ComputerWeekly.com TechTarget

E-guide

CW+ Content

Top 10 IT security stories of 2018

In this e-guide:

Just as WannaCry and NotPetya were the top IT security challenges of 2017, the discovery of the Meltdown and Spectre microprocessor vulnerabilities, and several similar vulnerabilities in the months that followed, were probably the single most challenging developments for enterprise IT security teams in 2018.

As enterprise teams raced to patch their systems, they faced patches that are incompatible, leading to crashes, reduced performance and lock-ups. And months after the bugs were disclosed, security experts are still divided over their significance, with some saying they opened up a dangerous new avenue of attacks, while others believe Meltdown and Spectre are not nearly as threatening as other recent bugs.

Otherwise, IT security news was dominated by the growing number of potential cyber threats to the enterprise and the resultant challenges facing IT security teams. A common theme throughout was that any organisation that has any online presence should consider itself a potential target for cyber attack, regardless of its size and industry sector, underlining the importance of IT security for the vast majority of organisations and businesses.

The top challenges for IT security teams highlighted during 2018 include ransomware, illicit cryptocurrency mining, fileless malware, cross-operating system attacks, hardware vulnerabilities – including Spectre and Meltdown – and vulnerabilities in internet-connected devices making up the internet of things (IoT), as well as other emerging technologies enabling digital transformation such as machine learning and artificial intelligence (AI).

But a recurrent theme in 2018, as in previous years, was that many organisations are still failing to get the basics right when it comes to cyber security. This was shown to be true with report after report linking cyber breaches to basic security failings or oversights. Allied to this, industry experts throughout the year pointed to the fact that organisations are failing to learn the lessons from past attacks to identify weaknesses and improve cyber defences.

One of the key goals for IT security teams identified through the year is to have visibility of where data lives and moves, and who has access to it, as well as ensuring that their organisations are cyber resilient, in the sense that they are able to recover normal business operations after any information security incident.

Other industry reports underlined the importance of cyber resilience as well as adopting a more proactive approach to security, with a growing number of information security suppliers providing the opportunity for IT security teams to switch to an intelligence-led approach to capitalise on the insights gained from all the security-related systems deployed throughout the enterprise.

Artificial intelligence in the context of cyber security has received a lot of attention in the past year, and while there are clear cases where AI technologies can help organisations to improve their cyber security capabilities, security experts have consistently warned that AI is not the answer to all information security threats, with some urging businesses not to put too much faith in using AI, but to focus instead on educating users on cyber hygiene and managing risks.

While AI was among the most discussed technologies in relation to cyber security, the zero trust model was among the most discussed approaches to security as an alternative to the traditional approach to address many of the new and emerging challenges. Supporters of the zero trust approach claim it is finally gaining traction because of the development of enabling technologies and the business benefits that appeal to business leaders. However, experts say IT security teams should be wary of marketing hype and focus instead on security architecture best practices to realise the benefits of the zero trust model.

Warwick Ashford, security editor

Contents

Meltdown and Spectre a big deal for enterprises

Warwick Ashford, security editor

Now the microprocessor exploits dubbed Meltdown and Spectre have been made public, security experts believe malicious actors will be quick to incorporate them into their cyber attack arsenals, and are advising there is no time for enterprises to delay taking action.

According to researchers at security firm McAfee, these exploits are uniquely attractive to malicious groups or persons because the attack surface is nearly unprecedented, the attack vector is relatively new, and the impacts – privilege escalation and leaks of highly sensitive memory – are detrimental.

The most likely way enterprises could be affected is in the exploits making it easier than ever for attackers to acquire domain administrator or other high-value credentials. The exploits may also allow an attacker to build a map of kernel memory layout, which could then be used in another attack.

Meltdown is an Intel processor-specific vulnerability that allows user processes to infer the contents of kernel memory by creating cache loads in locations based on the illegally referenced contents of the kernel memory, thereby leaking the contents.

Spectre, however, is not manufacturer-specific, and nearly all modern processors have the flaw. It uses conditional logic to train the system to incorrectly anticipate application behaviour. This tricks the system into breaking process isolation, temporarily executing instructions that create observable effects, constituting a covert channel.

According to Jeff Pollard, principal analyst at Forrester, the chip vulnerabilities highlight the complexity of the attack surface that enterprise security and risk professionals are charged with defending.

“Enterprise security teams will need to prioritise the testing and deployment of the patch, or risk leaving an opening for attackers to exploit. This is why we stress zero trust as a fundamental concept in cyber security. Your hardware is not secure, your software is not secure, and your security products are not secure,” he says.

What enterprises need to know about Meltdown

The good news is Meltdown is fixable with software updates. The Information Commissioner’s Office is among the leading voices advising enterprises in all sectors to apply as soon as possible the security updates for operating system software to mitigate against the Meltdown exploit.

Intel received assistance from operating system contributors to Linux, along with Microsoft and Apple developing operating system-level fixes for Meltdown for Linux, Windows and Mac OS.

Due to the nature of any patch or update, the McAfee Advanced Threat Research (ATR) team suggests that enterprises first apply manual updates on non-critical systems, to ensure compatibility with software that involves the potential use of low-level operating system features.

The most immediate threat to enterprises, according to Jarno Niemelä, principal researcher at F-Secure Labs, is the memory access provided by Meltdown, which affects every Intel processor made since 1995 that implements out-of-order execution, with the exception of Itanium and Atom.

Circumventing privilege escalation

Before Meltdown, Niemelä said an attacker needed to get system-level access to use credential-stealing tools such as Mimikatz. "But now, with Meltdown, such operations can be done without privilege escalation, which helps attackers significantly. Previously, an attacker was dependent on there being a local vulnerability that allowed privilege escalation," he told Computer Weekly.

Meltdown also makes some other attacks more dangerous, such as Rowhammer, which is based on flipping bits in memory by carrying out a specific sequence of memory operations and has typically been used in privilege escalation exploits.

Before Meltdown, said Niemelä, the effectiveness of Rowhammer was limited by the attacker being unable to see where the critical bits were in kernel memory, but now, as long as systems are not patched, an attacker can see what needs to be manipulated.

Another concern relating to enterprise security is that Meltdown potentially makes it possible for attackers to exploit vulnerabilities that were previously mitigated by kernel address space layout randomisation (ASLR).

Forrester Research recommends enterprises also:

- Patch hypervisors such as VMware ESXi.
- Expect firmware to be released by manufacturers to address underlying CPU microcode.
- Patch cloud workloads if they are running infrastructure as a service (IaaS).
- Discover the patch-level status of technology partners.
- Ensure bare metal servers cannot execute arbitrary code.
- Take advantage of monitoring tools.
- Scan the environment on a weekly basis to ensure the right level of situational awareness.

While cloud suppliers have already taken steps to patch underlying infrastructure, Forrester said enterprises must patch all virtual machines (VMs) and containers, too. But platform-as-a-service (PaaS) and software-as-a-service (SaaS) systems should not require any customer intervention.

PaaS and SaaS providers should install the patches for customers, but the UK's National Cyber Security Centre (NCSC) advised that if in any doubt, enterprises should check their service providers are aware of the issue and installing fixes.

Because Meltdown violates the boundaries developers and security professionals relied on for years to keep data secure, Forrester warned that without patching systems, all the data an organisation views, processes or transfers is at risk.

Third parties that take too long to update systems will put enterprise and customer information at risk, warned Forrester, urging enterprises to cooperate and collaborate to make sure partners take this threat seriously.

Enterprises that do not exercise basic hygiene by limiting access to administrators are already exposing themselves to unnecessary risk, said Forrester, warning that the likely vector for attack against a bare metal server was through exploitation of a vulnerability in an external service. "Now is the time to be extra diligent in remediating other software vulnerabilities," said Forrester.

Microsoft has released PowerShell scripts, and Linux includes commands to determine whether a processor is vulnerable to Meltdown. Until these techniques are incorporated into vulnerability management and infrastructure-monitoring tools, Forrester said using the available scripts and commands might be the only way to determine initial exposures and remaining exposures after patching.

What enterprises need to know about Spectre

Spectre cannot be fixed with software updates, which means it is a far bigger problem for the enterprise, according to Forrester.

Spectre can be mitigated only with microcode updates, but fixing Spectre permanently requires replacing the affected processors. However, the bad news is there is currently no hardware available without the flaw to replace affected processors with.

Given that new processors and architectures can take five to 10 years to hit the market, Forrester said sacrificing performance for the microcode fixes was the best option.

However, given the complexity of distributing those fixes by device manufacturers, the analyst said enterprises should plan to use other techniques to protect data from users and companies that have not applied the fixes.

In addition to applying fixes to microcode, enterprises should:

- Recompile applications built in-house using Retpoline instructions introduced by Google to isolate indirect branches from speculative execution.
- Plan to staff additional support resources during releases because there may be a spike in demand due to application performance issues or other problems related to the microcode patches.
- Prioritise application software updates related to Spectre as they are release

Prioritise cloud security

The steps that cloud providers are taking to counter Meltdown and Spectre largely involve updating the underlying technology stacks their services run on. However, Forrester noted that infrastructure and operations teams would need to update all virtual machines and containers that run on top of them.

When it comes to on-premise workloads, Forrester warned that enterprises would be responsible for their entire stack, including operating systems, underlying hypervisors and firmware. Enterprises may also need to update management interfaces that have their own CPUs, resulting in higher-than-normal workloads for sysadmins, reliability managers and cloud engineers.

In mitigating against potential Meltdown and Spectre attacks, enterprises are advised to prioritise securing their cloud deployments.

Forrester recommends CIOs should:

- Draw up a plan for communicating information about the chip vulnerabilities and the enterprise's strategy for remediating them.
- Work with the chief risk officer (CRO) to express impact in business terms for execs and the board.
- Celebrate the infrastructure and operations (I&O) team, which has a busy time ahead.

Both exploits lower the requirements for unauthorised parties to access and exfiltrate data from machines. For example, attackers no longer need code execution on a specific device or operating system instance because side channels for data leakage exist if an attacker is present on a system with an unpatched processor.

Enterprises must, therefore, expect that any information on their systems is being read by someone else as long as they remain unpatched.

To target a firm specifically, attackers must find a way to force the cloud infrastructure provider to place them on the same bare metal server where your systems reside. According to Forrester, this is difficult to achieve, and the most likely scenario is criminals will begin mining the systems of their cloud "neighbours" for monetisable information.

Apart from cloud environments, systems likely to be at highest risk are:

- Endpoints that cannot be guaranteed not to run untrusted code.
- Old systems running OS versions that cannot or will not be patched.
- Any system outside the firewall.

Prepare to take a hit on performance

The nature of the software updates to fix Meltdown and mitigate Spectre means the performance of enterprise computer systems will suffer.

Multi-tenant systems and applications that rely heavily on kernel-level system calls, such as databases, will be most affected, but according to Forrester, enterprises are less likely to see an impact on desktops, laptops, tablets and mobile phones running user-focused applications such as web browsers, messaging apps and word processing software.

Initial projections were that enterprises could see performance losses of up to 30%, but so far that does not seem to be the case. Chip makers and software suppliers have indicated that while the patches will add some degree of overhead to operating systems and virtualisation software, depending on the type of workload, they will not cause widespread performance problems.

These claims appear to be true in most cases, according to *GeekWire*, which cited John Graham-Cumming, who oversees a huge network of servers as chief technology officer at Cloudflare, as saying the various patches for Meltdown and Spectre appeared to have had a "negligible" impact on the Cloudflare infrastructure.

However, *GeekWire* said patches for Meltdown and Spectre were affecting applications that need to request data from the operating system kernel on a regular basis, while some mitigations for Spectre appear to be hitting performance for applications that tap into hardware virtual machines.

Most of the performance impacts come from transitions between user and kernel memory space, which means enterprises could batch operations that require such transitions and minimise their number, said F-Secure's Jarno Niemelä.

"So once developers are familiar with the new normal, they will be able to optimise their code to minimise the impact. Also, next versions of compilers will most likely contain optimisations to help in avoiding the impacts," he added.

Gartner's Nik Simpson says the potential performance impact is most likely to affect:

- Applications that are input/output or network intensive, as this sort of workload will involve constant interaction with the kernel of the operating system.
- Hosts that are running unsupported operating systems that the supplier does not plan to patch.
- Systems that run close to maximum capacity.

"Both of these options will increase overall costs. However, it's important to stress that the performance impact will be negligible for most applications, so there's no need to panic at this point, but it is something that will need watching," he said.

If software suppliers do not patch older versions of operating systems that are still in use, Nik Simpson, managing vice-president, architecture, at Gartner, warned this could cause problems for enterprises. "Because of this issue, organisations may be forced to update to phones and PCs running a supported version of the OS, and that may introduce application compatibility problems," he said.

Close web browsers

In addition to operating system patches, Niemelä recommended that enterprises harden the external attack surface, which is rather problematic, as especially Spectre attacks can also be run from Javascript executed by web browser.

How to mitigate performance problems

- Increase the CPU resources assigned to virtual machines.
- Buy hardware that is more powerful.

Because attackers could potentially steal passwords from user process memory when running as Javascript from a web page, Niemelä said it might be a good idea to train users to always close web browsers when not in use. “I have to admit that even a security-conscious person like me is very often at fault on leaving 20 or so pages in the background for later reading,” he said.

However, Apple has released updates for Mac OS and iOS to block Spectre exploits via the Safari browser, and Google has provided an experimental patch for Chrome. Enterprises should apply browser updates and patches as soon as they are available, said Niemelä.

“For high-value targets it might be worth considering using JavaScript blocking and limiting what scripts are allowed to run in a browser, but this tends to break the usability of modern websites,” he said.

Niemelä also recommended implementing multifactor authentication (MFA), so that even if an attacker was able to steal passwords, they would be useless without MFA access.

“We have to assume that even with OS patches, there may be residual risk of Meltdown and Spectre working on some conditions, but that can be mitigated by using high-quality endpoint protection solutions because, with the exception of JavaScript, both exploits need code running in a target system,” he said.

As a bare minimum, Simpson said enterprise IT teams should make plans to patch hypervisors and operating systems, and potentially update browsers.

“This may require internal testing before deployment to ensure there are no application compatibility problems and determine the extent of any performance impact. Also set aside maintenance time for affected systems, as patching the OS and hypervisor may require downtime,” he advised.

High profile, low risk

In summary, Meltdown and Spectre are significant vulnerabilities with a widespread impact, but the overall risk is low because exploitation of the vulnerabilities requires local admin access to the system, said Javvad Malik, security advocate at AlienVault.

"If someone has already compromised your system to that level, there are probably bigger problems to worry about. Google, AWS [Amazon Web Services] and Azure are already fully patched, so users should be protected. For on-premise computers and servers, the advice is to keep all systems fully patched and up to date.

"It's a major finding, but there have been no known instances seen in the wild, and there is little users can do beyond updating and patching all their systems," he told Computer Weekly.

Despite concerns about the potential impact of Meltdown and Spectre, McAfee has put a positive spin on the discovery of the exploits. "This was another major security flaw discovered and communicated by the information security community, as opposed to the discovery or leak of 'in the wild' attacks.

"Will this disclosure have negative aspects? Most likely, yes, but the overall effect is more global attention to software and hardware security – and a head start for the good guys on developing more robust systems and architectures for secure computing," the company's threat research team said in a blog post.

Next Article

Cyber security vulnerability concerns skyrocket

Warwick Ashford, security editor

System compromises and ransomware are the greatest threats to organisations, with 20% listing both as their primary concern, according to Neustar's *International cyber benchmarks index* report.

These are closely followed by distributed denial of service (DDoS) attacks (19%), financial theft (18%), and attacks on intellectual property (17%), the survey of security professionals across Europe, the Middle East, Africa and the US shows.

Nearly half of those polled (47%) see DDoS attacks as increasingly harmful to their organisation this year, up from 38% in 2017. On average, 40% of respondent organisations said they have been targeted by DDoS attacks.

Almost all companies surveyed (98%) have taken steps to minimise risks from attacks exploiting the Meltdown and Spectre chip vulnerabilities, with 90% of respondents saying they believe these attacks will become the norm.

Neustar's *Changing face of cyber attacks* report, which examined the effects of memcached attacks and the largest DDoS attack ever recorded at 1.7Tbps, demonstrates how the different types of threat propagating today, combined with the sheer volume of attacks, can paint a discouraging picture.

The report also underlines that today's threats seldom occur in isolation. For example, a DDoS threat in one segment can divert attention from malware in another, while ransomware can be used to hasten data exfiltration.

According to the report, IPv6 attacks will rise as companies adopt the new standard. Neustar thwarted what is believed to be the first IPv6 attack, which presented a new direction that attackers are likely to pursue as more and more companies adopt IPv6 and run dual IPv4/IPv6 stacks, the report said.

Running IPv4 and IPv6 in parallel speeds up IPv6 network implementation, but works against consistent security, the report warns. It adds that matters are complicated even further by the fact that many security tools still do not support IPv6 or may not be configured properly, which allows attackers to bypass firewalls and intrusion prevention systems, generating malicious IPv6 traffic that these controls do not recognise.

The growth of devices making up the internet of things (IoT) is paving the way for botnets, which are constantly evolving, the report said, pointing out that cyber criminals can rent or buy these botnets with ease, making these threats one of the biggest issues for enterprises today.

Rodney Joffe, Neustar senior vice-president and fellow, said the reports' findings should come as no surprise to anyone.

"Yes, security professionals are becoming more concerned about the level of threat to their organisations, because that same level of threat is continuing to rise at an extreme rate," he said.

"As we have seen over the past year, there are more threats to be aware of, whether in the form of DDoS, malware, application layer attacks or something else entirely, leaving professionals confused about where the next attack is coming from.

"To successfully prepare for a cyber attack in today's landscape is to accept that your organisation will be the next target. If you are online, you are susceptible to an attack. Whether you are most vulnerable or not is entirely up to you."

↘ Next Article

Europol cyber crime report highlights emerging threats to enterprise security

Tasmin Lockwood, guest contributor

Ransomware attacks are becoming more targeted and less opportunistic, Europol has found, while warning enterprises of the threat posed by new and emerging forms of cyber attack.

Ransomware is now a standard attack tool for cyber criminals, but there has been a shift from random attacks to targeting specific companies or people, *The internet organised crime threat assessment 2018* report by Europol warns.

While there was not a large volume of reports last year, mobile malware is expected to grow as users shift from online to mobile banking – a threat to both private and public organisations.

European states must also be aware of emerging threats, such as cryptomining and payment card fraud. The targeting of financial instruments is not a new phenomenon, but criminals are now attacking businesses and users of cryptocurrencies.

Another emerging threat flagged in the report is the popularisation of “true” cryptomining malware, which uses the processing power of infected machines to mine cryptocurrencies without the owner realising.

The findings anticipate a more pronounced shift towards privacy-oriented currencies, with an increase in extortion demands and ransomware within cryptocurrencies.

Europol executive director Catherine De Bolle said the report highlights why law enforcers must be up to date with emerging technologies.

“Cyber crime cases are increasingly complex and sophisticated,” she said. “Law enforcement requires additional training and investigative and forensic resources in order to adequately deal with these challenges.

“The policing opportunities arising from emerging technologies, such as big data analytics and machine learning, need to be seized.”

Skimming bank cards, where data is illegally collected from the magnetic strip, remains a common problem throughout Europe, but card-not-present fraud continues to be a dominant threat.

The continued decrease in card skimming is a result of geoblocking measures as data is often sold overseas via the dark web, where Europay, MasterCard and Visa (EMV) have implemented either slow or non-existent service.

Rusty Carter, vice-president of product management at Arxan Technologies, a company specialising in application attack prevention and self-protection for internet of things (IoT), mobile and other applications, said: “There is no technological reason why traditional skimmers should still be effective.
“The industry and institutions should be looking ahead to move beyond traditional cards and even chip and PIN, to more advanced MFA [multi-factor authentication] before authorising payments and withdrawals.

“CNP fraud further highlights the need for MFA in transactions. Institutions and issuers will need to build the infrastructure to enable PoS [point of sale] and online merchants, and start requiring it at least initially for high-value transactions.

“These are well-known security techniques in other industries and enterprise information security, where additional authentication factors and environmental conditions need to be present, such as a secured app for token retrieval by the user, in order to escalate privileges.”

According to Europol, the most effective defence against cyber crime is the education of potential victims. Law enforcement organisations should raise awareness of threats and trends while supporting prevention, it said.

This includes working with cryptocurrency-related businesses such as exchangers, mining pools or wallet operators. Cyber crime investigators should receive specialist training for investigating cryptocurrencies.

Enhance cooperation

De Bolle said: “Europol will continue its efforts to enhance cooperation with international law enforcement and government agencies, tech companies, academia and other relevant stakeholders. Only if we do this can cyber crime be combated effectively.”

Sir Julian King, European commissioner for the security union, said: “As the report shows, Europe is still faced with a range of security threats from terrorism and cyber.

“We will continue to take decisive action to tackle these threats through our proposals on terrorist content online, electronic evidence and on election security, and through our cyber security strategy.

“As this report highlights, to tackle these threats, we need to foster trust, information-sharing and cooperation between all stakeholders.”

The sexual exploitation of children continues to be the most disturbing aspect of cyber crime, with the report outlining how technology is facilitating this crime.

Access to internet-connected devices and social media, which often benefits from end-to-end encryption, means children are targeted more easily and exposed to vulnerabilities.

Self-generated images that are shared voluntarily may fall into the hands of sexual offenders, or minors may be exploited, the report warns.

Europol, which is now making sexual exploitation a cyber crime priority, believes the web has enabled offenders to interact with each other online and obtain indecent material of children in volumes that were unimaginable 10 years ago.

Responding to the findings, Dimitris Avramopoulos, European commissioner for migration, home affairs and citizenship, said the EU is especially committed to tackling cyber crime involving the sexual exploitation of children and terrorism.

“Cyber criminals continue to threaten and attack our citizens online, endangering both their virtual and physical integrity, especially the most vulnerable ones,” he said.

“Together with Europol, the EU is committed to step up its fight against all areas of cyber crime and especially the sexual exploitation of children as well as terrorist content online, both legally and operationally.”

↘ Next Article

UK firms too confident about cyber security

Warwick Ashford, security editor

Despite the growth in data breaches, senior executives at UK organisations think their cyber security protection is top-notch, a survey has revealed.

Three out of four executives from UK firms (75%) said their company was better prepared than their competitors – up from 60% a year ago – and 43% said their firm was a top performer, according to the survey by research and consultancy firm Ovum for Silicon Valley analytics firm FICO.

Despite this confidence, only 36% of organisations are carrying out regular cyber security risk assessments.

“These numbers suggest that many firms just don’t understand how they compare to their competitors, and that could lead to a lack of investment,” said Steve Hadaway, FICO’s general manager for Europe, the Middle East and Africa. “When we review firms’ cyber security risk with our FICO Enterprise Security Score, I can tell you that most firms are not above average.”

While this over-confidence was seen across the eight regions surveyed, Canada was the only country where more respondents (44%) said they were a top performer for cyber security protection.

Among UK industries, financial services firms were the most confident of all, with 55% saying their organisation was a top performer, and 41% saying said it was above average.

Telecommunications providers were second, with 42% saying their firm was a top performer. The least confident – or most realistic – respondents were in retail and e-commerce, with 38% saying their firm was a top performer, and just 19% rating it as above average.

“The grave risk posed to our privacy and security demands that firms take an honest view of their protection,” said Hadaway.

Maxine Holt, research director at Ovum, said IT leaders have more funding than ever to protect their organisations from the continuously evolving threat landscape and to meet complex compliance demands.

“These same IT leaders are undoubtedly keen to believe that the money being spent provides their organisation with a better security posture than any other – but the rapid pace of investment, often in point solutions, rarely takes an organisation-wide view of security,” she said.

Ovum conducted the survey for FICO through telephone interviews with 500 senior executives, mostly from the IT function, in businesses from the UK, the US, Canada, Brazil, Mexico, Germany, India, Finland, Norway, Sweden and South Africa. Respondents represented firms in financial services, telecommunications, retail and e-commerce, and power and utilities.

Last month, FICO announced that it is offering free subscriptions to the Portrait portal of the FICO Enterprise Risk Suite, which gives businesses access to their FICO Enterprise Security Score. The score, a machine learning-based cyber security rating service, can show organisations how business partners and cyber insurance underwriters see their network security, and can help them to benchmark their performance.

Next Article

Business not learning from past cyber security incidents

Warwick Ashford, security editor

Cyber security incident after incident is demonstrating organisations are still failing in the basics, but they also show that few are learning from others' past mistakes, according to Troy Hunt, Pluralsight author and security expert.

"A good example of this is the BrowseAloud compromise that hit thousands of government websites and organisations in the UK and around the world," he told Infosecurity Europe 2018 in London.

"Despite the fact this had a fairly significant impact, many organisations have not learned the lesson and most websites are not applying a free and easy fix, including those belonging to some UK and US government departments and some major retailers."

The problem was caused by the corruption of a file in the Browsealoud website accessibility service that was automatically executed in the browsers of visitors to the site.

In addition to running the BrowseAloud service in the browser, the corrupted file also launched cryptocurrency mining software to enable the attackers to tap into the computing resources of visitors to affected sites to mine Monero cryptocurrency for the benefit of the attackers.

“This can be stopped with the use of a content security policy (CSP), which is just a few lines of code organisations can add free of charge to their websites to ensure that only approved scripts run automatically when they use third party services like BrowseAloud,” said Hunt.

“Despite the incident highlighting this issue, barely anyone is using CSPs. In fact, only 2.5% of the world’s top one million websites currently use CSPs to defend against rogue content,” he said.

Hunt said a cryptocurrency miner was perhaps the one of the “most benign” forms of content attackers could have chosen to launch through the compromised BrowseAloud file. “In reality, we got off lightly this time around, but we have not seen any significant action by website owners in response.”

This incident underlines the fact that many websites use services and content from third parties, which represents a security risk because attackers could compromise this is the way that the BrowseAloud file was compromised and execute malicious code through millions of websites.

“An analysis of the US Courts website reveals that its home page represent 2.3Mb of data, which is the same size as the entire Doom game, and that almost a third of that is scripts, which is rather a lot of active content that is automatically loaded into visitors' browsers, especially when you consider that you can do just about anything with JavaScript," said Hunt.

Compounding the problem, he said, is that most organisations are poor at detecting malicious activity, which was well illustrated by the Sony Pictures cyber attack in 2014. "Various systems were compromised at the same time and different types of data stolen, but the first the company knew of it was when employees attempted to login and were greeted with a message saying: 'You've been hacked'."

According to Hunt, who runs the HaveIBeenPwned website that aggregates breached records and makes them searchable for those affected, most organisations either have no idea that they have been hacked, and even if they do, they have no idea what data may have been stolen.

"Many of them only find out when they get an email from me telling them that their data is available on the internet," he said, adding that this underlines that fact that detection is often difficult. "But choosing a breach detection tool can be equally difficult. There are so many suppliers selling breach detection solutions, but it is difficult to work out what actually works."

Organisations in the dark

Another indicator that organisations are not covering the basics, said Hunt, is that many organisations still have no idea of what company files are exposed to the internet.

According to security firm Varonis, 21% of all company folders are open to anyone on the internet, and of those open folders, 58% contain more than 100,000 files.

In summary, Hunt said organisations need to assess the state of their cyber security and ensure that at the very least they are addressing the basics because simple, well-known attacks are still working.

Organisations also need to understand that it is easier than ever for cyber attackers to make money out of their data thanks to the advent of cryptocurrencies.

Next, organisations need to understand that their websites and those that their employees visit to do their jobs are made up of code from multiple sources, and any one of these could represent a security risk.

And finally, in the light of the fact that choosing effective and affordable security solutions, organisations should not overlook those that are free and easy to implement.

UK finance sector cyber security pros admit shocking practices

Warwick Ashford, security editor

Two-thirds of UK information security practitioners admit to cyber security practices in their organisation that would “shock outsiders”.

This is the key finding of a survey of 201 UK-based IT security professionals who work in the financial services industry, commissioned by virtualisation and cloud infrastructure firm VMWare.

The survey indicates that IT security professionals in financial services firms are losing the battle to keep vital data safe against a rising tide of cyber threats, with 90% of respondents stating they have to make compromises which could leave other areas exposed when protecting their organisation against cyber threats, and half admitting that they do this regularly.

As the financial services industry continues to digitise, the study suggests too great a focus is placed on protecting the more visible consumer services, such as customer websites, potentially leaving exploitable holes surrounding internal systems and trading data.

Findings show that while there is a huge focus on protection for e-banking and customer applications, 71% of respondents said this is often at the expense of other systems.

The head of Europol, Rob Wainwright, is on record as saying the technological capability of some cyber criminal groups threatens critical parts of the financial sector, and because financial institutions store consumers' and enterprises' most critical, personal and private data, they are a highly attractive target for cyber criminals.

In the light of this fact, the survey report said the findings indicate a need to balance financial organisations' rapid digital transformation with stringent cyber security practices.

There also appears to be a sense of frustration in the direction those responsible for defending against security threats received, alongside a lack of understanding from leadership teams of the potential for breaches, the report said, with 53% of respondents saying they do not believe their leadership team understands the complexity of the cyber threats they are facing.

A quarter of respondents said the impact of cyber crime is simply treated as a cost of doing business, while 62% said they struggle to secure funding for urgent cyber security projects, and 65% said the stress associated with their role is difficult to cope with.

Ian Jenkins, head of network and security at VMware in the UK, said that in chasing the digital promised land, financial services organisations run the constant risk of overstretching already antiquated security infrastructures.

"Those on the front line defending against cyber threats clearly feel there are significant flaws ready to be exploited. This should act as a wake-up call that there are serious risks to data if security isn't baked into everything the organisations do. Ignoring them and the compromises they're having to make could be hugely damaging."

Richard Bennett, European head of accelerate and advisory services at VMware, said the past era of compromise towards cyber security must end.

"A revised approach to protecting digital assets, starting at a security by design philosophy, is required to allow IT security professionals to dynamically manage the myriad of threats now faced," said Bennett.

"This involves understanding that cyber security does not begin and end with IT, but is a challenge for the whole organisation. It is also about recognising that adaptive networking, applications and systems are no longer nice-to-haves, and that cyber hygiene is intrinsic to a company's digital footprint today."

In June 2017, a report by security firm McAfee and analyst firm Ovum said financial services organisations have developed unsustainable security infrastructures, characterised by a huge proliferation of tools, which lengthens response times and reduces effectiveness.

In an attempt to improve the cyber security of financial institutions in the UK, the Financial Conduct Authority (FCA) plans to introduce rules in August 2018 that will require banks to publish details of major security and operational incidents to expose the weaknesses of those with outdated IT infrastructures and compel all banks to be honest about the level of cyber security problems.

Next Article

Firms lack responsible exec for cyber security

Warwick Ashford, security editor

A lack of cohesion at the top means organisations are struggling to secure most important digital assets, a report reveals.

Responsibility for information security is not falling to any one senior executive function, according to the 2018 Risk:Value report from NTT Security.

The report, based on a poll of 1,800 senior decision makers from non-IT functions in global organisations in 12 countries, shows that at a global level, 22% of respondents believe the CIO is "ultimately responsible" for managing security, compared with 20% for the CEO and 19% for the CISO.

In the UK, fewer respondents point to the CIO (19%) and CISO (18%) while the CEO gets the biggest vote at 21%. The US (27%) and Norway (26%) buck the trend with more than a quarter of respondents suggesting the CEO is responsible, while in Singapore, 33% say it is the role of the CISO, which is highest figure across all countries.

In Switzerland, 10% believe the CFO is responsible for security.

"Responsibility for day-to-day security doesn't seem to fall on any one particular person's shoulders among our response base," said Azeem Aleem, vice-president consulting and UK&I lead, NTT Security.

"This narrow gap between the roles of CIO, CEO and CISO shows that no one executive function is stepping up to the plate," he said. "It could be a sign of unclear separation between the CIO and CISO though, as often they are the same or collaborate closely."

On the other hand, Aleem said findings could potentially raise concerns that the CEO is not more involved in security matters, given the potentially damaging affects to the business, but on the other, the findings could bring a sense of relief that CEOs are not managing a specialist task like security over and above other critical corporate responsibilities.

According to the report, although more people see the need for regular boardroom discussions about security, their organisations are failing to raise it sufficiently at the C-suite level. While 80% of all survey respondents agree that preventing a security attack should be a regular boardroom agenda item (up from 73% a year ago) only 61% say that it already is, which represents an increase of just 5% on last year.

The report also suggests this lack of cohesion at the top of the organisation means that many are struggling to secure their most important digital assets. Fewer than half (48%) of respondents globally – 53% in the UK – say they have fully secured all of their critical data. But with the General Data Protection Regulation (GDPR) now fully in effect, this is no longer an opportunity, but mandatory, the report notes.

However, companies are beginning to take control of their data as cloud computing best practices mature, with 27% reporting that the majority of their organisation’s data is currently stored on premise or in datacentres (25%). However, in 12 months’ time, a similar proportion (25% of respondents) say that it will be stored in a cloud environment.

Next Article

Time to implement new cyber security protections, says McAfee CEO Chris Young

Warwick Ashford, security editor

Cyber defence is becoming increasingly difficult, and there are three key indicators cyber security professionals need to look at and learn from, according to Chris Young, CEO of security firm McAfee.

These key indicators are the threatscape (what attackers are doing, the technology landscape), the reshaping of what is happening underneath it, and the regulatory climate and environment, Young told the opening session of the 2018 MPower cyber security summit in Las Vegas.

While the latest attack to dominate the headlines is cryptojacking, with the instances of new associated malware seeing a 500% increase in the past year, he said that looking back over the past 30 years the patterns are not new.

“What’s old is new again in cyber security. That is a trend that is as old as our industry itself,” said Young, citing WannaCry as a classic example of how attack methods endure, morph, change, evolve and combine new and different ways to spawn new generations of threats.

“The reason we see exponential growth in the complexity of the attack landscape is because there are force multipliers at work,” he said, adding that “there are ever more opportunities for attackers to insert new methods like living off the land attacks” that continue to make defenders’ jobs ever more challenging.

McAfee expects to see the increased use of scripting languages, abuse of legitimate application macros, file-less malware and cross operating system attacks.

As attackers continue to evolve, Young said defenders need to respond with greater precision in identifying attacks and with greater coverage and agility across the IT landscape.

In addition to the threatscape, he said defenders need to pay attention to the “shifting landscape of technology,” particularly the “major transformation” in the way applications are being developed, delivered and consumed, which is being driven by the cloud.

Software as a service (SaaS) is “completely changing the game”, said Young, and completely changing the way cyber defenders and cyber security suppliers need to think about their work.

“Enhanced connectivity is changing the nature of the interaction between the device and the application, they are becoming extensions of one another. Data increasingly resides between and among devices that are connected from everywhere and applications running in the cloud,” said Young.

Adding to the complexity, he said the role of the network is continuing to blur as users increasingly connect to applications and data in the cloud completely outside of organisational networks.

“On the other hand, with the IoT [internet of things], there are literally millions of new devices are connecting through those networks, and 5G is going to blow the doors wide open on this problem,” said Young.

“That convergence in our technology environments is as much a challenge as the convergence we are seeing in the threatscape, which means we will have to manage things differently, but we are not done yet because the regulators are now getting in the game,” he said.

Citing the EU’s General Data Protection Regulation (GDPR) as a prime example of significant regulatory change that is “upping the ante” around data protection and transparency in the use of data, Young said the GDPR is completely changing the regulatory landscape around the world.

The convergence in the threatscape, IT landscape, technology and the regulatory environment, is a pointer where cyber defence has got to next, he said.

“What it tells us is that it is time to speed up our ability to implement new methods of protection, to deliver the outcomes that cyber security professionals need to deliver on behalf of their organisations. It is time to unify threat defence and data protection in new ways in priority and in principle.

“They are not different domains. It is time to eliminate the silos that prevent us from being able to see, to manage and change our security controls in a changing operating environment. It is time to reap the benefits of every connected sensor we have available so we can get to those insights about our threat profile,” said Young.

Young argued that organisations that try to manage cyber security capabilities in siloed domains will fall behind.

“Attacks are increasing across devices and across platforms. They live in the cloud and manifest on devices and vice versa, so in time, your defences have to span different domains,” he said, adding that it is time for a new approach to cyber defence, starting with things that are “designed in and for the cloud to provide the agility and coverage that is needed.”

Noting his 2016 commitment to cloud and McAfee’s acquisition of Skyhigh Networks in January 2018, Young said McAfee now offers an “industry leading solution” that is designed to protect workloads, data and users across cloud-based software, platform and infrastructure environments as organisations move their infrastructure, data and users to the cloud.

“We now secure data in our cloud platform from, to and between clouds,” he said, which is done by applying behavioural analytics to identify threats and stop attacks that are born in cloud services. “We have converged the way we think about threat defence and data threat protection in our design just as they are converged in your cloud reality.”

Introducing MacAfee’s new Mvision portfolio, Young described it as a “new family of products” that are “cloud-led, cloud-native management-oriented” and built for the convergence that is happening in enterprise environments, encompassing a wide range of capabilities.

These already include ePO (ePolicy Orchestrator) as a cloud-based service, ENS (Endpoint Security), mobile security and cloud security. It will soon also include EDR (Endpoint Detection and Response).

“It’s the first of its kind family of cloud-based capabilities offering data protection and threat defence from the device all the way through to the cloud,” said Young, adding that it encapsulates what has been McAfee’s strategy for a number of years to “focus on where the action is”, which is in the cloud.

Mvision, said Young, is made up of five cloud-based capabilities representing McAfee’s commitment to the future. “[It is] our commitment to fearless innovation across all areas of our strategic roadmap, which delivers ultimately on a promise of true security [as a service],” he said.

“McAfee is the only company now that is empowering organisations to holistically manage security capabilities from device to cloud, and we are doing it all from within the cloud,” he said.

Looking to the future, Young said McAfee is setting its sights on providing unique insights into what is happening in any IT environment based on advanced analytics on data gathered from nearly a billion sensors deployed on consumer devices, within enterprises worldwide and across cloud environments.

“We are committed to an outcome-driven future where actionable insights can change the game for organisations against the attacker,” he said, by identifying what the attacker was after and whether they were successful or not, which device or third-party supplier was ‘patient zero’ and if the same attack has been seen elsewhere in the world.

While a lot of organisations can tell companies what is going on in their PCs and threats in the wild, "very few can bring it all together to give you the insight across the converging IT landscape the way that McAfee will," said Young.

"We believe that for all the convergence that is happening, it is time to harness that to give you unique insights, and it is the next phase of our journey."

Next Article

How AI will underpin cyber security in the next few years

Nicholas Fearn, guest contributor

Cyber criminals continue to launch increasingly sophisticated and devastating attacks on industrial, business and financial organisations around the world – and the damage from such crime could reach $6tn by 2021, according to a report from Cybersecurity Ventures.

It has become clear that organisations cannot simply rely on manpower and human interaction to fight off cyber attacks. Not only is it time-consuming for employees to spot potential threats, but it is also challenging to come up with security technologies to prevent them. So there are fears that businesses will continue to fall victim to hackers.

As a result, organisations are being forced to consider new ways to boost their cyber defences. Whether it is implementing new cloud strategies or big data analytics, many companies are showing that they can think outside the box when it comes to modernising their IT security defences.

But artificial intelligence (AI) is emerging as the frontrunner in the battle against cyber crime. With autonomous systems, businesses are in a far better place to strengthen and reinforce cyber security strategies. But does this technology pose challenges of its own?

Large organisations are always exposed to cyber criminals, and so they need appropriate infrastructure to spot and combat threats quickly. James Maude, senior security engineer at endpoint security specialist Avecto, says systems incorporating AI could save firms billions in damage from attacks.

“Although AI is still in its infancy, it’s no secret that it is becoming increasingly influential in cyber security,” he says. “In fact, AI is already transforming the industry, and we can expect to see a number of trends come to a head, reshaping how we think about security in years to come. We might expect to see AI applied to cyber security defences, potentially avoiding the damage from breaches costing billions.”

But Maude believes the use of AI in cyber security is a double-edged sword. While businesses will see the benefits, criminals will also tap into this technology to automate attacks. He says businesses could “see criminals and nation states using innovative AI attacks to do serious harm to everything from companies’ reputations to critical infrastructure”.

Andy Powell, vice-president and head of cyber security at professional services firm Capgemini, agrees that criminals could turn to AI to drive their attacks. “From a hacker’s point of view, AI will power attacks, from automatically generating and launching distributed denial of service (DDoS) attacks via the internet of things (IoT), to rapidly analysing code and system weaknesses before inserting exploitation methods,” he says.

New opportunities

Based in the UK, RazorSecure is an example of a cyber security company that is capitalising on the potential of AI. It uses AI techniques to recognise attacks targeting the aviation, rail and automotive markets, and is one of nine cyber security firms chosen to take part in GCHQ’s latest Cyber Accelerator.

Alex Cowan, CEO at RazorSecure, says AI and deep learning will transform cyber security approaches in the coming years. “Artificial intelligence is a big part of the future of cyber security,” he says. “One of the key areas we must solve is how to not only use deep learning for correlation detection, but also causation. Without understanding the ‘why’ behind a cyber security incident, we will always be chasing false positives and lacking the ability to prioritise a growing queue of cyber security incidents.

"Cyber security is a difficult enough problem. We must use AI to bring a new focus and to enhance and improve our ability to manage security of systems. Given the shortage of cyber security professionals and the explosion in IoT and cloud systems, at RazorSecure we are focused on working smarter, not harder. And as an industry, we must stop inflating the scale of the problem."

Headquartered in Cardiff, Amplyfi is a cutting-edge business that is using AI to transform cyber security research. It has created a machine learning platform that mines the deep web for key security trends. The company recently completed a project with Harvard University that explored North Korean biological warfare threats.

Chris Ganje, CEO at Amplyfi, says: "Artificial intelligence is prevalent across almost every industry and, among other things, is an indispensable tool to help uncover the threat landscape to organisations' competitive advantages.

"In cyber security, AI can automatically identify potentially malicious software behaviour, attack vectors and related anomalies in real time, allowing a continuously adaptive defence mechanism to identify and shut down intrusions faster and easier than ever before. This technological advancement not only significantly reduces the number of cyber security breaches, but also empowers analysts to better focus their time and speeds up the process to identify breaches from hundreds of days to mere hours."

Farrpoint, an independent consultancy that advises companies on matters surrounding IT infrastructure, cyber security and connectivity, has also shifted its attention to AI. It has worked with a number of high-profile clients, including Kwik Fit, Total and Clarks, and public sector organisations such as the Scottish government, the NHS and the London Borough of Greenwich.

Dan Brown, a cyber security consultant at Farrpoint, says companies can speed up response times by implementing machine learning. "Traditionally, identifying a cyber threat would require prior knowledge of the function and source of the threat," he says. "Machine learning means that technology can adapt and improve, using its learned knowledge to flag up shared characteristics of threats and pre-empt a previously unseen attack.

"The continual seep of AI into security offerings should help shift the balance of power, giving companies the upper hand, speeding up responses and helping to spot potential problems before they occur. AI is also able to spot, and adapt quickly to, changes in attack methodology."

Managing complex data

With threats becoming more complicated, cyber security professionals are dealing with a growing influx of data. Alexandra Mendes, a senior lecturer in computer science at Teesside University, believes AI is the answer.

“AI systems and techniques have a big role to play in cyber defence,” she says. “In recent years, with the huge increase in the number of systems and security attacks, the amount of data that cyber security professionals have to process has increased dramatically, to the point where it is impossible to process it manually.

“It is also almost impossible to manually detect patterns in the data that can be used to respond to, or prevent, security incidents. Modern AI techniques, such as machine learning and deep learning, have an important role to play in the analysis of that data. They are particularly useful for predicting attacks and providing response plans.

“In fact, these AI techniques have been used to improve the performance of intrusion detection systems. More classic AI techniques, such as AI planning, still have an important role in cyber security systems, for example in the generation of response plans for security attacks.”

Talal Rajab, head of cyber and national security at industry support organisation TechUK, takes a similar view to Mendes. He believes AI can help companies to simplify and quicken their cyber security strategies.

"AI allows companies to understand their adversaries better, predicting where the next attack may come from and helping them respond to cyber threats and attacks more quickly than they can now," he says. "Many companies are currently reliant solely on human expertise to detect anomalies. With the current cyber skills shortage, investing in AI can be a crucial tool in addressing the increase in frequency of attacks, both to businesses and individuals."

Big business benefits

Prakash Arunchalam, chief information officer at customer experience management firm Servion, also sees big business benefits in AI-driven security, and says the technology can improve efficiencies among IT and cyber security teams.

"As more and more devices get connected, the challenges of new security risks is sure to arise, and cyber security experts will need all the help they can get to meet these threats," says Arunchalam. "AI systems are designed to detect even the smallest changes in the environment, and they have the potential to act much faster and fix them. AI will be of tremendous help to identify and analyse such exploits and weaknesses to quickly mitigate more attacks. In 2018, AI-based cyber security technologies will become more mature."

Joining a new breed of security-conscious businesses, telecoms giant BT is using AI to stay ahead of attackers. Mark Hughes, CEO of the firm's security arm, explains how BT has developed a new AI-driven method to identify threats and protect its network.

"Our approach is to enable cyber analysts to perform 'hunting' for unusual or abnormal patterns in huge amounts of different types of data to find early indicators of cyber attacks," he says. "Our patented approach is based on 'intelligence augmentation', where we train a deep learning network to learn what normal network behaviour is and use data visualisation to present deviation from the normal behaviour to human analysts. Typically, the system is trained to produce tens of anomalies from hundreds of millions of logs."

With this technology, the company's 2,500 cyber security experts can get a much deeper insight into threats. Hughes adds: "Once an analyst selects a subset of the anomalies, deeper analysis is performed by the algorithms to determine whether the anomaly points to a real attack or a known vulnerability. In either case, this approach helps analysts deal with much larger volumes of data in a fraction of the time.

"We often refer to this approach of using AI within cyber security as 'Ironman' rather than 'Terminator', aiming to enhance human detection capabilities rather than replacing them."

Jeff Dickerson, CEO at point-of-sale software provider DaySmart, says his company has been using AI security technology from Burning Tree and CyGlass to keep an eye on potential cyber attacks. He says the growth and complexity of threat “makes it difficult for existing security tools to prevent or even to identify today’s’ attacks”. He adds: “We saw artificial intelligence as a way to assist our security team, by reducing the noise and focusing them on what is a potential threat.

“Using products such as CyGlass, which uses a layered AI approach to search through millions and even billions of network conversations and find anomalous behaviour, gives us the ability to find the needle in the haystack while providing a level of protection that cannot be offered with the security products we have become used to in recent years.”

Eben Upton, CEO and founder of Raspberry Pi, has ploughed money into AI security systems from Darktrace to safeguard his firm’s intellectual property. He says: “Darktrace’s AI technology for cyber defence is a game-changer. It provides us with full visibility into our network, including any connected personal devices, and other weak spots.

“Darktrace is unique in its ability to detect and remediate any emerging cyber threats, including ‘unknown unknowns’ that routinely bypass legacy security tools. It allows us to remain resilient in the face of a rapidly evolving threat landscape – despite a flexible IT policy and a lean security team.”

Transforming network security

Eric Ogren, a senior analyst at 451 Research, says the “most promising” area for AI in cyber security is in network security, helping businesses to secure their hybrid cloud infrastructure. “There is huge value in AI applied to network security,” he says. “For one, the network is a data source that never lies. What network security sees on the wire is what is actually happening – there is no dependence on untrusted hosts or agents self-reporting their health status.

“So mapping east-west and north-south flows with network traffic analytics provides a good metric for catching threats, streamlining traffic, and thus improving business outcomes. So much of security is looking outward into the dark web. Sandboxing is one example of reacting to what is actually executing in the network.

“Network traffic analytics with AI approaches twists security conventional wisdom to what is actually seen in the business, as opposed to *a priori* patterns of everything that can be a security risk. We have seen this with FireEye’s work in establishing sandboxing as a major security category based on actual execution performance. We see similar possibilities for AI in network security.”

If there is one technology that will have a massive impact on the world in the coming years, then AI is definitely it. But it is not just powering smart assistants such as Amazon’s Alexa – it is also becoming a prevalent force in the cyber security industry. Although businesses need to be mindful that AI is still relatively nascent, there are already many proven possibilities.

Next Article

Zero-trust security model gaining traction

Warwick Ashford, security editor

Traditional approaches to security are failing because enterprises continue to be breached despite spending billions of dollars a year on security technologies, says Torsten George, product evangelist at security software firm Centrify.

This means we need to do something different, he told Computer Weekly, with 66% of organisations admitting they are still getting breached an average of five times a year as the attack surface continues to expand with increased enterprise use of cloud services and employee-owned devices.

In addition, George said the enterprise is now facing threats introduced by internet-connected devices. "Let's not forget that the massive data breach at US retailer Target in 2013 started with compromising a smart climate control system that enabled the attackers to move laterally within the Target network, which was one of the first IoT [internet of things] breaches," he said.

A post-mortem analysis of the majority of breaches, however, reveals that identity is the top attack vector, with 81% of breaches being linked to weak, default or stolen passwords, which George said indicates that identity is an area organisations need to focus on.

"But currently, not much of the security budgets are being spent on protecting identity, despite it taking just one compromised credential to impact millions of data records and people, underlining that organisations can no longer rely on endpoint security and firewalls, but need to start implementing identity-centric security measures," he said.

This is where zero-trust security comes into play, said George, because it assumes that untrusted actors exist both inside and outside the corporate network and every user access request has to be authorised.

“Therefore, organisations have to remove trust from the equation, because if someone is camouflaging their attack behind a legitimate identity like a database administrator, even if the targeted data is encrypted, the attacker will still be able to access and decrypt it,” he said.

Against this background, George said the zero-trust approach – which was first outlined by Forrester Research and the US National Institute of Standards and Technology (Nist) – has been gaining traction, with Google using it as the basis of its BeyondCorp initiative.

“As a result, Google claims that they have not been hit by any credential-based attacks since implementing the approach of never trust, always verify,” he said.

According to George, verifying users is the first of four pillars of zero-trust security. The others are: validating devices, limiting access of privileged users wherever possible, and then applying machine learning to all these factors to step up the authentication processes wherever necessary.

“Machine learning enables organisations to apply access controls dynamically based on behaviour, time and other factors without requiring manual intervention by an administrator when circumstances change, such as connecting to the corporate network from a new location,” said George.

When it comes to verifying the user, there are three key elements, said George. First is identity consolidation, which involves tying access back to Active

Directory identities to improve accountability by eliminating the risky practice of sharing root passwords.

“This should be supplemented by using single sign-on, where users are not exposing their username and password for each application, but are using instead a one-time password that is time limited, so even if it is compromised, it cannot be used on an ongoing basis.”

Second, is the use of de-facto authentication everywhere, including privileged users and for accessing internal resources such as network devices and servers. “Anything that involves sensitive data and risk should use de-facto authentication, where there is a high degree of certainty that the user actually is who they claim to be,” said George.

The third key element of user verification, he said, is monitoring user behaviour and taking factors such as time and location into account. “If someone typically works between 6am and 7pm, but suddenly logs in at midnight, that should be flagged as abnormal behaviour and trigger additional authentication,” said George.

Partly thanks to improvements in technology capabilities, George said the move to zero-trust security has gained momentum in the past year.

“A study by IDG shows that 71% of security-focused IT decision makers are not just aware of the zero-trust security model, but are actively pursuing that.

Meanwhile, 10% are currently doing pilots and about 8% who have implemented it fully.”

In addition, George said a study by Forrester and Centrify shows that by applying best practices in line with zero-trust priciples, organisations recorded 50% fewer breaches within just two months.

“In addition to cost savings due to gains in incident response efficiencies and technology consolidation, the organisations also reported 67% greater confidence in supporting users on mobile devices and rolling out new partner and customer experiences because they felt they could ensure that participants were secure,” he said.

DevOps environments are increasingly being targeted by attackers, said George. “In this context, the study showed a 44% gain in confidence through applying zero-trust principles, and so overall it really is quite successful,” he said.

However, despite a growing number of organisations buying into the concept, George said some are being held back by the mistaken belief that it takes a lot of time and effort and that everything has to be done at the same time.

“In reality, implementing a zero-trust security model is a step-by-step process, with the first step typically being around identity assurance by consolidating identities and applying more de-facto authentication, before moving further to moving lateral movement by doing things like applying conditional access and enforcing the principle of least privilege," he said.

Once all these things are in place, George said organisations can then move on to auditing everything, analysing the risk, monitoring user sessions and integrating with the security information and event management (Siem) systems.

"But it does not have to be done all at once. It can be done step by step, and we have lost of customers that are doing exactly that, with some starting with securing their laptop environments, before moving to servers and cloud."

Studies show, said George, that there has been a shift towards understanding that security has to start with locking down identity. "But it has taken time, and now suddenly we are finally seeing zero-trust gain traction and gain favour with the c-suite as an effective way to address security challenges.

George is to discuss these topics in more detail in a session entitled: *How zero trust is creating a game-changing security experience* at the Cybersecurity Leadership Summit 2018 Europe in Berlin from 12 to 14 November.

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com