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 providers, 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 thing, financial risk.

Continued on page 2...

Contents

NEWS
Financial institutions become more confident about cyber-security but weaknesses remain 1
Zero days last for years 2
FEATURES
Encryption as the cornerstone of big data security 5
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.
Software vulnerability management: how intelligence helps reduce the risk 10
Every year, thousands of software vulnerabilities are discovered and the exploitation of these vulnerabilities can cause extensive damage. Organisations need to have a complete picture of the vulnerability landscape as it applies to them. A programme founded on vulnerability intelligence will help minimise the risks, says Vincent Smyth of Flexera Software.
Why communication is vital during a cyber-attack 12
Cloud-based communications platforms can help an organisation improve emergency communications and most effectively recover from the effects of a cyber-attack. Critical communications platforms can help businesses prepare for a breach to limit downtime and damage, explains Nick Hawkins of Everbridge.
The Russians are coming! Are security firms over-hyping the hacker threat? 15
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? Tim Ring surveys a number of experts to ask if we’re addressing the real threats.
Ransomware and the GDPR 18
Ransomware is getting sneakier and is being used to attack an ever-greater range of organisations. And there can be serious compliance complications if your systems are affected, explains Andy Green of Varonis.
News in brief 3
Reviews 4
The Firewall 20
Events 20
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. 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...
Software vulnerability management: how intelligence helps reduce the risk

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.

References


Criticality of software vulnerability advisories. Source: Flexera Software.