behind it.

There have been some excellent books on the history and development of crypto. David Khan's *The Codebreakers*, *Crypto* by Steven Levy and *The Code Book* by Simon Singh all provide accessible guides both to the history and the basic principles of cryptography. But those are largely aimed at a general audience and steer away from the most difficult element of the subject – mathematics.

Joshua Holden isn't so shy. This work specifically looks at the essential mathematical foundation of codes. Ultimately you can't separate cryptography solutions from the mathematics that drive them. If you want to convince yourself that your encryption methods are genuinely secure, you have to employ maths to do that. Similarly, if you want to attack a cipher, you'd better be a mathematician.

Flipping through the book you will see a number of equations, although they're outnumbered by graphs and diagrams. Holden suggests that a high school level grasp of algebra, plus "a willingness to think really hard about it" is all you need to get through the book, and that seems about right. And it's not as though you need to solve the equations – you just need to understand intuitively what they're illustrating.

The first couple of chapters take us through the history of ciphers and some familiar names crop up here – Caesar's cipher, Vigenère and so on. But right from the beginning Holden takes a mathematical perspective, such as examining the probabilities of certain letters appearing in simple substitution ciphers.

As it's not attempting to be a manual on how to create or break ciphers, Holden is able to moderate the complexity of the mathematics to keep the text within the grasp of keen readers who, however, haven't undertaken college-level maths courses while satisfying his aim of showing that, fundamentally, cryptography *is* mathematics.

So who should read this book and what does it achieve? If you are a software developer or information security practitioner and want a deeper understanding of how crypto works than you can get from the books aimed at more general readers, then *The Mathematics of Secrets* definitely fits the bill. The section on public key cryptography is especially valuable. The same goes for the general reader who is curious about how our information is protected and isn't scared by algebra. The book does a great job of illuminating the mechanisms underpinning cryptography – how they work and why, sometimes, they don't.

There is also a final section on the future of crypto, including quantum cryptography which is making more than a few people nervous. Inevitably some of this is speculative, but it drives home an important message. Our privacy and security rely on the innovative and inspired products of mathematical minds – the same minds that are deployed to break those products. Crypto never stands still – it is constantly evolving, leaving old methods unreliable and even dangerous. If you want to ensure your safety, you not only need to use cryptography, you need to understand it. This book goes a long way to helping with that.

There's more information available here: http://press.princeton.edu/titles/10826.html.

– SM-D

Encryption as the cornerstone of big data security

Colin Tankard

Colin Tankard, Digital Pathways

Big data refers to huge data sets that have come about through the phenomenal growth being seen in the volume of information collected, produced, analysed, shared and stored by organisations. By analysing big data sets, valuable insights can be gained into how patterns of data are associated to enable better-informed decision-making, which can aid in competitiveness and drive innovation. According to Gartner, 48% of organisations had invested in big data capabilities in 2016.

Big data sets harness information from multiple sources such as databases, data warehouses, log and event files, security controls such as intrusion prevention systems and user-generated data from sources such as emails and social media posts. The information collected can be in either structured form, such as in the columns of a database, or unstructured, such as information contained in a word-processing document. Increasingly, data feeds are from devices – and transactions from devices –that make up the Internet of Things (IoT) and this looks set to increase dramatically. As well as this, an increasing number of organisations are looking to incorporate data feeds from physical security systems, such as building access control and smart building management systems.

Swathes of information

All of this information is fed into a centralised big data management system so that the data can be correlated for analysis. Much of that data will be highly sensitive, including information related to customers, employees and suppliers, financial data, intellectual property and a vast array of other information. Some of the information will come from within the network: other sources may be remote, such as in cloud applications, data held on mobile devices and that originating from the IoT.

Breaches of sensitive information expose organisations to many risks, including theft of intellectual property, loss of revenue or reputational damage. Other risks include financial penalties and other sanctions for non-compliance with regulations demanding that high levels of security be applied to sensitive data. The need to protect personally identifiable information is currently top of mind for many executives preparing for compliance with the forthcoming EU General Data Protection Regulation (GDPR). Compliance is mandatory as of late May 2018 and sanctions for non-compliance can be severe.

"It can be challenging to find all potentially sensitive information and to understand relationships among data sets. Tracking which users have access to sensitive data can also be difficult"

For reasons such as these, security is a key consideration when designing big data analysis projects and programmes. According to IBM, there are a number of challenges in securing big data environments. It can be challenging to find all potentially sensitive information and to understand relationships among data sets. Tracking which users have access to sensitive data can also be difficult, especially where security controls are inconsistent, applied differently in traditional and big data environments and because access must be controlled across so many disparate data sources. IBM urges that organisations should plan ahead for security when implementing big data programmes, ensuring that security is considered strategically and built into all big data environments from the start.

As shown in Figure 1, data governance can be more of a concern in big data environments than in traditional systems.[1] This requires that organisations must take a proactive approach to privacy, security and governance with big data programmes, in order to ensure that all data and the insights that can be gained from the data are protected and secure.

Security through encryption

Encryption and key management should be considered the cornerstone of any data security strategy and big data programmes are no exception. Encryption can dramatically lower the risks associated with data compromise. According to ENISA (European Union Agency for

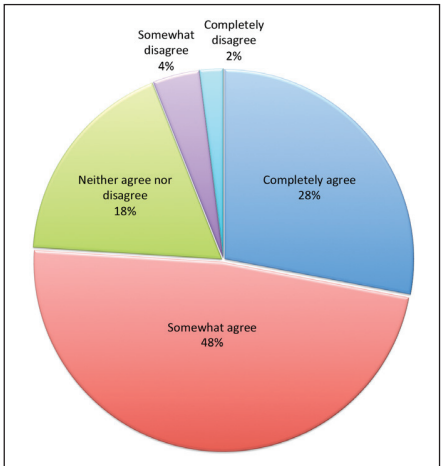


Figure 1: Responses to the statement, 'Data governance is more of a concern with big data analytics than it is with traditional systems'. Source: Vanson Bourne, SoftServe big data analytics report 2016.

Network and Information Security), the following are essential for protecting data in big data environments:

- Encrypt data in transit and at rest, to ensure data confidentiality and integrity.
- Ensure a proper encryption key management solution is deployed, considering the vast amounts of devices that must be covered.
- Consider the timeframe for which data must be kept – data protection regulations might require that you dispose of some data due to its nature after a certain time period.
- Design databases with confidentiality in mind – for example, any confidential data could be contained in separate fields so that they can be easily filtered out and/or encrypted.

The main drivers for using encryption technology solutions are shown in Figure 2.[2]

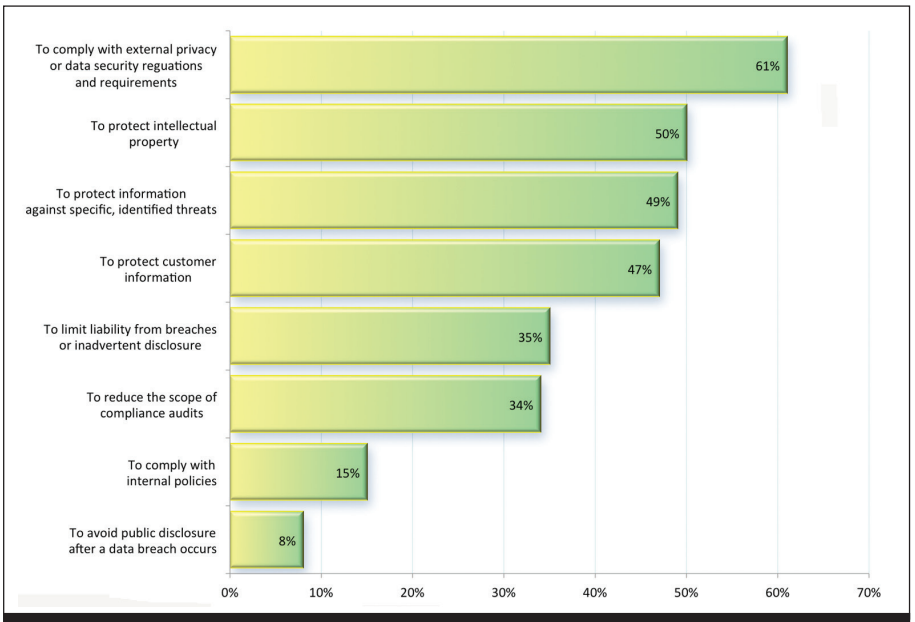


Figure 2: Main drivers for using encryption technology solutions. Source: Thales e-Security/ Ponemon Institute.

All sensitive data should be encrypted, including that in databases, spreadsheets, word documents, presentations and archives. At some point, data may move out of the organisation, perhaps communicated among employees and business partners, or placed in the cloud for storage, where it can be accessed via mobile devices. When data is moved out of an organisation, it is vital that the encryption keys remain within the organisation to prevent anyone inappropriately accessing the keys, which will allow them to decrypt and read the data. If the keys are not protected, employees of the cloud service provider could potentially access data, or it could be subject to demands by government agencies that data be handed over, often without the knowledge of the organisation that owns the data. Ensuring that encryption keys are not stored with encrypted data will also help to prevent the data being compromised by hackers.

Many laws that demand that affected parties and authorities be notified in the event of a breach provide a safe harbour if the data that is stolen has been adequately encrypted so that notification is not necessary. Even where a regulation does not provide this safe harbour, the use of encryption will be considered when the safeguards that an organisation has put in place are investigated, potentially reducing the sanctions that could be applied.

The new General Data Protection Regulation of the EU that becomes effective in May 2018 requires that 'appropriate safeguards' are applied to the personal data of EU citizens when that data is collected and processed. However, as with many regulations and standards, little guidance is provided within the GDPR regarding what those safeguards should be. The exceptions to that are the calling out of encryption and pseudonymisation as appropriate protections. Pseudonymisation looks to anonymise data by removing unique identifiers. However, it is not deemed to be as secure as encryption since, in some noteworthy cases, anonymised data has been de-anonymised using other publicly available data. To prevent this, anonymised data should never be stored alongside other data in plain text that could lead to an individual being identified.

The scope of data protection has also been broadened out with the GDPR to encompass any organisation that handles data related to EU citizens, regardless of where the organisation is based or the data is stored. Sanctions for non-compliance can also now be meted out to organisations that are merely processing data, perhaps on behalf of others, rather than just those who are considered to be data controllers.

Any organisation performing big data projects should now be in the process of preparing to meet the compliance challenges of the GDPR, especially since the fines for non-compliance have been increased considerably. It is likely that any big data project includes information related to individuals, providing another reason why data security is essential. The use of encryption will go a long way towards providing that security.

While encryption will help to protect data from misuse, fraud or loss, it is essential that the ability to perform big data analysis is preserved. IBM has published some best practice guidelines for ensuring this. It recommends that data be masked both to protect the actual information from theft or loss and also so that there is a functional substitute for occasions when the real data is not required, in order to boost privacy. Sensitive data can be masked either at its source or within the big data platform. Unstructured information such as that found in textual, graphical and form-based documents should be redacted to protect it from misuse. IBM also reiterates that data should be encrypted when at rest and in motion and stresses that a combination of these measures will provide the best protection and help an

organisation to better achieve good data governance and regulatory compliance.

Data classification is also key for enabling sensitive data to be identified and therefore better protected. Data classification will help to determine which data is the most sensitive and where it is stored. This is something that should not just be left to the IT department, but should include the involvement of line-of-business personnel since they are likely to best understand the sensitivity of the data with which they work. It should also include compliance officers who are tasked with keeping abreast of new regulatory requirements. This is not a one-off process, but something that should be reviewed regularly. IBM states that the 'crown jewels' of an enterprise should be prioritised for protection above all other data and investigation should be made into where a data breach could most negatively impact the business.

Integrated security platform

When dealing with big data environments that touch so many parts of the organisation, encryption also needs to be pervasive. This requires that it is provided as a platform that offers granular controls, robust encryption and centralised management incorporating all data sources being used for big data analysis. This will help to optimise efficiency and ease security concerns, as all sensitive data sources will be included in the encryption programme, as well as making compliance easier to achieve. It will ensure that policies can be applied in a consistent manner, reducing the administrative effort associated with encryption. This will also free up personnel from time-consuming tasks so that they are able to focus on the core task of big data analysis.

While encryption should be the cornerstone of data security for any organisation, it is not sufficient in isolation. Rather, it should be tightly integrated with other security controls, including endpoint security, network security, application security and physical security systems, which are increasingly being run over IP-based networks.

Granular access controls are a must, especially since decrypting data for analysis leaves data in the clear. Once a user is granted access to an encryption key, it is necessary to track all their interactions with the data, including what they access and what they do with the data. Access must be continuously controlled, enforcing strict adherence to the entitlements that a particular user has been given. This is even more essential for privileged users, who often have access to the most sensitive information. Enforcing access controls works best when the security platform being used is tied into user management directories such as Active Directory or other LDAP systems that are currently used by most organisations for defining and controlling which users can access what.

"Once a user is granted access to an encryption key, it is necessary to track all their interactions with the data, including what they access and what they do with the data"

By tightly enforcing access controls, users can be prevented from providing access to others that have not been granted similar entitlements, so ensuring that unauthorised users cannot gain access to sensitive data. Access control enforcement will also help considerably in auditing and reporting requirements, increasing the ability of an organisation to achieve and approve compliance with the regulations that they face and in achieving good corporate governance.

For protecting big data environments, encryption technologies should also be integrated with other security controls, including endpoint security, which is especially required given the amount of access by mobile devices in most organisations. This will also become increasingly important as more IoT devices come into use, providing valuable data sources for big data environments. Integration with other security controls such as intrusion prevention systems and firewalls will help to reduce the possibility of big data breaches or the detection of any threats that have impacted the network.

Also useful is integration with security information and event management (SIEM) systems, which is the source of much information used in big data environments, both data feeds in real time and forensic information. SIEM systems provide visibility over events occurring in the network. Once deemed to be valuable primarily for compliance purposes, they have now come into their own for their usefulness in providing actionable intelligence required for improved decision-making and for improving security preparedness and defences.

Conclusions

Big data programmes benefit organisations in many ways, driving competitiveness and innovation. But they can also increase security risks owing to the vast amount of sensitive information that is often included in the huge data sets being analysed. Data security is a must for any organisation for protecting the business. Encryption should be a key part of any big data environment to ensure that sensitive information is adequately protected.

About the author

Colin Tankard is managing director of data security company Digital Pathways, which specialises in the design, implementation and management of systems that ensure the security of all data, whether at rest within the network, in a mobile device, in storage or in transit across public or private networks.

References

1. 'Softserve Big Data Analytics Report'. Softserve, 2016. Accessed Mar 2017. www.softserveinc.com/en-us/newsroom/knowledge-centre/softserve-big-data-analytics-report/.
2. '2016 Global Encryption Trends Study'. Thales e-Security/Ponemon Institute. Accessed Mar 2017. www.thales-esecurity.com/knowledge-base/analyst-reports/global-encryption-trends-study.

National infrastructure – the next step for seasoned hackers

Lewis Henderson

Lewis Henderson, Glasswall Solutions

While the general public may not be aware, those tuned into the realm of cyber-security were likely to have been disturbed by an event that took place in late December 2015. As temperatures continued to drop in Ukraine, hundreds of thousands of households suddenly lost access to power. Many of the country's western residents, including half of those living in the Ivano-Frankivsk Oblast, were left in the cold, with no electricity whatsoever.[1]

The most shocking element of the blackout was its cause. It was later revealed that the systems of three regional operators had been targeted and infected in a BlackEnergy malware attack, in what was the first publicly confirmed hacker-caused power outage to ever occur. The Sandworm Gang, the group of hackers who developed BlackEnergy, are believed to have also been behind a number of attacks targeting government agencies in Ukraine, as well as Poland, including a data breach of the North Atlantic Treaty Organisation (NATO) that occurred in 2014. Due to the intense political climate in Ukraine, certain authorities have accused the Kremlin of pulling the strings for the blackout and the previous attacks, though any solid lines between Moscow and the Sandworm Gang have yet to be drawn.

"Data breaches continue to occur across Japan's national infrastructure organisations as well, putting valuable private data in the hands of unknown, presumably state-sponsored, hacking groups"

Just weeks after the blackout in Ukraine, Israeli Energy Minister Yuval Steinitz shocked attendees of the CyberTech 2016 computer security conference with news that the nation's Electricity Authority had been the target of a "severe" malware attack. Though Steinitz was adamant that the attack did not result in any power outages, *The Times of Israel* reported that some of the authority's computer systems had to be shut down for two days following the attack.[2] So far, it is unclear who are the culprits behind the attack.

More recently, California's Hollywood Presbyterian Medical Centre made headlines around the world when news broke out that it had given in to a vicious ransomware attack. A group of unknown hackers held the hospital's computer systems hostage, demanding 40 bitcoins (£12,050) in return for a digital key that would allow operators to regain control of the systems. The 434-bed hospital quickly agreed to pay the ransom, fearing the consequences of what might have occurred otherwise.

Similar events continue to add up across the globe, with the Parliament of Western Australia announcing a trojan infection had made many of their computers and phones inoperable. Data breaches continue to occur across Japan's national infrastructure organisations as well, putting valuable private data in the hands of unknown, presumably state-sponsored, hacking groups.

Keeping up with growing threats

The world of cybercrime expands incrementally each day, leading to the current state of affairs in which even national infrastructure organisations are vulnerable to the growing sophistication of hackers. To newsreaders around the world, and especially for the hundreds of thousands of victims in Ukraine, the ability of hackers to worm their way into critical infrastructure and even cause mass blackouts is understandably shocking. To those with a deep familiarity of the cyber-security field, this handful of recent events, while still incredibly alarming, may not come as such a surprise.

"No government is highly motivated to make any significant changes to the status quo when addressing the risks associated with Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems"

Although on the decline, many organisations have a legacy of utilising outdated IT and operating systems, such as Windows XP, that are no longer supported by manufacturers. To explain why, speed of innovation isn't a driving factor as in general IT – once something is deemed functional and reliable, with a good safety record, there is less motivation to update or upgrade. More alarmingly to the cyber-security layman,

malware running on Industrial Control Systems (ICS) networks can be tolerated for longer periods, provided it does not disrupt operations, which does not fit the logic generally used in IT.

Most disturbingly, there is minimal legislation globally to drive cyber-risk reduction to protect ICS. Though it is no doubt a bold statement, no government is highly motivated to make any significant changes to the status quo when addressing the risks associated with ICS and Supervisory Control and Data Acquisition (SCADA) systems. The question must be asked, is this intentional government policy to allow some of the world's largest organisations the freedom to operate with fewer restrictions?

Within the commercial sector, many businesses are beginning to take heed of the evolving threat posed by hackers, though many still face the disastrous consequences of data breaches, which are increasingly being launched via email through file-based attacks. Across all businesses, roughly 94% of successful data breaches and 78% of cyber-espionage assaults are the result of file-based attacks and the figures continue to grow each year.

While enterprises risk losing vast amounts of money and the goodwill of their customers, national infrastructure organisations that don't have adequate security measures in place are potentially putting the livelihoods – and even lives – of their citizens at risk.

The face of cybercrime

While hackers are typically described as being purely motivated by profit, those operating outside of the business realm, focusing on government bodies, are often suspected to come from hacktivist groups or even well-funded and secretive organisations operated by foreign governments.

Regardless of their motivation, cyber-criminals are in many cases using increasingly more effective social engineering to make their way into crucial systems because organisations are unwittingly giving the information away. In order to bolster their social engineering operations, hackers also utilise advanced intelligence-gathering tactics that can include acquiring personal information from social media, professional networking websites, through gathering seemingly benign metadata from a number of sources, such as files found on official websites that have not been sanitised or documents intercepted during exchange in order to identify information such as user IDs, server paths, software versions and even employee reference data. This activity helps the hacker profile employees, supply chains, internal workflows, processes and procedures, and is the kind of information leak that security specialists find on a regular basis during the discovery phase.

"Due to the advancing capabilities of hackers and the ever-decreasing adequacy of traditional perimeter security solutions, national infrastructure operators must turn towards innovation to solve the cyber-security gaps that will only grow wider over time"

By acquiring this information, hackers can then forge a series of convincing emails to an employee, posing as a trusted regular contact and tricking the employee into opening a malware-laden document – most often a PDF, Word, PowerPoint, Excel or other common file type – or clicking on a link designed to place a zero day exploit into the organisation's system, which is then timed to execute at a later date. In order to mitigate this specific vector, organisations must ensure they prevent data leakage caused by poor internal processes and weak management protocols, keeping private information away from would-be exploiters.

Conventional defences

Conventional, perimeter security measures, even so-called 'leading edge' approaches such as sandboxes, are unable to detect the malicious code hidden within common file types. Sandboxes in particular are designed as quarantines in which files are analysed for mere minutes before being deemed safe. The tampered files used by cyber-criminals, on the other hand, are programmed to go live weeks or even months after being embedded within a company's systems.

One of the major flaws in perimeter security solutions is that they are backward-looking, as they only search for lines of code that have already been identified as malicious. Furthermore, these solutions are typically reliant on constant updates as new exploits are discovered by the provider. The unfortunate reality is that any cyber-criminal using newly-developed exploits will be able to sneak the code through any perimeter security measure or sandbox, as these technologies won't recognise it as malicious.

In addition to offering little defence against file-based threats, sandboxes are notorious for producing high amounts of false positives – in some cases over 60% – which can take up a massive amount of time for IT teams to resolve.

Due to the advancing capabilities of hackers and the ever-decreasing adequacy of traditional perimeter security solutions, national infrastructure operators must turn towards innovation to solve the cyber-security gaps that will only grow wider over time.

Any change is fraught with unique challenges, but cyber-security needs to be tackled head on if the organisations responsible for supplying our clean water, electricity and fuel can be trusted as proactively tackling this complicated problem.

The attack on Ukraine's power grid could be seen as a proverbial floodgate, unleashing a slew of similar attacks, such as the one Israel recently faced, on unprepared infrastructure organisations. Whether this will be the case has yet to be seen, though the big question remains – what is the worst thing a person or group could do to a critical asset if they possessed the intent, access and knowledge to perform a malicious act? Keeping in mind the knowledge of what is now possible, these organisations would be wise to adopt a solution that can guarantee they don't become the next target of the new face of cybercrime.

About the author

Lewis Henderson is director of client engagement at Glasswall Solutions. He is

a seasoned cyber-security professional with 17 years' experience of delivering highly advanced technical security solutions into enterprises and government. Having published a series of cyber-security management guides geared towards educating the C suite in cyber-risk, his recent focus is researching the evolving risks in cyber and industrial control systems. The research is aimed at raising awareness at a senior level to ensure that the constant cyber- and ICS risk is approached in an informed and pragmatic way.

References

1. 'December 2015 Ukraine power grid cyber-attack'. Wikipedia. Accessed Feb 2017. https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyber_attack.
2. 'Steinitz: Israel's Electric Authority hit by 'severe' cyber-attack'. Times of Israel, 26 Jan 2016. Accessed Feb 2017. http://timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/.

Software vulnerability management: how intelligence helps reduce the risk

Vincent Smyth

Vincent Smyth, Flexera Software

Recently, a widely publicised news report revealed that tens of thousands of computers could have been exposed to hacker threats due to malicious online advertisements that ran on major media companies' websites, including the BBC.[1] These incidents are becoming increasingly commonplace and serve as a chilling reminder of how exposed we all are to the threats caused by software vulnerabilities that are exploited by malicious hackers.

Every year, thousands of software vulnerabilities are discovered in thousands of products. Exploitation of vulnerabilities can cause extensive damage. Chief security officers probably don't need to be reminded of the high stakes surrounding software vulnerability management. The numbers speak for themselves. For instance, in 2015 there were 16,081 vulnerabilities discovered in 2,484 vulnerable products.

The cost is enormous for organisations that must deal with a successful vulnerability exploit by a hacker. According to PwC, the average financial loss attributed to cyber-security incidents was $2.5m in 2015.[2] And that cost does not take into account the brand and reputational damage caused by a successful hack.

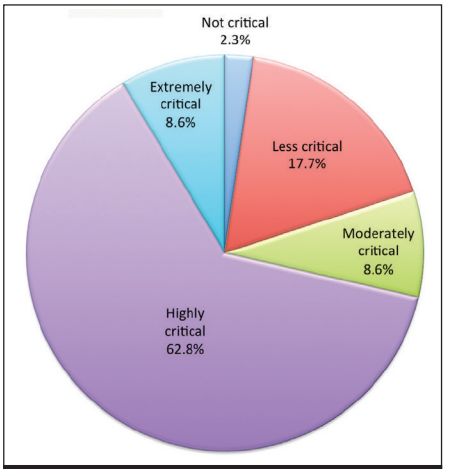
The good news is that 84% of all registered vulnerabilities had patches available on the day of disclosure.[3] Consequently, organisations can have the greatest impact on reducing their risk profile by proactively patching known vulnerabilities before they are exploited and, in the process, minimising the attack surface. But what is the fastest and most cost effective way of doing so? It starts with vulnerability intelligence.

Relevant threats

With an overwhelming number of software vulnerabilities reported every day, security departments can easily become overwhelmed with even the most basic aspects of addressing the problem, such as answering the question, 'Which vulnerabilities apply to us?'.

Companies need to filter out the known vulnerabilities and concentrate only on those impacting the organisation. That entails comprehensive asset discovery and inventory to determine which systems are potentially threatened by the known vulnerabilities. Once the universe of known vulnerabilities is winnowed down to only the subset impacting the enterprise, then teams can focus their attention.

Getting an accurate picture of IT assets in inventory is easier said than done. Most companies cannot accomplish this without implementing software asset management (SAM) processes



Criticality of software vulnerability advisories. Source: Flexera Software.

and technology. Fortunately, SAM has emerged in recent years as a bulwark against wasteful software spend – and many leading organisations around the world either have already implemented SAM or are in the process of doing so. Among other things, SAM solutions enable organisations to automate the process of discovering and inventorying their software (and hardware) assets – wherever they reside.

The challenge, then, is for the security and IT operations teams within organisations to recognise their mutual need for asset discovery and inventory and work together (and not in silos) to collect this data. If an organisation already has a SAM implementation in-house, security teams should be aware of this and utilise the discovery and inventory data as the common 'version of the truth' for determining which vulnerabilities apply to them. Moving forward, as SAM and security continue to converge, SAM tools are increasingly integrating capabilities with software vulnerability management tools – which, ultimately will help siloed security and IT operations teams work better together.

Refining security efforts

Picture this: a company's IT environment holds thousands of different applications and systems, all interconnected. Every year, as thousands of vulnerabilities are discovered in thousands of products – some are extremely critical and their exploitation can cause extensive damage – these need to be dealt with straight away. Others are not very critical and can be dealt with in due course. Security teams need to match their own environment with the vulnerabilities that are discovered, assess the risk the vulnerabilities pose and then prioritise mitigation of the vulnerabilities.

This in itself is a daunting task. Add to it that every day, some 300 new vulnerability alerts are reported globally. But in fact, on average, only about 8% of these 'reported' vulnerabilities turn out to be real. To know which threats to take seriously, it is necessary to thoroughly investigate them. This is highly skilled work that must be performed by experts in their field.

If curating vulnerability information is not a main line of business, companies most likely will not have the resources or the motivation to employ a full team of people whose only purpose is to monitor and curate vulnerability information. Instead, organisations must find a trusted software vulnerability management resource whose function is to perform this work, providing vulnerability *intelligence* – not just information.

"With limited time and resources available to patch the hundreds – or even thousands – of vulnerabilities that may impact an organisation, how are security teams to know which are the most important?"

Vulnerability intelligence means that reported vulnerabilities are actually verified, with additional intelligence, delivered in a format that security teams can use and act upon, which explains how to handle the issue. Moreover, it means that the intelligence has been tested, vetted and is relevant – so that the information delivered pertains only to vulnerabilities in products relevant to the specific environment. For instance, beyond verification of a vulnerability's existence, vulnerability intelligence should detail what IT security teams need to know to mitigate the risk to the organisation by the vulnerability.

Good vulnerability intelligence will not only verify the existence of a vulnerability, but will also rate the vulnerability's criticality. This is important because, as noted, not all vulnerabilities are created equally. And with limited time and resources available to patch the hundreds – or even thousands – of vulnerabilities that may impact an organisation, how are security teams to know which are the most important?

As this sounds very theoretical, it may be helpful to provide an example. The Secunia Research team provides vulnerability advisories in this manner. Beyond verifying and detailing the vulnerability, these advisories assign to it a criticality rating of 1 to 5 – with 1 representing the least critical and 5 representing the most critical.

The criticality of a vulnerability is based on the assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors and whether an exploit exists for the vulnerability and is being actively exploited prior to the release of a patch. The vulnerability ratings are as follows:

- **Extremely critical (5):** typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP and SMTP or in certain client systems such as email applications or browsers.
- **Highly critical (4):** typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction but there are no known exploits available at the time of disclosure. Such vulnerabilities can exist in services like FTP, HTTP and SMTP or in client systems like email applications or browsers.
- **Moderately critical (3):** this rating is also used for vulnerabilities allowing system compromise on LANs in services such as SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet. Typically used for remotely exploitable denial of service vulnerabilities against services such as FTP, HTTP and SMTP and for vulnerabilities that allow system compromises but require user interaction.
- **Less critical (2):** typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.
- **Not critical (1):** typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This

rating is also used for non-sensitive system information disclosure vulnerabilities (eg, remote disclosure of installation path of applications).

Armed with reliable intelligence covering reported and verified vulnerabilities, which of those verified vulnerabilities apply to an organisation's own hardware, software and systems and – of those that apply – which are more critical and which less, security teams can then begin to establish an effective remediation plan.

The proactive nature of software vulnerability management presupposes that it is less costly to avoid successful attacks than to fix the problem after an attack has occurred. Therefore, organisations need to understand what IT assets exist within their environments that could be the target of attack. They need to have a complete picture of the vulnerability landscape – and, more importantly, a picture of which vulnerabilities apply to them. Then finally, organisations need an accurate and reliable assessment of the criticality of those vulnerabilities, so they can prioritise remediation. A thorough programme founded upon vulnerability intelligence will help minimise the attack surface, reducing the risk that a successful exploit can occur.

About the author

Vincent Smyth is senior vice-president EMEA at Flexera Software, responsible for driving revenue, market share and customer satisfaction in the independent software vendor, high-tech manufacturer and enterprise account domains. Prior to Flexera Software, he held several sales management responsibilities for Business Objects, PTC and Computer Associates. He has extensive experience of doing business across Europe and the Middle East.

References

1. Kirk, Jeremy. 'Large advertising-based cyber-attack hit BBC, New York Times, MSN'. Infoworld, 16 Mar 2016. Accessed Feb 2017. www.infoworld.com/article/3044880/security/large-advertising-based-cyber-attack-hit-bbc-new-york-times-msn.html.
2. 'The Global State of Information Security Survey 2017'. PwC. Accessed Feb 2017. www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
3. 'Vulnerability Review 2016'. Flexera Software, 16 Mar 2016. Accessed Feb 2017. www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/.

Why communication is vital during a cyber-attack

Nick Hawkins

Nick Hawkins, Everbridge

Cyber-attacks are a constant threat to organisations. However, cloud-based communications platforms can help an organisation improve emergency communications and more effectively recover from the effects of a attack.

In today's globalised business environment, organisations of all sizes face the prospect of falling victim to a cyber-attack or IT outage that could cause serious damage to their infrastructure and ability to operate. The need to combat cybercrime is rising up the UK Government's agenda with the opening of the National Cyber Security Centre (NCSC). According to its 2016-2021 report, the NCSC's role will be to manage national cyber-incidents, provide an authoritative voice and centre of expertise on cyber-security and deliver tailored support and advice to government departments, the devolved administrations, regulators and businesses.

Despite the improvement of cyber-security techniques, criminals have developed sophisticated ways to disrupt systems and steal data. The need to prepare for cyber-attacks is more important than ever.

True cost of cyber-attacks

According to Cisco's '2017 Annual Cyber Security Report', more than one-third of the organisations that experienced a cyber breach in 2016 reported a loss of customers, business opportunities and revenue.[1] The '2017 SonicWall Annual Threat Report' reported an increase from 3.8 million ransomware attacks in 2015 to 638 million in 2016.[2] In March 2016 alone, ransomware attack attempts rose from 282,000 to 30 million.

Cyber-attacks cost UK businesses a total of £34.1bn between summer 2015 and 2016, with each attack costing an average of £4.1m and taking 31 days to resolve.[3] While large corporations, which invest millions of pounds in cyber-security, have the potential to recover easily from such a crisis, for most Small/Medium Enterprises (SMEs) and Non-Governmental Organisations (NGOs) cyberbreaches can have more far-reaching and detrimental consequences.

No business is safe

Investing large sums of money into cyber-security is not a guarantee of success, as shown by a number of recent high-profile cyber-attacks against large corporations all over the world – including the BBC, Sony's PlayStation Network, HSBC and eBay.

Sony lost control of its entire network. Hacker group Guardians of Peace stole personal information from tens of thousands of current and former workers and published them on the web. This included social security numbers, salaries of top executives and five Sony-produced movies.

More than 155,000 TalkTalk customers had their personal information, including bank details, accessed by hackers as a result of the data breach in October 2015. Last year, following a hack in 2012, LinkedIn reported the extent of the damage caused by that hack, with more than 117 million people's personal details offered for sale.

It is not just large organisations that are targeted: government departments and agencies, rail networks and local businesses regularly find themselves in the same position. When attacks occur, crucial services are compromised and the reputational impact can quickly reduce consumer confidence and brand value. Large-scale attacks also have the ability to impact share price value. Planning what to do when a cyber-attack occurs is important, but how victims communicate in an attack is equally critical.

Effective communication

In the event of an emergency, effective communication is crucial. When IT systems go down, an organisation needs to be able to communicate with its employees and co-ordinate an effective response. The longer this process takes, the bigger the impact that the crisis will have.

A successful cyber-attack can affect multiple communication methods. If your phone and voice mail system is VOIP-based, you may lose your company phone system. If your employee hotline runs through your voice system, this could also be lost. If your company website is hosted in-house, it may go down, meaning customers, employees, the general public and the media cannot find you. If company telephone bridges are running through your phone network, they may not be available. And if the core network is compromised, every computer becomes a standalone machine with no access to company records. Human resource information, employee contact information, vendor lists or other key phone lists may be inaccessible.

With multiple resources affected, how will you communicate? A critical communication platform can be used for the following:

- Employee information: pushing information to employees about the company status and messaging.
- Conference bridges: using toll-free conference bridges for employee, vendor, senior management, board of directors and other key stakeholder phone calls.
- Stakeholder groups: using pre-defined groups that have been created for key stakeholders to push information via phone, text or email.

Because no business or organisation is totally immune from the dangers of a cyber-attack, it is vital that crisis management plans are in place to minimise impact and ensure a return to business-as-usual practice as quickly as possible.

Preparing communications

- **Assess:** what is happening? What is the impact? Determine the likelihood, severity, and impact of the incident
- **Locate:** who is in harm's way? Who can help? Identify resolvers, impacted personnel and key stakeholders
- **Automate:** which team members need to act?
- **Communicate:** what should employees do? Notify employees on what action to take and keep stakeholders informed

Having a plan

An effective crisis management plan consists of two key components: quick, reliable and secure communication with all employees to notify them of the situation and the efficient deployment of resources to resolve the issue. It is important that businesses consider a number of questions to prepare for a cyber-attack.

What threats could impact your organisation? Companies have to understand the type of threat the organisation could experience and the impact it could have. For example, it could result in loss of services or data. The solution will differ depending on the threat.

Do you have a response plan? Cyber-attacks often happen out of office hours. An IT incident response plan must be in place to combat an attack even if it happens at 5am. An efficient response plan will include methods of communication for specific stakeholders. Alerts will also differ depending on whether the attack has just occurred and if malicious code has laid dormant on the network. IT engineers require different instructions from regular employees.

Who needs to be included in an IT incident response plan?

- IT security: these are the people who are likely to fix the issue. If an organisation does not have a dedicated security team, employees must be assigned to deal with a security crisis when it occurs.
- Incident team: who is going to co-ordinate the response? Who should be contacted following a breach and how are you going to reach them? Define an escalation point.
- Legal counsel: if, for example, customer credit card details are stolen, legal support may be necessary.

Who are your stakeholders? There are a number of stakeholders who should be considered. For example, if customer data is stolen, the following stakeholders would need to be consulted:

- C-level executives – businesses must consider when and how to consult their C-suite. For example, it may be necessary for the CEO to release a statement.
- Media relations department – to ensure strategic messaging is in place when informing customers about the incident and handling inquiries from the press.
- Customer services – need to be informed to prepare for incoming customer enquiries.
- Employees – employees must be kept up to date throughout the process to ensure they are prepared for

calls from customers and the press. Employees must be aware of when and how to escalate queries.
- Customers – organisations are legally obliged to inform customers of a data breach. The ability to communicate with customers en masse in real time is important.

Cloud power

As cloud-based critical communications platforms are not reliant on one network, organisations that used the platform to send out an emergency notification are assured that the message will get to the right people. Most organisations rely on internal email to communicate in the event of a crisis, despite the fact that a cyber-attack might impact the email network. In doing so, organisations are exacerbating the issue and potentially providing hackers with critical company information.

By having a system that operates entirely independent of an internal communications network, organisations can ensure that the bilateral lines of communication between management and staff remain open – even in the event of a cyber-attack or IT outage that may compromise an internal network, or a rush of calls that may overload a telecommunications network.

By using cloud technology to automate the time-intensive emergency cascade process, resources can be deployed far more effectively and efficiently than before, ensuring that the safety of everyone involved is better protected. In doing so, communications technologies can not only help protect business assets but save the lives of employees. In an emergency, organisations cannot waste time searching spreadsheets and schedules to manually notify employees.

Multi-modal

Critical communications platforms are already deployed by businesses, local authorities and national governments around the world to warn and advise people in the event of a crisis. These incidents can range from sourcing a relevantly skilled IT technician to repair a broken server, to engaging with the public during a terror threat. Central to the success of critical communications platforms are two key functions. The first is the capability to deliver messages using a variety of different methods – this is known as multi-modal communications. No communications channel can ever be 100% reliable 100% of the time, so multi-modality transforms the speed at which people receive the message. Multi-modality facilitates communication via multiple communication devices and contact paths, including email, SMS, VoIP calls, social media alerts and mobile app notifications, among many others.

Multi-modality ensures that it is easier to receive a message. Two-way communication makes it simpler to confirm a response. In a critical emergency, every second counts, so organisations can use communications platforms to create and deliver bespoke templates that require a simple push of a button to respond to. In doing so, the level of response to critical notifications can increase significantly.

For instance, if a cyber-attack compromises an e-retailer's website, every second costs the business money. An IT engineer must be located and available to help as fast as possible. Two-way communications enable the business to send an alert to the IT team, giving them the option to reply with 'available and onsite', 'available and offsite' or 'not available'. Organisations can build a clear picture of the incident and prepare for downtime if necessary.

Combined, multi-modality and two-way communications transform critical communications from an incident alerting platform into a communications tool where organisations can respond smarter and faster. In situations where multi-modal communications and response templates are deployed together, response rates to messages increase from around 20% of recipients to more than 90%.

Conclusion

As technology continues to advance, cyber-attacks are on the rise and organisations need to have the tools in their armoury to be able to communicate and recover quickly in the event of a crisis. It is an organisation's response to a cyber-attack that will determine the severity of its impact. Critical communications platforms can help businesses prepare for a breach to limit downtime and damage. Companies have a duty of care to keep customer information secure. Legal implications could be applied if responsibilities are not fulfilled. An efficient, well-practised incident response plan can maintain brand reputation and ensure that a business is not forever known for the number of customer bank details or thousands of pounds worth of revenue it lost.

About the author

Nick Hawkins joined Everbridge as managing director EMEA in April 2015. He is an experienced business leader and has managed sales and service teams within the services, IT and communications industries for more than 25 years. Hawkins has extensive experience in the security industry and spent more than 10 years in the Metropolitan Police.

References

1. 'Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches And The Actions That Organizations Are Taking'. Cisco, 31 Jan 2017. Accessed Mar 2017. http://investor.cisco.com/investor-relations/news-and-events/news/news-details/2017/Cisco-2017-Annual-Cybersecurity-Report-Chief-Security-Officers-Reveal-True-Cost-of-Breaches-And-The-Actions-That-Organizations-Are-Taking/default.aspx.
2. '2017 SonicWall Annual Threat Report'. SonicWall. Accessed Mar 2017. www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/.
3. Ashford, Warwick. 'Cyber attacks cost UK business more than £34bn a year, study shows'. Computer Weekly, 14 Jul 2016. Accessed Mar 2017. www.computerweekly.com/news/450300330/Cyber-attacks-cost-UK-business-more-than-34bn-a-year-study-shows.

The Russians are coming! Are security firms over-hyping the hacker threat?

Tim Ring

Tim Ring, freelance journalist

UK Government cyber-expert Dr Ian Levy recently warned organisations to beware of their security solutions suppliers, because they massively exaggerate the hacker threat. But is he right?

Britain's new National Cyber Security Centre (NCSC) – the flagship in the country's £1.9bn fight against cyber-crime – is a haven of security best practice. So when one of its senior directors recently accused the cyber-industry of "massively" over-hyping hackers' abilities in order to sell their own products, the sector was stung into some serious soul-searching.

The colourful criticism, delivered by NCSC technical director Dr Ian Levy at the Enigma 2017 conference in California, hit the headlines in The Register and BBC News.[1,2] Levy lambasted the security industry for peddling "medieval witchcraft" – exaggerating the skills of hackers in order to claim that only *their* security hardware and services could magically defeat such adversaries. Yet most cyber-attacks are not APTs (advanced persistent threats), Levy said – usually it's just "Adequate Pernicious Toe-rags" who are doing the hacking.

"If you call it an advanced persistent threat, you end up with a narrative that basically says 'you lot are too stupid to understand this and only I can possibly help you – buy my magic amulet and you'll be fine'," Levy said. "It's genuinely medieval witchcraft." Pointing out that a telco was recently taken offline by an SQL injection flaw that was older than the alleged hacker involved, Levy's message was that organisations should take action to protect themselves, rather than sit back and rely on their suppliers. The NCSC wants to promote "active security" said Levy – active as in "getting off your arse and doing something".

Challenging message

It's a challenging message that makes uncomfortable reading for the cyber-industry, branding them as pedlars of FUD (fear, uncertainty and doubt). But hang on – just days after Levy spoke out, no less a person than his boss, NCSC chief executive Ciaran Martin, was explaining how the UK had been hit by 188 high-level attacks in the previous three months, believed to originate from nation-state actors and following "a step change in Russian aggression in cyberspace".[3]

He was backed up by UK Defence Secretary Sir Michael Fallon, who warned that Moscow was carrying out sustained cyber-attacks against Western democracies and critical infrastructure, "weaponising misinformation" in a bid to destabilise governments and weaken Nato.[4] And in the US, intelligence agencies have accused Russian state hackers of interfering in the US presidential election by stealing and leaking damaging emails from Hillary Clinton's Democratic Party.[5]

So the NCSC, the same highly respected organisation that has accused the cyber-industry of hacker-hype, is also issuing dramatic warnings about the cyberthreat. In the face of such apparent contradiction and confusion, has the industry got its message to users wrong? And if it has got it wrong, what is the 'right' message it should be sending out?

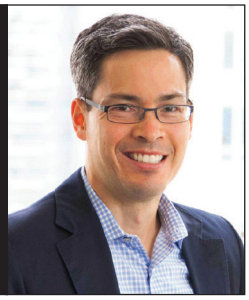
Striking a nerve

Levy's criticism clearly struck a nerve, prompting a number of cyber-industry insiders to weigh into the debate over whether security warnings are motivated by commercial self-interest, or people's best interests. On the one hand, Gigamon EMEA marketing director Trevor Dearing strongly supported warnings like those issued by Ciaran Martin, saying: "In this day and age, we simply cannot afford to be complacent when it comes to cyber-security. While it may seem like vendors are spreading fear and uncertainty among their customers in order to boost sales, the fact remains that many companies simply aren't fully aware of or prepared for the current cyber-security climate.

"Unfortunately cyber-attacks are not decreasing in frequency and when you look a critical national infrastructure (CNI), a major breach could lead to consequences far worse than hacking an email account. Power grids, airports and healthcare organisations are all moving their systems online and are becoming prime targets. Security vendors are not trying to create a 'boy who cried wolf' scenario, as unfortunately the 'wolf' is well and truly there, remaining hidden in organisations' networks."

Others in the industry support Levy's stance. "It's definitely true that many security vendors do use scare tactics during the selling process and it does get out of hand," said Tim Chen, CEO of DomainTools.

Trevor Dearing, Gigamon: "We simply cannot afford to be complacent when it comes to cyber-security."



Tim Chen, DomainTools: "Many security vendors do use scare tactics during the selling process.

Philip Lieberman, CEO of Lieberman Software, qualifies this: "Without question, some security software vendors provide a never-ending stream of hyperbole to create fear of hackers and their destruction. However, although each vendor says they have the 'silver bullet' to stop the problem, the reality is that only the effectiveness is in question, not the threat itself. The US has been reporting massive numbers of intrusions. The effectiveness of the solutions may be in question, but the threat and consequences are real."

Core message

Lieberman gets to the core of Levy's message: organisations should think more about how they can protect themselves and question whether a focus on specific 'silver bullet' security solutions to APT threats will magically safeguard them. Tellingly, this same theme is pursued in a new 'Black Report', released in February by security firm Nuix. Supporting Levy's view, the survey's starting point is that since cyber-attacks have continued to multiply and succeed, despite years of effort by the security industry, then vendors have self-evidently got their message (and the solutions they offer) wrong.

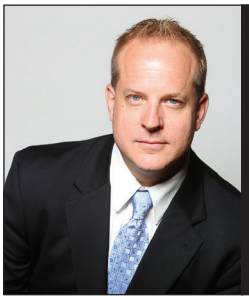
Echoing Levy's accusations of hype, Nuix CISO Chris Pogue says: "Countless security solution providers have claimed their widgets were all you needed to prevent attacks and if you would only buy this feature or that add-on, your organisation would be practically un-hackable. Well, we all bought their solutions and expected to be safe, yet we were still compromised. So there is obviously something to this problem beyond what we have been led to believe, that continues to plague virtually every organisation on the planet."

Nuix's take is that security firms are failing to send out the right messages to users and the reason is because they are peddling the same limited information gathered from attack victims. As Pogue says: "During my tenure in the cyber-security space, I have read literally hundreds of threat reports that all seemed to report the same thing: attacks are happening all over the world. Attacks are growing in frequency across all target verticals. No data is safe. Organisations are failing to prevent or detect attacks in any sort of meaningful way." This isn't helping, Nuix says. Instead, security firms should be pinpointing exactly which anti-hacking solutions work and which don't, based on talking to the attackers themselves.

The 'hackers' that Nuix surveyed are in fact penetration testers – 'white hats' whose job is to test organisations' security and so are paid to think and act like hackers. And what these pen testers reveal is:

- The best countermeasures are endpoint security (according to 36% of the respondents), then intrusion detection and prevention systems (29%) and firewalls (10%).
- The least-effective solution is antivirus software, which troubled only 2% of hackers.
- Security decisionmakers get the best ROI from intrusion detection and prevention systems and the worst ROI from data hygiene and information governance, followed by perimeter defences and incident response.

But the report's overall conclusion is that organisations should deploy multiple security solutions, based on the finding that 20% of 'professional hackers' boast that *no* security countermeasures can stop them. As Nuix says: "This clearly demonstrates the importance of defence in depth. Any individual security control can be defeated by an attacker with enough time and motivation. However, when an organisation uses a combination of controls, along with security training, education and processes, the failure of any single control does not automatically lead to data compromise."



Chris Pogue, Nuix: "There is obviously something to this problem beyond what we have been led to believe."

Not so simple

The Nuix view that the hacker threat is severe but that many security firms have been promoting the wrong solutions and sending out the wrong messages, gets support from a number of industry commentators. One area of consensus is that, as Ian Levy said, vendors go overboard on warnings about sophisticated state-sponsored APT attackers wielding scary zero-day vulnerabilities, while claiming they have the 'right' solution to this threat.

F-Secure security advisor, Sean Sullivan, agrees that: "APT is a label that has outlived its usefulness". He points out that highly motivated state threat actors (like the Cozy Bear/Fancy Bear hacker teams) could well "start with basic techniques, because they very often do the job. But I would not call those basic attacks".

Chen at DomainTools takes a similar line: "Measured by both count and dollar value, basic crimeware is by far the most prevalent and effective. APT attacks are newsworthy because of their sophistication and the high profile of the targets. But while potentially very damaging for the APT target, overall the impact is low versus the litany of crimeware being spread worldwide every day via phishing, malvertising and other high-volume techniques."

Alex Mathews, lead security evangelist at Positive Technologies, also supports Levy's warning about APTs and over-playing hackers' skills. He points out: "Hackers don't always need to be skilled masterminds to break into some very serious connected infrastructure. That is the real problem. The whole modern digital environment is vulnerable, both from advanced attacks and, sadly, from critical technology being

Sean Sullivan, F-Secure: "APT is a label that has outlived its usefulness."

secured with things like default passwords. Our research shows that a lot of people, even system administrators, still use simple passwords like '123456'. If this is the case, then even advanced security can be defenceless from someone with a very low level of skill. However, there will always be skilled threat actors using ever more inventive ways to breach companies and that shouldn't be overlooked."

Victim blaming

Interestingly, Pogue at Nuix says the over-the-top focus on APTs can be blamed on the victims of hacking, as well as the security industry itself. He said: "In my experience over 19 years and close to 2,500 investigations, I can only recall a very small percentage of breaches that involved complex attack vectors. The overwhelming majority of breaches were facilitated by poor IT hygiene, human error or negligence.

"Over the years I have noticed a pattern emerge: organisations that have suffered a data breach overstate the complexity of the attack, while understating the impact. This is manifested in statements indicating that the attack was 'tremendously complex', 'involved a zero-day exploit', or involved nation state actors. Usually the spokesperson makes the reassuring claim that they are confident that no customer data was accessed or impacted. Then, sometimes days or weeks later, it is reported that the attack was carried out by a teenager, that the exploit was brute-forcing a weak password and that all customer data was harvested and exfiltrated.

"Calling an attack an advanced persistent threat (APT) is a great terminology and makes for great media, but is likely misrepresentative of the actual attack. There most certainly are hostile nation-state actors and tremendously complex attack patterns that involve zero-day exploits. But the supposed complexity of many attacks reported in the media was very likely written by crisis communications experts and attorneys with the specific goal of protecting their client."

Defence in depth

Along with the consensus that a focus on APT attacks and solutions can be misleading, there is also agreement with Levy's view that focusing on 'magic' solutions (aka silver bullets) is also unrealistic.

Sullivan believes there is no single threat and no simple message to send out about attacks: "It's important to understand that threats are moving from basic commoditised crimeware to potentially more motivated bespoke extortionists. Yesterday's basic botmaster can much more easily be today's motivated, yet opportunistic, extortionist. In the past, bots in a corporate network were utilised more or less as consumer-based bots were. Today, it's more likely the botmaster will identify it's a business and will leverage that, or will sell off the resource to somebody."

When it comes to the most effective countermeasures, Sullivan says: "Defence in depth is definitely good, but so is resilience. Do you have incidence response (IR) companies on retainer? You may find that you can't get good IR people when you need them if you don't. Assume a failure and plan for a fast recovery."

Mark James, IT security specialist at ESET, supports the same message about defence in depth: "Cyber-defence is so much more than just putting software or hardware in place and hoping to catch the bad guys. Of course that's the nature of this industry, but it's not enough to just do that, you have to think out of the box and we are back again to multi-layered defences. Being on the lookout for both modified and existing attack vectors along with completely new techniques is the only way to stay safe – doing the basics while learning and reacting in real time, along with utilising modern defences and expert knowledge."

Mark James, ESET: "Cyber-defence is so much more than just putting software or hardware in place and hoping to catch the bad guys."

Chen is less convinced, pointing out: "Defence in depth is effective, but expensive. Network perimeter and endpoint protection is critical, along with directed training for all employees. We recommend proactive efforts around logging and threat hunting for more mature organisations."

But Pogue elaborates on the recommendation of 'defence in depth' put forward in Nuix's report. He says: "According to our survey, the most impactful countermeasure is endpoint technology. But no security control is immune from circumvention or defeat, so endpoint technology should never be relied on as the sole defensive mechanism. The assumption should always be that protective measures will fail, humans will make mistakes and procedures will fail to be followed. This is precisely the reason why utilising a defence-in-depth approach is so effective.

"This should be the priority for any organisation that is trying to build up its defences…layer upon layer, precept upon precept until you have created a mesh of deflection and detection capabilities. Then start the testing process, every day, looking for weaknesses, fine-tuning detection capabilities and training your incident response teams until they have the muscle memory of a professional athlete and can react without really even thinking about it."

Conclusion

It seems clear from industry insiders that there is no easy way for vendors to tread the fine line between responsibly alerting the world to the cyberthreat and being accused of yelling "The Russians are coming, the Russians are coming" just to sell their own brand of snake oil. But there is some agreement that focusing on single silver-bullet solutions and the

'APT' threat is at best misleading and at worst damaging. Many commentators also support the message that organisations need defence in depth – and that maybe there should be more honesty among vendors that their own solution set may not be enough.

So, between Ian Levy's wake-up call to users to beware vendor hype and engage in active defence and Ciaran Martin's warning that the hacker threat is all too real, the NCSC may be sending out a consistent message: that a range of security measures is needed to deal with a complex and evolving cyberthreat where even the most sophisticated attackers may rely, like script kiddies, on exploiting the most basic flaws.

About the author

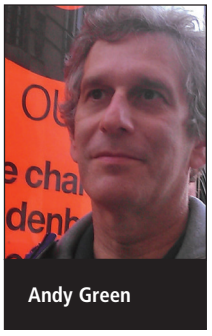
Tim Ring is a freelance business & technology journalist specialising in cyber-security.

References

1. Thomson, Iain. 'GCHQ cyber-chief slams security outfits peddling "medieval witchcraft"'. The Register, 3 Feb 2017. Accessed Mar 2017. www.theregister.co.uk/2017/02/03/security_threat_solutions/.
2. 'Security firms 'overstate hackers' abilities to boost sales'. BBC News, 3 Feb 2017. Accessed Mar 2017. www.bbc.com/news/technology-38853502.
3. Kerbaj, Richard. 'Russia steps up cyber-attacks on UK'. The Sunday Times, 12 Feb 2017. Accessed Mar 2017. www.thetimes.co.uk/article/russia-steps-up-cyber-attacks-on-uk-rl262pnlb.
4. 'MPs question UK's cyber-attack defences'. BBC News, 3 Feb 2017. Accessed Mar 2017. www.bbc.co.uk/news/technology-38845582.
5. Gayle, Damien. 'CIA concludes Russia interfered to help Trump win election, say reports'. The Guardian, 10 Dec 2016. Accessed Mar 2017. https://www.theguardian.com/us-news/2016/dec/10/cia-concludes-russia-interfered-to-help-trump-win-election-report.

Ransomware and the GDPR

Andy Green, Varonis


Andy Green

Ransomware is a unique form of hacking that leaves data intact but still disrupts enterprises around the globe. This special malware encrypts computer files, network file shares and even databases, thereby preventing user access. To release the files, the victim is asked to pay a ransom to the cyberthieves. It is completely diabolical and you would think with such brazen criminal activity, there would be relevant data security laws that would kick in. And there are.

EU-wide laws, the current Data Protection Directive (DPD) and new General Data Protection Regulation (GDPR), have or will have an impact on companies in terms of compliance and reporting. But before we discuss them, let's get a handle on the ransomware epidemic.

A dramatic uptick in ransomware incidents is a worrying trend and, while they are seen as an inconvenience, many fail to consider these attacks as a serious security incident. It is proving effective and therefore lucrative for cyber-criminals, with the US's FBI warning ransomware could become a $1bn industry 'very soon'.[1] The Department of Homeland Security also reports that in 2016, ransomware infections on a global basis were at an all-time high. And security researcher Kevin Beaumont recently noted that the popular variant, Locky, was infecting devices at the rate of 4,000 per hour.[2]

There are many ransomware variants but they tend to act in a similar fashion. A particularly virulent one is Cerber, which Microsoft confirmed has clocked in over 200 infections from December to January on corporate endpoints operating Windows 10 Enterprise. It is unleashed when an unsuspecting user clicks on a phishing email attachment, in this case a Word document, although the malware comes in many guises. Once the user opens the document it launches a macro that ultimately starts the attack.

A hard-to-detect PowerShell script downloads the malware payload from the attacker's command and control (C2) server. This malware – a binary executable, not a script – is also set to autorun on reboot, thereby making it persistent. At this point, the heavy lifting is done by this evil executable, which traverses the file system and encrypts each file with a different key.

Cerber keeps track of all the file encryption keys by appending the key used to encrypt each file to the end of that file and then in turn encrypts that segment with a special key that is retrieved from the C2 server. The attacker's server effectively holds the key to the keys – the key that will unlock the specific encryption keys for each file.

Regardless of whether an organisation pays the ransom, there can still be regulatory implications in having this malware disrupt file systems. Next year, if an organisation has its data encrypted by ransomware, it may have to report this breach to a data protection authority (DPA) under the new GDPR, which comes into play in May 2018, before the UK is predicted to leave the EU.

But since 1996, EU countries have been under the Data Protection Directive (DPD), which covers 'personal data' collected by companies from consumers. The DPD defines personal data as 'any information relating to an identified or identifiable natural person'. This would cover traditional identifiers, such as name, address and phone number,

as well as Internet-era handles such as email, IP address and online user names.

The DPD acted as a kind of template and EU countries were supposed to 'transpose' the rules into specific national legislation. A country's DPA then enforces the law – in the UK, for example, it is the Information Commissioner's Office (ICO). Organisations that have personal data encrypted by ransomware could come under investigation by the ICO for failing to take 'appropriate measures' to keep the personal data secure.

While the DPD does *not* have a breach notification requirement, a few EU countries have added notification to their own national data laws. In Germany's case, for example, a breach requires actual exposure of the personal data to a third party. This would imply, however, that ransomware, if it only encrypts the personal data, does not need to be reported.

Going forward, the EU GDPR, unlike the DPD, will be a uniform law across the EU, as well as including a 72-hour breach notification requirement. The new regulation clarifies a data breach as the "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". That means access alone is considered a breach and so ransomware that encrypts personal data would appear to require a notification to individuals and the relevant DPAs.

Whether notification is necessary rests on the regulation's 'harm threshold' and this is open to interpretation at present. The GDPR states that no notification is required if the "personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". And the same threshold is applied when notifying the affected individuals. We'll have to wait for clarification on breach notification from the EU regulators prior to the GDPR's implementation.

Limit the damage

Ransomware is a menace, but that doesn't mean it can't be stopped. Companies need to defend against and reduce the risks of ransomware. Regardless of their actual response obligations, they should act as if they *will* need to notify customers and authorities and have procedures in place to reduce further unauthorised access and restore data access.

Ransomware is getting sneakier and perimeter and monitoring defences fail to catch it. Many malware variants are able to bypass new, next-generation firewalls, IDS, Security Information and Event Management (SIEM) alerts and even malware detection agents running on infected workstations.

Organisations need a system in place that looks for anomalous behaviour, such as rapid encryption or malicious non-human activity, to avoid falling prey to rapidly evolving and adapting ransomware attacks.

Here are four recommendations to reduce the impact from ransomware:

- Classify data: know where personal data is stored on file systems, especially in unstructured formats in documents, presentations, and spreadsheets.
- Restrict access: limit access to personal data on a need-to-know basis or through role-based access controls. The goal is to make it difficult for attackers to access important data after hacking an ordinary user – say, through a phishing email – and launching ransomware based on that user's credentials. Organisations should also remove and/or archive outdated or stale personal data, further reducing the attack surface.
- Monitor: since ransomware is essentially crawling a file system, navigating through each directory and examining files, it has a very distinct signature. Ordinary users whose credentials the ransomware is leveraging, do not perform these kinds of large-scale scans. Therefore, monitoring software, particularly based on User Behaviour Analytics (UBA), should be able to detect the ransomware and limit the number of files that are encrypted.
- Back-up and recover: finally, companies should be regularly performing back-ups of their file systems, especially critical and sensitive data and have in place a recovery plan for restoring the data in the case of cyber-attacks.

About the author

Andy Green is a technical content specialist at Varonis, a provider of data governance software. He is a veteran technology journalist with over 12 years of experience writing about high-tech topics for B2B publications, market research firms as well as several software companies. At Varonis, he is focused on drawing connections between data security, compliance regulations and real-world IT solutions. Besides developing research reports and other critical content, he actively contributes to the Varonis blog at blog.varonis.com. In his limited free time, Green also covers the local NYC startup scene for The Technoverse Blog (TvB), which he founded.

References

1. Weisbaum, Herb. 'Ransomware: Now a billion dollar a year crime and growing'. NBC News, 9 Jan 2017. Accessed Mar 2017. www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646.
2. Beaumont, Kevin. 'Locky ransomware virus spreading via Word documents'. Medium, 17 Feb 2016. Accessed Mar 2017. https://medium.com/@network-security/locky-ransomware-virus-spreading-via-word-documents-51fcb75618d2#.8lmpqv24i.

The Firewall

The eSignature comes of age

Colin Tankard, Digital Pathways

In recent years, the use of digital or electronic signatures has rapidly increased in an effort to streamline all types of business transactions. The eSignature can not only be used as an actual certifiable signature, just as we did with a pen, but can also be used to encrypt the contents of a document, thus making it accessible only to those whom the owner of the eSignature has granted permission. Furthermore, the protected document can be additionally controlled to ensure that the content cannot be changed.

There are two types of electronic signatures: those based on a Public Key Infrastructure (PKI) and those that are not. Digital signatures that do not use PKI cannot: offer a unique signature for each user; identify the signer (authentication); detect changes in the documentation after signing (non-repudiation); or offer a guarantee of sole control for the signer (non-repudiation).

Digital signatures that do use PKI can: bind signers with respective user identities by means of a certificate authority (CA); allow individuals to encrypt messages to each other; and establish message integrity, confidentiality and user authentication, even if the parties have never had prior contact.

PKI technology relies on three components. A Registration Authority (RA) provides the authentication process in the network that verifies user requests for a digital certificate. The RA tells the Certificate Authority (CA) to issue the digital certificate. The CA issues the digital certificate, which contains a public key and the identity of the owner. This certificate validates that this public key actually belongs to the certificate. Finally, there's a database, a repository that stores the digital certificates.

The Certificate Authority is the most important element of a PKI structure and must be secure and cost-efficient. The digital certificate proves the ownership of a public key/private key pair by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the public key/private key pair.

There are many scenarios where documents need to be shared but the authenticity of the content needs to be proved, such as legal documents sent between organisations and their legal teams during a merger. In this example, the CA already acts as a trusted third party between the requestor and the distributor of legal documents and the signature is verified and used to secure the complete document. The ability of a receiver to read the document is in the hands of the owner, who can control how the document is treated. For example, it could either be read-only, or collaboration may be allowed, with each party changing or adding to the document by using their eSignature to sign their modifications. This provides strong control of a document's life cycle and, in the case of a merger should the deal fall through, the eSignature can be revoked.

There are many benefits to using an eSignature within any size of business and with the pending General Data Protection Regulation (GDPR), the need to identify, control and destroy sensitive data will become a key factor in every company's data security compliance strategy.

EVENTS CALENDAR

3–5 April 2017
InfoSec World
Orlando, Florida, US
http://infosecworld.misti.com/

3–7 April 2017
Financial Cryptography and Data Security
Malta
http://fc17.ifca.ai

4–6 April 2017
Cyber & Information Security Research Conference
Oak Ridge, Tennessee, US
www.cisr.ornl.gov/cisrc17

10–14 April 2017
HITBSecConf
Amsterdam, Netherlands
http://conference.hitb.org

18 April 2017
Flat Cap 2017
Leeds, UK
www.flatcapcon.com

24–28 April 2017
Xeefcon
Gdansk, Poland
www.x33fcon.com

30 April–4 May 2017
Eurocrypt 2017
Paris, France
https://eurocrypt2017.di.ens.fr

2–5 May 2017
RuhrSec
Bochum, Germany
www.ruhrsec.de/2017/

3–4 May 2017
Security & Counter Terror Expo
London, UK
www.counterterrorexpo.com