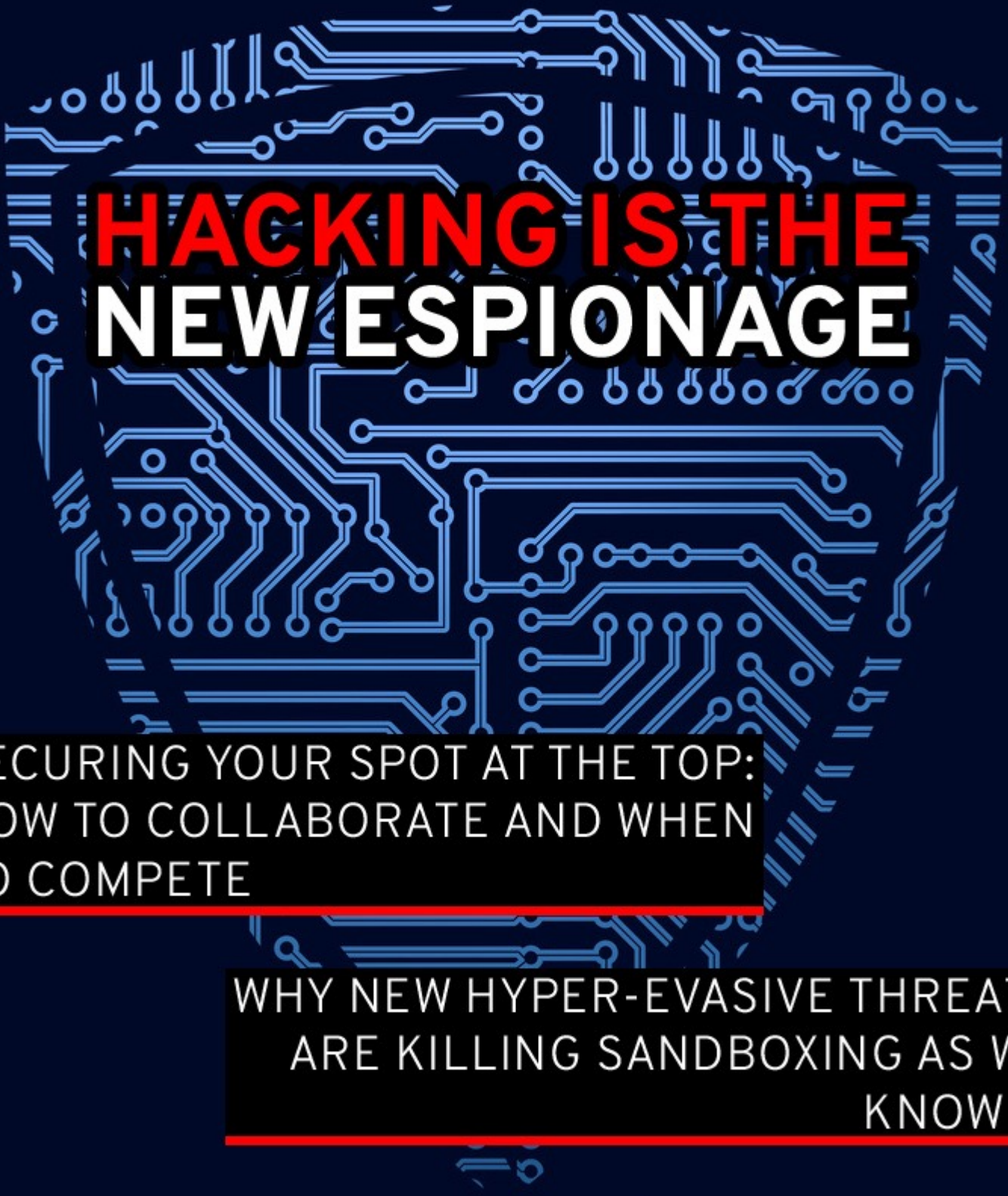
[+] (IN)SECUREMagazine

Issue 51, 09/2016



HACKING IS THE NEW ESPIONAGE

SECURING YOUR SPOT AT THE TOP: HOW TO COLLABORATE AND WHEN TO COMPETE

WHY NEW HYPER-EVASIVE THREATS ARE KILLING SANDBOXING AS WE KNOW IT

WHAT CAN MICROSOFT PATCH TUESDAY TELL US ABOUT SECURITY TRENDS IN 2016?

TABLE OF CONTENTS

(IN)SECURE Magazine 51
CONTRIBUTORS LIST

- **Babak D. Beheshti,** Associate Dean of the School of Engineering and Computing Sciences at NYIT.
- **Clyde Bennett**, Chief Healthcare Technology Strategist at Aldridge Health.
- **Ross Brewer**, VP and MD of EMEA at LogRhythm.
- **Ben Desjardins**, Director of Security Solutions at Radware.
- **Eric O'Neill**, National Security Strategist at Carbon Black.
- **Jeff Schilling**, Chief of Operations and Security at Armor.
- **Karl Sigler**, Threat Intelligence Manager at Trustwave.
- **Sigurdur Stefnisson**, VP of Threat Research at CYREN.
- **Amos Stern**, CEO at Siemplify.
- **Ronen Yehoshua**, CEO at Morphisec.

Visit the magazine website at www.insecuremag.com

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@helpnetsecurity.com
News: **Zeljka Zorz**, Managing Editor - zzorz@helpnetsecurity.com
Marketing: **Berislav Kucan**, Director of Operations - bkucan@helpnetsecurity.com

Are all IoT vulnerabilities easily avoidable?

Every vulnerability or privacy issue reported for consumer connected home and wearable technology products since November 2015 could have been easily avoided, according to the Online Trust Alliance (OTA).

OTA researchers analyzed publicly reported device vulnerabilities from November 2015 through July 2016, and found the most glaring failures were attributed to:

1. Insecure credential management including making administrative controls open and discoverable.
2. Not adequately and accurately disclosing consumer data collection and sharing policies and practices.
3. The omission or lack of rigorous security testing throughout the development process including but not limited to penetration testing and threat modeling.
4. The lack of a discoverable process or capability to responsibly report observed vulnerabilities.
5. Insecure or no network pairing control options (device to device or device to networks).
6. Not testing for common code injection exploits.
7. The lack of transport security and encrypted storage including unencrypted data transmission of personal and sensitive information including but not limited to user ID and passwords.
8. Lacking a sustainable and supportable plan to address vulnerabilities through the product lifecycle including the lack of software/firmware update capabilities and/or insecure and untested security patches/updates.

“In this rush to bring connected devices to market, security and privacy is often being overlooked,” said Craig Spiezle, OTA Executive Director and President. “If businesses do not make a systemic change we risk seeing the weaponization of these devices and an erosion of consumer confidence impacting the IoT industry on a whole due to their security and privacy shortcomings.”

PCI Council wants more robust security controls for payment devices

The PCI Council has updated its payment device standard to enable stronger protections for cardholder data, which includes the PIN and the cardholder data (on magnetic stripe or the chip of an EMV card) stored on the card or on a mobile device.

Specifically, version 5.0 of the PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) Modular Security Requirements emphasizes more robust security controls for payment devices to prevent physical tampering and the insertion of malware that can compromise card data during payment transactions.

The updates are designed to stay one step ahead of criminals who continue to develop new ways to steal credit and debit card data from cash machines, in-store and unattended terminals and mobile devices used for payment transactions. Payment devices that directly consume magnetic stripe information from customers remain a top target for data theft, according to the 2016 Data Breach Investigation Report from Verizon.

“Criminals constantly attempt to break security controls to find ways to exploit data. We continue to see innovative skimming devices and new attack methods that put cardholder data at risk for fraud,” said PCI Security Standards Council CTO Troy Leach. “Security must continue to evolve to defend against these threats. The newest PCI standard for payment devices recognizes this challenge by requiring protections against advancements in attack techniques.”

Vendors can begin using PCI PTS POI Modular Security Requirements version 5.0 now for payment device evaluations. Version 4.1 will retire in September 2017 for evaluations of new payment devices.

Public cloud services market to grow to $208.6 billion in 2016

The worldwide public cloud services market is projected to grow 17.2 percent in 2016 to total $208.6 billion, up from $178 billion in 2015, according to Gartner, Inc. The highest growth will come from IaaS, which is projected to grow 42.8 percent in 2016. SaaS is expected to grow 21.7 percent in 2016 to reach $38.9 billion.

“The aspiration for using cloud services outpaces actual adoption. There’s no question there is great appetite within organizations to use cloud services, but there are still challenges for organizations as they make the move to the cloud. Even with the high rate of predicted growth, a large number of organizations still have no current plans to use cloud services," said Sid Nag, research director at Gartner.

IT modernization is currently the top driver of public cloud adoption, followed by cost savings, innovation, agility and other benefits. The focus on IT modernization indicates a more sophisticated and strategic use of public cloud services. Not only are public cloud services being used to recognize the tactical benefits of cost savings and innovation, but they are also being used to establish a more modern IT environment — an environment that can serve as a strategic foundation for future applications and digital business processes.

Security and/or privacy concerns continue to be the top inhibitors to public cloud adoption, despite the strong security track record and increased transparency of leading cloud providers.

Most organizations are already using a combination of cloud services from different cloud providers. While public cloud usage will continue to increase, the use of private cloud and hosted private cloud services is also expected to increase at least through 2017.

The increased use of multiple public cloud providers, plus growth in various types of private cloud services, will create a multi-cloud environment in most enterprises and a need to coordinate cloud usage using hybrid scenarios.

Compromised electronic health records may haunt you forever

A recent report on the Deep Web black market for electronic health records (EHRs) by researchers affiliated with the Institute for Critical Infrastructure Technology has pointed out that healthcare systems are relentlessly and incessantly attacked.

"Vulnerable legacy systems and devices that lack the ability to update and patch are Frankensteined into networks possessing newer technologies that can be updated and patched. As a result, the organization's IoT microcosm becomes collectively vulnerable as effective layers of security cannot be properly implemented," the analysts noted. "Without the input of cyber risk management professionals and without comprehensive oversight, they will continue to make socially negligent decisions that gamble the electronic health information of US citizens between antiquated security, insufficient fiscal and regulatory penalties, and the fingertips of tantalized insatiable adversaries."

By now, we also realized that the risk and impact of compromise of EHRs is usually and mostly shifted to us (the patients). But what most still don't recognize is that if our EHRs get compromised just once, and sold repeatedly all over the Dark Web, we'll likely have problems for the rest of our lives. Information that is contained in those records can be used for many different types of fraud and attacks, such as medical identity theft, submission of false claims, acquisition of controlled and prescription substances, and obtainment of medical devices. But the list of dangers doesn't stop there – criminals can also create fake identities, perpetrate tax fraud, access government benefits, or try to extort patients. Another problem is that there are still no legal protections for medical identity theft victims.

"Stopping the damage, disputing the charges, and correcting the record can consume all of a victim's time and energy," the researchers noted, adding that "even if the victim learns of the compromise before the information is exploited, remediation can still cost over $1,500 in fees and consume their free time for up to five years."

"Due to the longevity of the record, adversaries may continue to exchange and exploit the compromised information for the rest of the victim's life. For some, such as children, this can drastically hinder their future financial stability and limit the potential lives that they could lead," the researchers concluded.

Chrome will start labeling some HTTP sites as non-secure

Slowly but relentlessly, Google is pushing website owners to deploy HTTPS – or get left behind.

The latest announced push is scheduled for January 2017, when Chrome 56 is set to be released and will start showing in the address bar a warning that labels sites that transmit passwords or credit cards over HTTP as non-secure.

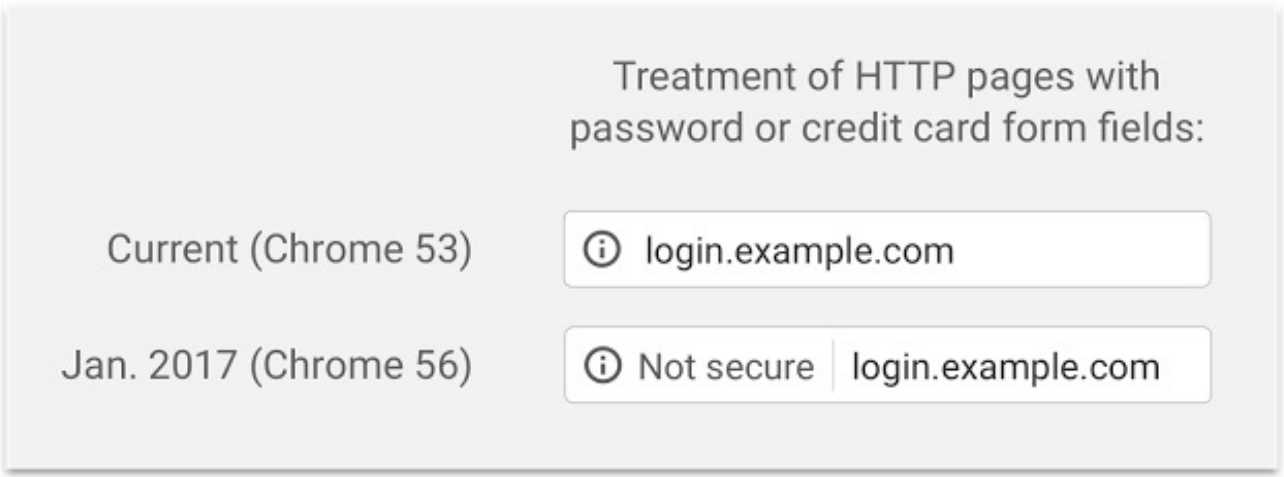
In due time, all HTTP pages will be labeled by Chrome as non-secure, and ultimately, the HTTP security indicator will turn red, and sport the same "Danger!" triangle with which sites with broken HTTPS are currently marked.

Google is in the perfect position to spearhead the campaign aimed at pushing the collective Internet towards the default use of HTTPS. Changes in Chrome are one way to do it.

Previously employed tactics include prioritising websites using HTTPS in Google Search rankings and adding a new section to the company's Transparency Report that allows users to keep an eye on Google's use of HTTPS, and HTTPS use of the top 100 non-Google sites on the Internet.

"A substantial portion of web traffic has transitioned to HTTPS so far, and HTTPS usage is consistently increasing," noted Emily Schechter, of the Chrome Security Team.

"We recently hit a milestone with more than half of Chrome desktop page loads now served over HTTPS. In addition, since the time we released our HTTPS report in February, 12 more of the top 100 websites have changed their serving default from HTTP to HTTPS."



The hidden cost of the insider threat

Organizations are spending an average of $4.3 million annually to mitigate, address, and resolve insider-related incidents – with that spend surpassing $17 million annually in the most significant cases, according to the Ponemon Institute.

While the report notes that user credential theft and malicious or criminal activity carried a more substantial cost-per-incident, the frequency and volume of insider incidents caused by employee and contractor negligence recorded the highest annual cost, averaging nearly $2.3 million.

In line with expectations, legacy solutions – such as data loss prevention (DLP), user awareness and training, and network intelligence – ranked among the most frequently deployed tools (at 46 percent, 43 percent, and 35 percent respectively). Yet, despite being the most pervasive, the incremental cost savings driven by these legacy technologies were among the lowest recorded, with network intelligence and user training yielding $0.3 million.

Top trends in security testing and vulnerability management

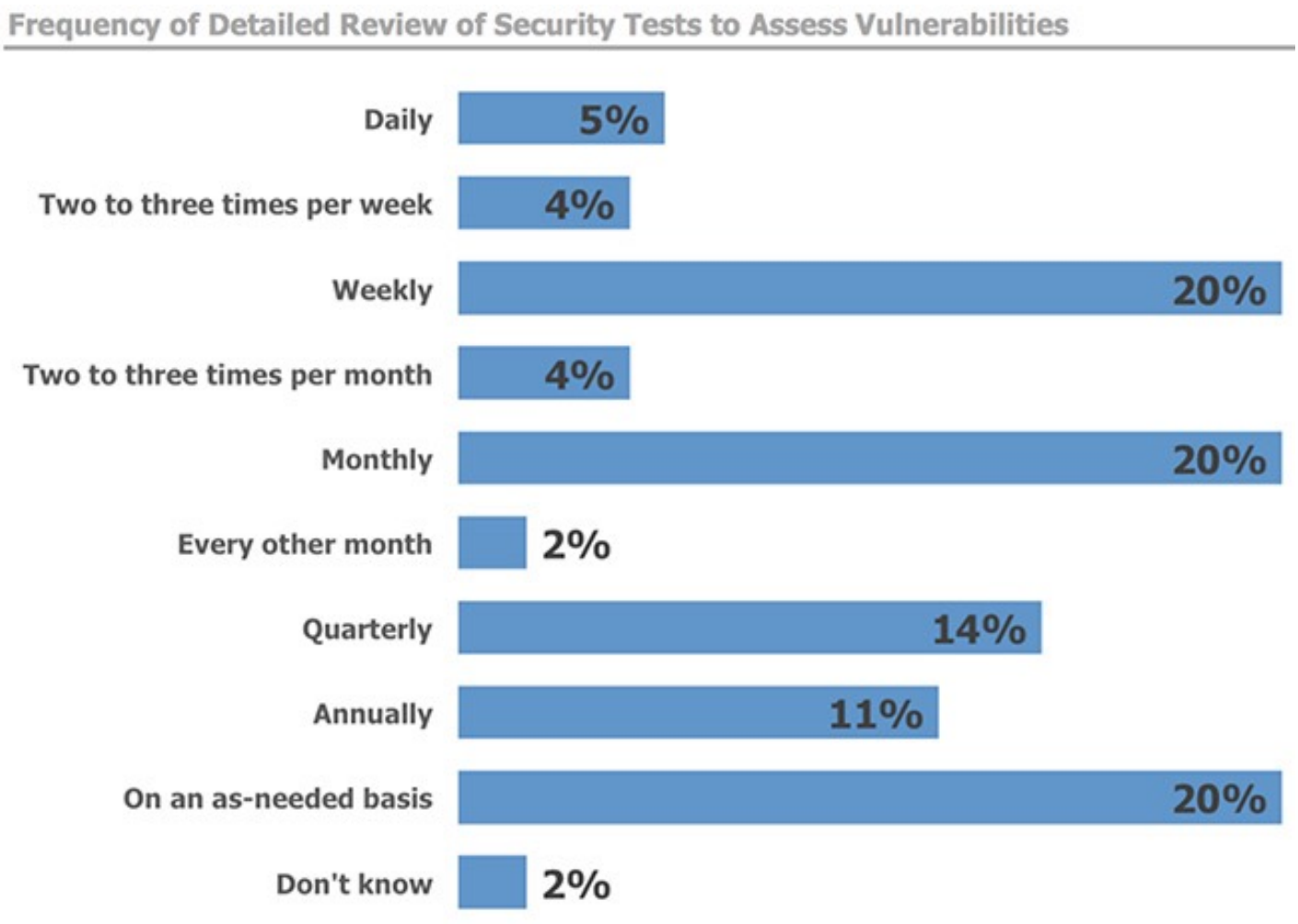
Many businesses fail to conduct frequent security testing despite believing that it's critically important to securing their systems and data. One in five of businesses surveyed admitted they don't do any security testing, despite the fact that 95 percent of survey respondents reported encountering one of the dozen common security issues associated with security vulnerabilities.

One in five organizations has not performed security testing of any kind during the past six months. Among those that do conduct security testing, 66 percent do so only monthly or less frequently, and most do not perform regular security testing after every infrastructure change. Most organizations conduct security testing using a combination of in-house resources and third-party testing services, although two in five organizations manage security testing only in-house.

Despite the fact that many organizations do not conduct security testing, two-thirds believe that security testing is a valuable best practice.

Both security testing and reviews of these tests are not commonplace: only 5 percent perform detailed reviews of security testing to assess vulnerabilities on a daily basis and only 24 percent do so weekly or multiple times during the week. Meanwhile, 25 percent of the organizations surveyed perform these reviews only quarterly or annually, and 20 percent do so only when they perceive the need, creating a situation where businesses are simply guessing when to test their systems.

Among the leading security testing challenges discovered in the survey, the most commonly cited are insufficient staffing, insufficient time with which to perform the security tests, and insufficient skills to support regular testing.



Source: Osterman Research, Inc.

Hacking is the new espionage

Eric O'Neill

Today's headline-making hacks are the natural evolution of traditional espionage.

In the past, spies leaned heavily on recruiting insiders or moles to steal secrets. Historically, spies would remove information from office buildings (frequently in hard copy and later on floppy disk) and leave the information in "dead drops," which served as prearranged clandestine sites that could later be "serviced" by foreign intelligence.

Today, the way we store and share secrets and critical information leaves the "keys to the kingdom" vulnerable to outside attack. While recruiting a trusted insider remains the most effective way to breach a firewall, spies have changed their tactics to address the changes in operational security in the digital world.

As cyber security has evolved so have spies. Today's attackers are criminals and spies who have pivoted to survive in a new age of information theft. They are devious, sophisticated, technologically proficient, often well funded, and leverage traditional espionage techniques to perpetrate cyber penetrations.

An example of modern-day espionage via hacking is spear phishing conducted via social media and email. Email not only serves as our chief communication methodology, but also to sign contracts and distribute records. Everything we do now leaves a trail, including all we do on email and social media.

The best spear phishing attacks leverage social media and involve reconnaissance research about the target. To conduct the Anthem attack, the attackers combed through LinkedIn data on Anthem employees to identify system administrators and hit them with specially crafted emails.

Social media is one of the new playgrounds for spies. Everything an attacker needs to convince a target to click on a link in email can often be mined from personal social

SOCIAL MEDIA IS ONE OF THE NEW PLAYGROUNDS FOR SPIES

media accounts. I constantly tell my audiences at cyber-security keynotes not to click on links in emails or open attachments, even if you believe the email came from your sister, is about the party you both attended the week prior, and uses expressions that only your sister would use. These are all things a spy can learn by perusing your Facebook or Instagram account for a few minutes.

Reactive vs active response

Too often, law enforcement and security professionals react to crime instead of actively stopping it before it happens. Also too often, they won't know a crime has been committed until way too late.

An example of this is the hack of the Democratic National Committee (DNC). US officials have stated that the attack persisted for roughly a year. The hacks occurred despite a warning from the FBI that the DNC may be a target after the State Department and White House were compromised.

According to the DNC, after the warning, security policies were changed. It appears that may have been too little, too late. Attackers were either already in the system and remained undetected for the year-long breach, or changed their own approach to avoid detection. Despite the warning, attackers continues to be one step ahead of security.

Another example of this cat-and-mouse game came from The Office of Personnel Management (OPM), which was breached in March of 2014. The breach went unnoticed by the OPM until April 2015. It has been described by federal officials as one of the largest breaches of government data in United States' history. Attackers may have compromised some 21.5 million records, including biometric data and documents related to security background investigations.

TOO OFTEN, LAW ENFORCEMENT AND SECURITY PROFESSIONALS REACT TO CRIME INSTEAD OF ACTIVELY STOPPING IT

The breach occurred despite the Government Accountability Office warning that the OPM (among other agencies) was vulnerable to attack and should immediately correct weaknesses and fully implement security programs.

To defeat cyber espionage, cybersecurity professionals must disrupt the "attack - remediate - attack" cycle, by defending the endpoint, controlling applications, sharing knowledge about possible intrusions, and actively hunting for threats.

This disruption requires cybersecurity professionals to take an active role in defending against a predator by becoming a spy hunter.

An example of the "attack – remediate – attack" cycle in physical security is best explained using barriers. In the past, terrorists frequently loaded explosives into trucks and smashed them into government buildings.

ORGANIZATIONS MUST COLLABORATE IN REAL TIME TO SHARE THREAT INFORMATION AND THE FORENSICS BEHIND BREACHES

The first World Trade Center attack in 1993 involved a van loaded with explosives parked in the underground parking beside what the terrorists thought was the central support column.

In response to these vehicle attacks, security and law enforcement remediated by building barriers (everything from jersey walls to massive planters with steel cores) to create spacing around government buildings that prevent vehicle attacks.

As these defenses went up and stopped one problem, the terrorists actively explored new attack vectors. Unable to drive trucks into buildings, they turned to airplanes.

If law enforcement and security become more active in hunting threats and brainstorming possible attack vectors before spies launch attacks, cyber espionage will become more expensive, time consuming and burdensome.

The goal of cybersecurity should be to layer defenses in such a way that the cost of attacking a protected organization is so high that the criminals will turn to other targets.

Additionally, the FBI, CIA, NSA, military intelligence assets, and friendly foreign intelligence units must continue to work together to collaborate and share information to prevent the most deadly and damaging terrorist attacks and to catch the most sophisticated spies.

Often, these highly sophisticated spies are state actors (as in the case of China's PLA unit 61398) or state-sponsored actors (such as the DNC hackers believed to be working for the Russian government). Money provides such attackers freedom to carefully research and probe targets and then leverage intelligence and the best equipment and resources possible. This creates a very uneven playing field when these attackers hunt small companies and individuals that do not have the benefit of the FBI and CIA to defend them.

Companies and organizations must collaborate in real time to share threat information and the forensics behind breaches in order to defend themselves against foreign intelligence units (spies). This requires a certain level of sharing of cyber information between competitors.

In the wake of the recently reported hacks - DNC, DCCC, Equation Group - it's time for the US to start treating cybersecurity as national security. Our democracy is at risk. In fact, the upcoming presidential election could be at risk, too.

Addressing the inefficiencies of our cyber infrastructure should be a top issue in this year's election cycle. The fact that it is has been, at best, a footnote in both candidates' platforms is an indication of where our national cybersecurity ranks on the list of priorities.

Eric O'Neill is the National Security Strategist for Carbon Black (www.carbonblack.com).

New hyper-evasive threats are killing sandboxing as we know it

Sigurdur Stefnisson

Like military generals, IT security professionals frequently fight the last war using weaponry and tactics that worked in the past, while the enemy has studied our countermeasures and is already applying new methods.

Today we face a new generation of malware which we might term “hyper-evasive” – threats that have never been seen before, in volumes never seen before, and which have been designed to evade traditional malware defenses, and specifically, current sandboxing technology. These threats require a rethinking of our battlefield strategy.

The evolution of threats

To understand today’s threat landscape, we should consider the evolutionary history of cyber threats, while keeping in mind that each new class of threats emerged from the criminals’ detailed understanding of the limitations of then-current protection technologies. While a rough chronological retelling is possible, my purpose here is to give a quick sense of classification, and emphasize that techniques are frequently cumulative – nothing ever really “goes away.” We might consider the following “tiers” of malware sophistication:

Tier 1: Basic malware

These compromise a computer in order to gain access to its resources and – on occasion – its data. Attacks of this type are slow-moving and frequently noisy and obvious, and can be blocked by analyzing a virus to capture a hash fingerprint or signature, and then using this hash to identify and block subsequent copies of the virus.

Tier 2: Polymorphic malware

Although they are often basic viruses under the hood, polymorphic viruses first emerged in the early 1990s: malicious code that mutates and changes its appearance each time it infects a new object in order to avoid pattern recognition by antivirus software.

The emergence of polymorphic malware triggered the arrival of behavioral heuristics as a countering technology, whereby the behavior of the code execution during an emulation is observed. The development of application sandboxing in the 1990s was a key response to polymorphic malware.

The advent of server-side polymorphism has taken malware to the next level, with back-end web services hiding the mutation engine where defenders cannot inspect it. Sophisticated algorithms ensure that each time a download occurs from a URL you receive a different file, and attack methods frequently involve encryption, droppers and packers.

Tier 3: Hyper-evasive malware

Cyren has noted an emerging trend of threats incorporating many known evasion techniques within a single piece of malware. Attackers have evolved their techniques to the point where malware rarely contains obviously suspicious code and originates from "unknown" sources or from code lodged in compromised, trusted sites. As the use of sandboxing for malware defenses has increased, malware that is "sandbox aware" has become more prevalent.

Usually assumed to be the purview of large enterprises, a recent study commissioned by Cyren and conducted by Osterman Research (July 2016) found that over 50 percent of small and mid-sized companies (100 to 3,000 employees) have also deployed an appliance-based sandboxing capability.

But such "hyper-evasive" threats are increasingly difficult for traditional, appliance-based sandboxing to detect, as the malware coders use sophisticated evasive tactics to exploit limitations in the architecture of appliance-based sandboxing.

Limitations of traditional application sandboxing

Traditional application sandboxing has become a critical last layer for corporate information security to attempt to stop infiltration. It pushes suspicious objects to a simulated end-user computing environment running on an appliance in a corporate data center.

While the overall volume and sophistication of unknown objects was relatively low, and turnaround time was consequently fast, this approach was deemed sufficient. However, the broad deployment and very success of appliance-based sandboxes has led to not-surprising innovation by criminal enterprises, as per the usual historical pattern.

It is worth restating that the variety and depth of testing that is possible within first-generation sandboxes is limited. Among the realities of traditional sandboxing that are being exploited today are:

1. The fixed amount of physical resources (i.e. memory and processing power) available in a sandbox appliance, which limits the scalability of the solution in terms of total analysis object load and depth of analysis performed.
2. The reliance on virtualized environments, the presence of which can be detected by malware.
3. The lack of diversity in the scope and origination of the tests employed, with the variety and nature of tests limited to those devised by the specific sandbox vendor.
4. The fact that any specific sandbox is best at one kind of analysis, e.g. OS or registry or network behavior analysis.

This last element is the most critical limitation of all, as it enables malware developers to optimize analysis detection techniques for each sandbox platform, knowing that once they have found a "tell" for the particular sandbox being used, their evasive techniques will get them past what is effectively the organization's last line of defense. No method is provided by traditional sandboxing solutions to harness together sandboxes of different types (or from different vendors) in a collaborative analysis model, to enable a broader and deeper scope of testing with a pooling of analysis results.

How hyper-evasive threats evade detection

Sandboxing solutions deploy two types of analysis:

- Static analysis is performed by the system without executing the suspected code. Examples of static analysis techniques include file fingerprinting, extraction of

- hard-coded strings, file format metadata, emulation, packer detection, and disassembly.
- Dynamic analysis is performed by the system while the suspected code is executed inside a protected (sandbox) environment. Examples of dynamic analysis techniques include analyzing the difference between defined points, and observing run-time behavior.

To combat the growing use of first-generation sandboxes, cybercriminals have developed evasive techniques for use against both types of analysis.

Some of the techniques are sophisticated, while others perform simplistic tests to determine if the malware is in a real or simulated (sandbox) environment.

TO COMBAT THE GROWING USE OF FIRST-GENERATION SANDBOXES, CYBERCRIMINALS HAVE DEVELOPED EVASIVE TECHNIQUES FOR USE AGAINST BOTH TYPES OF ANALYSIS

Common techniques for evading sandbox analysis include:

- Detecting the existence of a virtual environment
- Delayed activation – attempting to "outwait" the sandbox
- Awaiting human interaction like mouse movements that could not result from a simulation
- Making payload execution conditional.

As an example of this last approach, we are seeing recent ransomware downloaders that have added the requirement of an additional parameter for the execution of the downloaded ransomware code. A sandbox may have the download file itself, but it does not have the full script – so it would not detonate in the sandbox because it is missing one component (a parameter).

Consider the impressive list of functions identified by Cyren researchers within a single variant of Cerber ransomware, which uses multiple methods to check for the presence of, and therefore hide from, a sandboxing environment.

Virtual machine check functions:

- Parallels
- QEMU
- Oracle VirtualBox
- VMWare
- an unknown VM.

Debugger process check functions:

- CommView Network Monitor
- WinDump
- WireShark
- DumPCAP
- OllyDbg
- IDA Disassembler
- SysAnalyzer
- SniffHit
- SckTool
- Proc Analyzer
- HookExplorer
- MultiPot.

Sandbox check functions:

- Loaded modules check against
  - sbiedll.dll - Sandboxie
  - dir_watch.dll, api_log.dll - Sunbelt Sandbox
- Volume serial number checks against
  - ThreatExpert
  - Malwr
- Mutex name checks against
  - Deep Freeze - Frz_State
- Other file path checks on modules used in sandbox setups
  - C:\popupkiller.exe
  - C:\stimulator.exe
  - C:\TOOLS\execute.exe
- String checks from memory
  - test_item.exe
  - \sand-box\
  - \cwsandbox\
  - \sandbox\

The inclusion of this variety of functions shows that malware writers are hard at work researching sandbox and debugging technologies that the security industry is most likely to use in solutions, and proves that they can simply embed more anti-sandbox/debugger/VM modules in their malware as they see fit, significantly increasing the evasiveness of the threats.

Conclusion

The appropriate response to the advent of hyper-evasive malware, which can evade any given sandbox and was designed to exploit the relatively limited processing power of appliance-based solutions, is to exponentially improve the analytical capacity of the sandboxing systems. This can be done by subjecting malware to multiple and varied sandboxing environments while applying increasingly sophisticated analysis, something now possible via the elastic processing scale and Big Data analytical capabilities of cloud computing.

The best countermeasure is to automate the strengths of human analysts – in particular their capacity for complex decision-making and even “hunches” – through a cloud-based processing model.

Sigurdur Stefnisson is the Vice President of Threat Research at CYREN (www.cyren.com).

How to choose a perfect data control solution for your enterprise

Zeljka Zorz

Not long ago, people used to come to work and work off of a desktop computer, tied to the network. Today, they work on their mobile devices, physically untethered to it.

In fact, the majority of the work and email is done on mobile devices, and this changed how people interact with data and how we keep it safe.

This shift is why it's important for businesses to maintain a certain level of visibility when it comes to data, and have the ability to use tools like Dynamic Data Protection (DDP) to ensure that if policies need to be adjusted for specific users, IT admins can do so in real-time.

"As information travels, this introduces new ways to access data and collaborate using tools like Dropbox and other productivity tools, so security must also evolve and change to keep pace," says Prakash Linga, CTO of data security company Vera.

"On top of that, it's not longer sufficient to rely on perimeter defenses when it comes to information security. You have to collapse the data control and policy enforcement down to the data. Any effective and usable data security solution will encompass the best of both worlds: it will secure information with granular and flexible policies, and enable employees to continue their workflow seamlessly, while still giving companies optimal security."

A perfect enterprise data security solution

Data control and visibility is a huge problem that large and small companies need to be mindful of.

A good data security solution is one that works as you want it to but it's also equally important that it's easy to use by your employees, management, and partners. The best technical solution will not mean much if they don't want to use it because it gets in the way of their work.

"In an ideal world, you want your users to maintain productivity, while still giving IT the confidence they're doing so in a secure way," Linga points out.

"Organizations spend too much time and money trying to focus on one aspect of the problem by adding more defenses, rather than focusing on the primary reason employees aren't using the security tools already in place."

The ideal data control solution should also offer robust data control tools with a user-friendly backend, to make life easier for IT and security teams. Managing policies and data at scale is a challenge and, according to Linga, this is one of the reasons why Data Loss Prevention (DLP) hasn't taken off as expected.

A great data control system will be one that fits well within a specific and complex enterprise ecosystem – across different companies, meshing well with existing collaboration and productivity tools, and covering every data workflow.

Finally, the solution has to be always on, so that organizations can be confident that their most critical business information is secure whether it's at rest, behind a firewall, or has been moved outside their network.

"For a lot of security savvy people, it's all about having strong security controls. What we've learned from conversations with customers, prospects, and industry research is the biggest problem is keeping honest users honest," says Linga.

"I'm referring to people who inadvertently share information they shouldn't. For example, an executive accidentally fat-fingers a confidential financial document or earnings report to the wrong person."

A great data control system will be one that fits well within a specific and complex enterprise ecosystem

Data control and the Internet of Things

"The nature of data is changing rapidly. Today, it's mostly collaboration and exchange between two people, but tomorrow it's with IoT and other devices and approaches," says Linga.

We know that makers of IoT devices and the software that makes them "smart" regularly disregard security, and that IoT is slowly infiltrating both homes and offices.

"Small quantities of data is often shared between devices and, if you look at the information as a snapshot in time, it might not be sensitive or something you care about at that moment. However, over an extended period of time, you may start to see patterns, and it becoming more relevant from an enterprise and consumer standpoint," he adds.

Enterprises will have to find a way to keep on top of things, and be ready to pivot as fast as needed to tackle the known and yet unknown challenges of data security in the age of IoT.

"Both security and privacy needs to evolve for the new workflow around data and collaboration," he concludes.

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine & Help Net Security (www.helpnetsecurity.com).

At Armor, we prevent data breaches. By combining analysis from our battle-tested security experts, and data from more than 50 global threat streams, we protect your most sensitive data by identifying and blocking the latest threats before they are public - helping you take back the element of surprise.

NOW IT'S YOUR TURN. ▸▸▸
Get the latest Armor Threat Intelligence Briefing

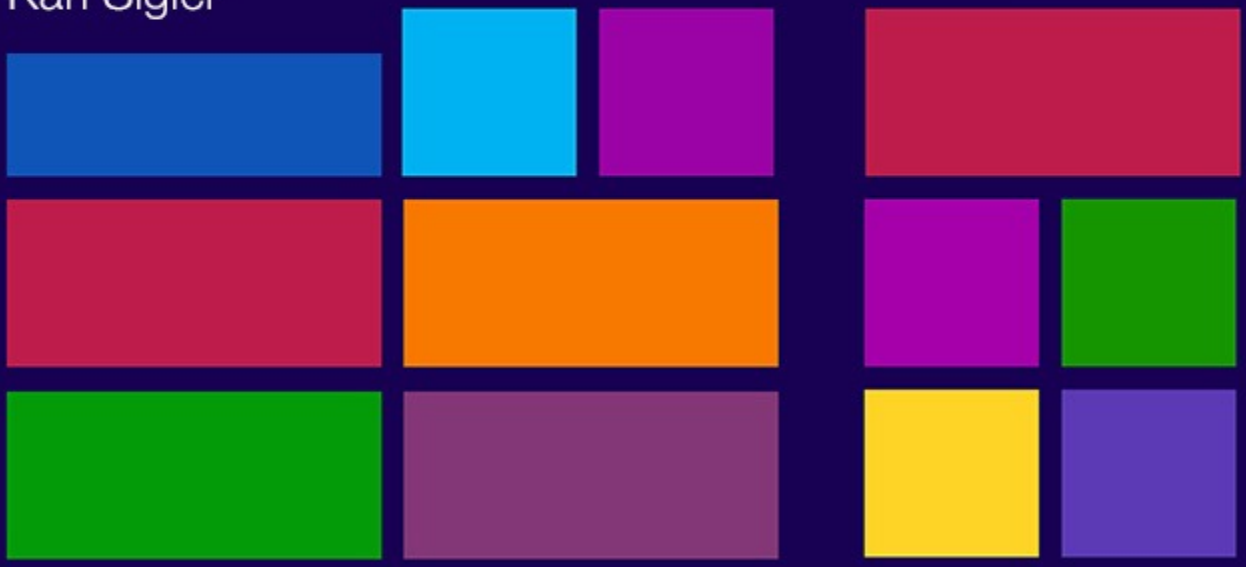
SIGN UP NOW

ARMOR™
BETWEEN YOU AND THE THREAT

armor.com | 1 877 262 3473

What can Microsoft Patch Tuesday tell us about security trends in 2016?

Karl Sigler



Patch Tuesday (or Update Tuesday, as Microsoft preferred to call it) used to occur on the second Tuesday of each month. This was the day when Microsoft released patches for its various products and was often the bane of system admins and hackers alike.

System admins were forced to patch all of the systems they are responsible for, while criminals sometimes found that the exploits they had used up to that point no longer worked.

Microsoft has now done away with Patch Tuesday in the form that it came in for years, but the first eight Patch Tuesdays that came and went since the beginning of the year can tell us something about security trends in 2016.

By the numbers

First let's take a look at the raw numbers. From January through August 2016 Microsoft released 101 security bulletins. Each bulletin contains patches for a specific product like Microsoft Office or Internet Explorer.

Of these bulletins 44 were rated as Critical and the remaining 57 were rated as Important.

Bulletins rated as Critical typically cover the most severe type of vulnerability, Remote Code Execution (RCE). An RCE vulnerability allows an attacker to exploit it from anywhere on the network or Internet without any special privileges.

Bulletins rated as Important still address serious vulnerabilities, but exploitation of those typically requires certain access or can result in limited damage. These are typically vulnerabilities that allow Privilege Elevation (making a regular account into an administrator one) or Denial of Service (temporarily taking down a service).

Each bulletin typically contains multiple patches for a single product. For instance, August's bulletin for MS Office provided patches for five unique vulnerabilities. For identification purposes, each vulnerability is issued a unique number according to the Common Vulnerabilities and Exposures (CVE) program.

The aforementioned 101 bulletins addressed 266 unique vulnerabilities (or CVEs).

The most common patches

The most commonly affected products were Internet Explorer and the newer Windows Edge web browser. These two products have showed up with a bulletin rated Critical every month in 2016 (and for many, many months before 2016). This doesn't necessarily mean that these products are naturally insecure.

These products are likely the most used pieces of software Microsoft supports. They are also constantly exposed to threats. Their whole job is to process untrusted content from the public Internet. Looking at it from this perspective, it's no surprise that vulnerabilities in these products are exposed first.

Overall, 72 unique CVEs were patched in Internet Explorer and 57 were patched in Windows Edge. Keep in mind that many of those vulnerabilities are shared between both products.

With the idea that vulnerabilities tend to be found in more popular software first, it's probably not a surprise that the third most commonly affected product is the Microsoft Office suite. With a total of 39 CVEs since January, the Office suite has made a showing with either a Critical or Important rated bulletin every month this year. This doesn't include the dozens of vulnerabilities that affect the Office suite indirectly: critical vulnerabilities in the MS XML Core, OLE, Java/VBScripting engines, and even maliciously created fonts in the Microsoft Graphics Component can all be exploited by opening the wrong Office document.

THE MOST COMMONLY AFFECTED PRODUCTS WERE INTERNET EXPLORER AND THE NEWER WINDOWS EDGE WEB BROWSER

Zero-day vulnerabilities

The most critical vulnerabilities will always be the zero-day vulnerabilities. A zero-day vulnerability is one that is discovered by criminals before the vendor knows of it. This gives the criminals a chance to develop an exploit for the vulnerability and successfully target victims as no patch is available or is still pending.

In the first eight months of this year two zero-day vulnerabilities affecting Microsoft products have been revealed. I'll stick to Microsoft products only and ignore the multiple Adobe Flash zero-day vulnerabilities even though the Flash engine is embedded in both Internet Explorer and the Edge browser.

The first zero-day was CVE-2016-0167, a privilege elevation vulnerability in Windows patched in bulletin MS16-039 in April. It was revealed to the public by FireEye reserchers, and prior to that exploited via a spam campaign that contained a malicious Microsoft Word document. When the document was opened and the vulnerability exploited, the document would automatically execute malware. The criminal group behind the campaign used the zero-day to deliver malware to financial institutions and grab payment card track data.

The second zero day was CVE-2016-0189, which affected Internet Explorer and was patched in bulletin MS16-051 in May. The attackers who exploited it first sent out malicious links via a spear-phishing campaign to users in South Korea.

South Korean vendors were forced by law in 1999 to adopt ActiveX controls that use the country's SEED encryption cipher for e-commerce transactions. Since Internet Explorer is the only browser that still supports Active X, the country is very dependent on the browser, making them ripe targets for this type of zero-day. This zero day was detailed by Symantec researchers.

Exploits on the dark web

Also this year, a criminal offered information about a zero-day flaw for sale on an underground market for Russian-speaking cyber criminals. We've always known that zero-days have been sold in the shadows, but in this business you usually need to "know people who know people" in order to buy or sell this kind of commodity. This type of business transaction is conducted in a private manner, meaning either through direct contact between a potential buyer and the seller, or through a middleman.

We've also seen zero-days exploited by the Angler Exploit Kit. Last year Angler introduced four zero-day exploits. This, and a constantly refreshed offering of new exploits, allowed Angler to become to the most popular exploit kit on the market in 2015, representing 40% of all exploit kit-related incidents.

The underground crime forum where the aforementioned zero-day was offered for sale serves as a collaboration platform where criminals can hire malware coders, lease an exploit kit, buy web shells for compromised websites, or even rent a whole botnet for different purposes. However, finding a zero-day listed between these fairly common offerings is definitely an anomaly.

The zero-day in question was claimed to be a Local Privilege Elevation (LPE) vulnerability in Windows and came with videos showing the exploit executing. The auction started at $95,000 in Bitcoins but the seller quickly dropped the price down to $90,000, and finally to $85,000. The auction was eventually closed and evidence of it deleted, but we'll probabaly never known whether this was due to the seller finding a buyer or due to the vulnerability getting patched before the sale was made.

The fact that the first zero-day of the year and the zero-day that was auctioned off both allowed for privilege elevation is telling. In the first eight months of this year, Microsoft has patched 49 privilege elevation vulnerabilities in various components.

Although the exploit of such a flaw can't provide everything an attacker needs, it is still a very much needed puzzle piece in the overall infection process.

For instance, an LPE exploit paired with a client-side RCE exploit can allow an attacker to escape an application that implements sandbox protection like Google Chrome or Adobe Reader. Moreover, an LPE exploit provides the means for the attacker to persist on an infected machine, which is a crucial need for APTs (Advanced Persistent Threats). In general terms, an LPE exploit can be leveraged in almost any kind of attack scenario.

Was the threat of Badlock overhyped?

The biggest "disappointment" this year was Badlock. The existence of this flaw was announced with much fanfare in March. The announcement came with a dedicated domain and webpage, a cool icon and a memorable code name, but no details about the nature of the bug. For that, professionals had to wait until the April Patch Tuesday. That gave the security community three weeks to get worked up about whether this vulnerability was going to be big or a bust. It ended up being the latter.

Badlock ended up being helpful in a man in the middle (MITM) attack scenario, meaning that an attacker needs to be listening on the exact same network as the client or server in order to perform the attack. This means that any attack requires a pre-authenticated session. It only affects open, authenticated sessions using SMB to authenticate a system or to manage users or policies on a remote.

In other words, any effective attack requires the attacker to be in the exact right place at the exact right time.

As silly as they may seem to some in the industry, these so-called "celebrity vulnerabilities" can be very useful. It can be easier to communicate the importance of a vulnerability with a name rather than one with just a CVE designation. A prime example of this is Heartbleed. Heartbleed was a critical vulnerability and the name, website and icon helped draw attention to it. It could be argued that more servers were patched in a short time because of the high profile brought on by the name.

OVERALL, 266 VULNERABILITIES OVER AN EIGHT-MONTH PERIOD SOUNDS LIKE A LOT OF VULNERABILITIES, BUT NOT ALL VULNERABILITIES GET EXPLOITED

Since Heartbleed, however, the bulk of these celebrity vulnerabilities have been more or less non-issues. I'm not saying that these aren't vulnerabilities that could cause a breach or data loss. However, most of them stole the spotlight from much more critical vulnerabilities, and that is a problem.

The other problem is that the type of build-up that occurred with Badlock often forces sysadmin teams to waste valuable resources.

These pre-releases force an "all hands on deck" situation in order to prepare for the worst-case scenario. Admin teams were preparing to patch their servers for a major Badlock vulnerability and were auditing their firewall policies for Badlock suspected access instead of making sure that their user base was set to auto-update or that their client browsers aren't using Flash anymore.

Patch preparation

Speaking of preparing for patches, it is important to have a patching policy in place that allows you to patch your most valuable and vulnerable assets as quickly as possible. This of course means knowing which assets are valuable and which are at risk in your environment. This is generally performed through ongoing network scanning to keep an up-to-date inventory and risk assessment to nail down how vulnerable those assets are.

Typically you'll want to focus on your public facing servers (webservers and email servers) first, because they are exposed to attack and tend to be the most valuable assets. You'll also want to focus on your end users, as they are constantly exposed to a wide range of threats and are gatekeepers for important internal data.

Overall, 266 vulnerabilities over an eight-month period sounds like a lot of vulnerabilities, but not all vulnerabilities get exploited. A quick check of public sources shows only 30 public exploits for them. Naturally, these are just the exploits and PoCs we know about.

More surely exist in the underground, but the problem for the criminal is how to keep those exploits unknown. The more an exploit is used the more likely it is to be discovered, and the vulnerability patched.

Patching - and patching quickly - is an important part of securing systems and networks. However, tracking released patches can provide us with helpful insights.

While many system admins and network engineers focus almost completely on vulnerabilities that might affect their servers, we have seen that client software like Internet Explorer and Microsoft Office often presents a greater risk. And while Remote Code Execution vulnerabilities are always the ones that claim the spotlight, Privilege Elevation vulnerabilities are often the ones used to complete a compromise and maintain persistence.

Karl Sigler is Threat Intelligence Manager at Trustwave (www.trustwave.com) where he is responsible for research and analysis of current vulnerabilities, malware and threat trends. Karl and his team run the email advisory service, serve as liaison with Microsoft MAPP program, and coordinate disclosures of discovered vulnerabilities.

Mirai Linux Trojan corrals IoT devices into DDoS botnets

Mirai, a newly discovered and still poorly detected piece of Linux malware, is being used to rope IoT devices into DDoS botnets.

Researchers from MalwareMustDie have recently gotten their hands on several variants of the threat, and have discovered the following things:

- It comes in the form of an ELF file (typical for executable files in Unix and Unix-like systems)
- It targets mostly routers, DVR or WebIP cameras, Linux servers, and Internet of Things devices running Busybox – the "Swiss Army knife of Embedded Linux."
- The attackers first gain shell access to the target devices by taking advantage of the fact that most have a default password set for the SSH or telnet account. Then they load the malware.
- The malware sets up several delayed processes and then deletes malicious files that might alert users to its existence. It then starts opening ports and establishes contact with its botmasters, and scans for other accessible devices to infect. For other actions, it awaits further instructions.

They consider Mirai to be the direct descendant of an older Trojan dubbed Gafgyt (aka BASHLITE, aka Torlus), which is one of the main contributors to the rise of DDoS-for-hire services.

In order to protect their devices from this threat, administrators are advised to close up their telnet service, to block the TCP/48101 port (if unused), and to make sure their Busybox execution can be run only on specific user.

US 911 emergency system can be crippled by a mobile botnet

What would it take for attackers to significantly disrupt the 911 emergency system across the US? According to researchers from Ben-Gurion Univerisity of the Negev's Cyber-Security Research Center, as little as 200,000 compromised mobile phones located throughout the country.

The phones, made to repeatedly place calls to the 911 service, would effect a denial-of-service attack that would made one third (33%) of legitimate callers give up on reaching it.

If the number of those phones is 800,000, over two thirds (67%) would do the same.

Naturally, the researchers – Mordechai Guri, Yisroel Mirsky, and Yuval Elovici – haven't performed such an attack on the actual, nationwide system. Instead, they have created a simulated cellular network based on North Carolina's 911 network (as information about it is widely available) and attacked it instead.

According to their findings, the 911 system in North Carolina could be partially overwhelmed by mere 6,000 infected devices.

The problem, the researchers say, rests in the fact that current FCC regulations require that wireless carriers must immediately route all emergency calls to local public safety answering points, regardless of the mobile phone's available identifiers (like IMSI and IMEI, which tell if the caller is a subscriber to their service and identify the mobile equipment, respectively).

"A rootkit placed within the baseband firmware of a mobile phone can mask and randomize all cellular identifiers, causing the device to have no genuine identification within the cellular network. Such anonymized phones can issue repeated emergency calls that cannot be blocked by the network or the emergency call centers, technically or legally," they pointed out.

There are several countermeasures that can mitigate such an attack, including implementing "call firewalls" on mobile devices, and public safety answering points implementing "priority queues" that would give precedence to callers with more reliable identifiers.

Attack prevention options include the disallowing of 911 calls from NSI devices, and trusted device identification.

CodexGigas: Malware profiling search engine

CodexGigas is a free malware profiling search engine powered by Deloitte Argentina, which allows malware analysts to explore malware internals and perform searches over a large number of file characteristics.

Instead of relying of file-level hashes, users can compute hashes over features such as imported functions, strings, constants, file segments, code regions, or everything that is defined in the file type specification. This provides more than 142 possible searchable patterns that can be combined.

When it comes to development challenges, the authors tried to gather a massive amount of malware in order to test the software. "We currently have about 25 million samples, that's 15 TB of malware. Turns out that amount of data is not as easy to manage as we thought. When processing data, for every extra millisecond it takes to process a sample on average, it takes seven hours to process the whole database," Luciano Martins, CodexGigas developer, told (IN)SECURE Magazine.

You can check for updates on the CodexGigas Twitter profile (@CodexGigasSys), and the download is available here: github.com/codexgigassys.

Five ways to respond to the ransomware threat

While organizations wrestle with the ever-pressing issue of whether to pay or not to pay if they're victimized, Logicalis US suggests CXOs focus first on how to protect, thwart and recover from a potential attack.

1. Create a modern defense
It is critically important to plan for the possibility of an attack by developing comprehensive visibility and access to extensive details on how the malware entered the organization's environment in the first place.

2. Take an architectural approach
In some limited situations, point solutions can be effective, but not with ransomware. The most effective way to address the ransomware threat and other pervasive cyberattacks is to take a holistic architectural approach to security that encompasses the entire network including its systems and endpoints as well as the organization's cloud and mobile strategies.

3. Prevent the spread of malware
If an attacker's malware does enter the network, it has the ability to spread like a fast-moving cold among passengers on an airplane. The key at this stage is to compartmentalize data using network micro-segmentation strategies that make it more difficult for malware to spread laterally within the environment.

4. Plan your recovery
The unfortunate truth is, despite the security industry's best efforts, no organization is entirely immune to attack. Therefore, it's critical to examine how the organization will recover if it is breached.

First, be sure you're backing up. Second, test, test and re-test the backup and restore process; a backup is only valuable if the data can actually be restored when it's needed. It's also important to ensure that the restore can be done at the system level since file-based recovery may not be enough.

Consider, too, how much redundancy is required; if the organization is hit, do you have an uncorrupted source from which you can immediately recover?

5. Create a pay or no-pay policy
Do you have an uncompromised data backup from which you can restore? What is the cost to restore vs. pay – both monetarily and in terms of the business' ability to function in the meantime? Ultimately, the decision comes down to how business-critical the compromised data is to the organization. If you do decide to pay, In most cases, you can talk the price down, so it may make sense to consider not paying the first amount offered."

Gugi banking Trojan outsmarts Android 6 security

The Gugi Trojan's aim is to steal users' mobile banking credentials by overlaying their genuine banking apps with phishing apps and to seize credit card details by overlaying the Google Play Store app. In late 2015, Android OS version 6 was launched with new security features designed specifically to block such attacks. Among other things, apps now need the user's permission to overlay other apps, and to request approval for actions such as sending SMS and making calls the first time they want to access them.

Kaspersky Lab experts have uncovered a modification of the Gugi banking Trojan that can successfully bypass these two new features. Initial infection with the modified Trojan takes place through social engineering, usually with a spam SMS that encourages users to click on a malicious link.

Once installed on the device, the Trojan sets about getting the access rights it needs. When ready, the malware displays the following sign on the user's screen: "additional rights needed to work with graphics and windows." There is only one button: "provide."

When the user clicks on this, they are presented with a screen asking them to authorise app overlay. After receiving permission, the Trojan will block the device screen with a message asking for 'Trojan Device Administrator' rights, and then it asks for permission to send and view SMS and to make calls.

If the Gugi banking Trojan does not receive all the permissions it needs, it will completely block the infected device. If this happens, the user's only option is to reboot the device in safe mode and try to uninstall the Trojan, an activity that is made harder if the Trojan previously gained 'Trojan Device Administrator' rights.

Aside from these security workarounds and a few other features, Gugi is a typical banking Trojan: stealing financial credentials, SMS and contacts, making USSD requests and sending SMS as directed by the command server. To date, 93 percent of users attacked by the Gugi Trojan are based in Russia, but the number of victims is on the rise. In the first half of August 2016, there were ten times as many victims as in April 2016.

There's a reason why so much friction exists between security professionals and senior management or line of business (LOB) groups: poor communication.

For security professionals, the problem originates from two distinct issues:

1. Security doesn't effectively explain the realistic nature of the threat, both direct and indirect, in business terms.
2. Ineffective communication of the potential business impact of security measures and how they affect the end user or customer.

The second of these often leads to the biggest challenge for effective communication with the C-level and LOB managers. It can also result in delayed approval for a security project.
A clear example of this is when, immediately after a deployment, a LOB manager begins receiving calls from the field that their business applications are no longer functioning properly.

This example exposes the core issue: how security people view their jobs and the jobs of the LOB managers they support. LOB managers and their leadership see their role in the company as generating revenue and profits. Security typically sees its job as protecting company assets by defending against intrusions, whether internal or external.

At a glance, those job descriptions seem entirely appropriate. This brings us to perception. The LOB managers see security people as colleagues, a support service that is helping them do their job. Therefore, they assume that security people understand the products and services they're selling, and how the end user interacts with them. Security people, however, often focus entirely on their role as a defender.

Setting the scene for miscommunication

Let's use another example to demonstrate this communication breakdown:

A security professional informs the LOB owner that a specific security mechanism needs to be altered (upgraded, replaced or added). They will do an exhaustive job of explaining the benefits of this change from a security perspective. The LOB owner will nod and more than likely accept that the security

professional knows what he or she is talking about and accept the change as a good move. Next, they will ask about price and how long the deployment will take, generally receiving specific answers - so far, so good.

At this point, they will ask something generic, such as "Anything else I need to know?" or "What are the non-security implications of this change?" That's where things are put in place for an inevitable blow-up. Security will mention a couple of things to be aware of and might even say that there's nothing to worry about. Then, the deployment occurs and the LOB owner's phone starts blowing up.

Back to security goes the manager, only to be told that this was expected. Why didn't security inform the LOB owner of that when asked about other implications? It's not out of malice or even negligence. It's because they are thinking like a security organization (thwarting attacks) and not like a LOB owner (understanding the precise ways customers use the company's offerings).

Talking through the solution

The solution sounds a lot easier than it actually is: security professionals need to spend time with their business colleagues to learn how customers interact with the company's products or software. It's a good idea for security to go through the routine training on how the product is used, and to observe the end-user customers working with the product.

Until security has an intimate hands-on understanding of the end-user-product interactions, how can they be expected to provide the C-Level and LOB owners a comprehensive list of post-deployment functionality changes?

In theory, this could lead to a change that will make security far more indispensable to the business. This would certainly be a boon, as security is often viewed in the same less-than-enthusiastic way as insurance, legal, PR and IR departments. They are often not seen by rank-and-file employees as adding value. They are seen as protecting against potential damage, but if security does its job perfectly, nothing happens. An absence of something bad happening is hard to trumpet on a resume.

It's akin to an effective insurance policy. Companies are happiest when the insurance policy is never needed, which can make those premiums seem like wasted money.

When top-notch security professionals do their job, nothing happens. Will the CEO be tempted to devalue that security investment? If something bad happens, then the security department failed. It's a no-win scenario. But if security professionals refocus their attention on business functionality, the picture begins to change.

Let's go back to that conversation between the security and business professionals from earlier. What if that proposal detailed the ways this software would force changes in operations and suggested different processes that would benefit the end-users, while also allowing the desired security improvement? Suddenly, that security professional is an ally. The business professional will be impressed with his or her end user functionality knowledge.

Business is a team sport

This won't be easy. It's like persuading a cryptographer that they need to sit with customers to master how end users use the software. That cryptographer will ask how will that help them defend the company. The answer is: "It will turn you into an ally of your business peers, which will make our security requests get approved faster and easier."

The reality is that all employees of the company, regardless of position, are ultimately there to help the company make money and profit. That's easy to see when someone's job title is "salesperson" or "marketing manager." However, that's not the case when their job is fine-tuning firewalls or managing multi-factor authentication.

This proposed change in approach and communication will not be easy, but it's necessary.

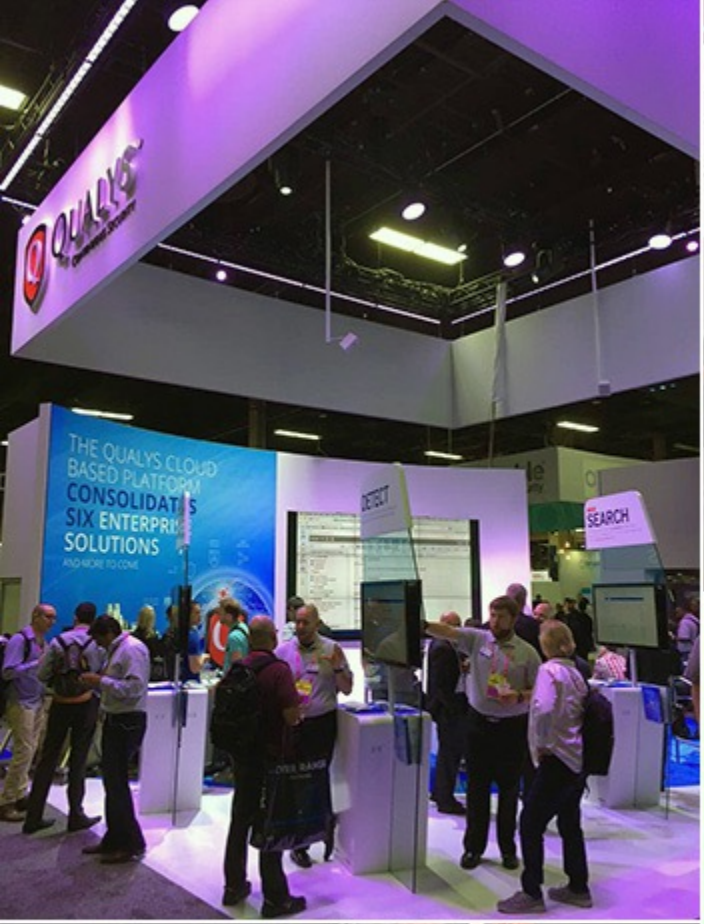
Jeff Schilling is chief of operations and security for Armor's cyber and physical security programs for the corporate environment and customer hosted capabilities (www.armor.com).

Black Hat USA 2016 welcomed more than 15,000 infosec professionals – academics, world-class researchers, and leaders in the public and private sectors.

The Black Hat Review Board, comprised of 24 of the world's foremost security experts, evaluated more submissions this year than ever before. This year's conference welcomed 175 speakers and researchers across more than 70 technical trainings and nearly 120 research-based briefings on stage.

Show highlights

- ***Keynote Dan Kaminsky***, Chief Scientist, WhiteOps, and one of seven "key shareholders" able to restore the Internet's DNS if necessary, presented "The Hidden Architecture of our Time: Why This Internet Worked, How We Could Lose It, and the Role Hackers Play" to a room of nearly 6,500 attendees.
- ***Black Hat CISO Summit*** welcomed 150 executives from top public and private organizations for an exclusive program intended to give CISOs and other infosec executives more practical insight into the latest security trends and technologies and enterprise best practices.
- ***Black Hat Arsenal*** returned for its seventh year, offering researchers and the open source community the ability to demonstrate tools they develop and use in their daily professions. This year's event featured 80 tools – a 22% increase from 2015 – the largest line-up to date.
- ***Removing Roadblocks to Diversity*** - Panel + luncheon featured some of the top women in the security field sharing their paths to success, as well as the “why” and ways to fix the dramatic underrepresentation of women and minorities in the security industry, even as the talent gap deepens.
- ***Black Hat Business Hall*** was action-packed, with nearly 270 of the industry's top companies showcasing their latest technologies and solutions. Attendees also enjoyed the bustling Career Zone, as well as the Innovation City for impressive startups.


QUALYS
THE QUALYS CLOUD BASED PLATFORM
CONSOLIDATES SIX ENTERPRISE SOLUTIONS
AND MORE TO COME
SEARCH


warebytes
Avecto
Avecto
POLARITY


LogRhythm
The Security Intelligence Company


We Prevent Data Breaches
ARMOR
What's Your Dwell Time?
THE SECURITY OUTCOME THAT MATTERS


black hat
USA 2016
IC20
IronScales
Remarkably [secure]


black hat
NETWORKING LOUNGE
Microsoft
Microsoft

Apple finally announces bug bounty program

Apple is finally going to monetarily reward security researchers for spotting and responsibly disclosing bugs in the company's products. The announcement that a bug bounty program is going to be set up by the company this September was made by Ivan Krstić, Apple's head of security engineering and architecture, at Black Hat USA 2016.

His presentation was also rather uncharacteristic for Apple, as it included the sharing of details about several of the companies data protection and security technologies.

Krstić revealed that the Apple bug bounty program will be invite-only at the beginning: only a few dozen researchers have been asked to participate.

Their names haven't been revealed, but it is known that they have worked with Apple in the past. Still, he said that the company will accept bug reports from other bug hunters, if the found flaw is deemed critical enough.

In due time, everybody will be able to participate in the program, and its scope will widen, too.

For now, we know that Apple will pay a maximum of:

- $200,000 for flaws in secure boot firmware components
- $100,000 for flaws that allow the extraction of confidential material protected by the Secure Enclave
- $50,000 for vulnerabilities that can lead to execution of arbitrary code with kernel privileges
- $25,000 for holes that allow access from a sandboxed process to user data outside of that sandbox, and
- $50,000 for vulnerabilities that can let attackers access to iCloud account data on Apple servers without authorization.

The actual reward amount will depend on the severity and exploitability of the bug. Apple will require researchers to submit a proof-of-concept exploit of the bug on the latest iOS version and hardware.

Remote Butler attack: APT groups' dream come true

Microsoft security researchers have come up with an extension of the "Evil Maid" attack that allows attackers to bypass local Windows authentication to defeat full disk encryption: "Remote Butler".

Demonstrated at Black Hat USA 2016 by researchers Tal Be'ery and Chaim Hoch, the Remote Butler attack has one crucial improvement over Evil Maid: it can be effected by attackers who do not have physical access to the target Windows computer that has, at one time, been part of a domain, i.e. enterprise virtual network, and was authenticated to it via a domain controller.

Evil Maid attacks got the name from the fact that even a hotel maid (or someone posing as one) could execute the attack while the computer is left unattended in a hotel room.

The most recent of those was demonstrated by researcher Ian Haken at Black Hat Europe 2015, when he managed to access the target user's data even when the disk of its computer was encrypted by BitLocker, Windows' full disk encryption feature.

The vulnerability that allowed this attack was definitely patched by Microsoft in February 2016, and the good news is that this patch also prevents attackers from effecting a "Remote Butler" attack.

But its unlikely that everybody applied the patch.

"While being a clever attack, the physical access requirement for [Haken's Evil Maid attack] seems to be prohibitive and would prevent it from being used on most APT campaigns. As a result, defenders might not correctly prioritize the importance of patching it," Be'ery and Hoch explained, and urged those admins who haven't already implemented it to do so as soon as possible.

Or, if that's not possible, to implement some network and system hardening and defense-in-depth policy to minimize the risk of the attack being executed.


black hat
USA 2016


KALI


outthink


BUSINESS HALL
black hat
USA 2016
LADIES

Armor Anywhere: Managed security for any cloud

As growing businesses increasingly rely on public, private and hybrid cloud platforms in addition to internal infrastructures, at Armor launched Armor Anywhere to keep sensitive data safe.

Compatible with popular cloud platforms, including AWS and Azure, Armor Anywhere secures data 24/7 while providing visibility across a multi-cloud infrastructure.

“The modern threat landscape presents sizeable challenges for companies managing sensitive data, particularly those facing strict compliance requirements,” said Chris Drake, founder and CEO, Armor.

“Armor Anywhere is a battle-tested security solution backed by threat expertise that complements our customers’ unique needs. It simplifies security, so they can focus on growth and driving revenue, not defending against sophisticated cyberattacks. We deploy an effective and scalable approach so customers can leverage our security knowledge and talent at a fraction of the cost of doing it themselves,” Drake added.

Armor Anywhere allows customers to monitor and defend operating systems with security technology and controls, backed by an elite security operations center (SOC).

Armor experts utilize the latest threat intelligence, as well as a proprietary, highly-automated agent to deliver around the clock security, patch monitoring, log and event management, malware protection, file integrity monitoring and external vulnerability scans.

The solution is designed to meet PCI and HIPAA compliance standards, and be audit-ready in defense of ePHI, PII and payment data.

With Armor Anywhere, organizations can also enjoy a shared approach to both risk and security responsibility to optimize IT spend and cloud accessibility.

Global network shares phishing attack intelligence in real-time

IRONSCALES, a multi-layered phishing mitigation solution that combines human intelligence with machine learning, launched Federation, a product that will automatically and anonymously share phishing attack intelligence with organizations worldwide.

“Instantaneous sharing of phishing attack intelligence will make it substantially easier for enterprises and organizations to consistently remain secure and in control,” said Eyal Benishti, CEO of IRONSCALES.

IRONSCALES’ employee-based intrusion prevention system is the first phishing solution with an automatic one-click mitigation response. This functionality makes it possible for IRONSCALES to expedite the time from attack to remediation from weeks to seconds, without ever needing the SOC team’s involvement.

IRONSCALES first challenges all users with a series of staged, real-world email attacks in order to evaluate their individual level of awareness. Based on an analysis of performance, a tailored phishing training campaign, using advanced simulation and gamification, is created to maximize individual awareness and responsiveness to social engineering techniques.

Once trained, vigilant employees, upon suspicion of a phishing attack, can trigger a real-time automated forensic review through the click of just one button, without requiring active SOC team participation.

Within minutes, forensics is completed, and an intrusion signature is sent directly to both endpoints, email servers and the SIEM, which then triggers an immediate enterprise-wide automatic mitigation response, such as quarantines, disabling of links and attachments, and even permanent removal of email, protecting the entire organization from the attack.

Important event information is then automatically and anonymously shared via Federation to ensure the same attack won’t hit any other company under IRONSCALES protection.

Perhaps we, as cyber security practitioners, should be thanking the perpetrators of ransomware and other high profile attacks. While years of prodding, pleading and presenting mounds of evidence to top execs earned us a toehold with the C-suite, the now ever-present headlines have shoved us all the way in.

A survey by KPMG of CEOs from top global companies found that nearly a third see cyber security as the issue having the biggest impact on their companies today. However, now that cyber security leaders have earned a place at the table, they are finding the seat isn't all that comfortable. A full half of these same CEOs report they are not fully prepared for a cyber event.

With every threat or, even worse, internal breach in the news, the pressure on security leaders grows. In response, they add more layers of technology in an attempt to plug gaps, real and imagined.

No silver bullet

It's hard to give up the dream of that cyber silver bullet. The one technology that will keep endpoints secure, business and customer information safe and our company's name off the latest cyber victim list. The one solution that will reassure the C-suite and board members, now that they understand that cyber security is not just a tactical problem but a strategic issue.

But the recent discovery of critical vulnerabilities in the Symantec security suite has dispelled that dream once and for all. CISOs need to focus on several complementing security technologies versus relying on one security vendor or platform - focus on creating a new cybersecurity stack that balances traditional and innovative approaches through a deliberate strategy that always keeps benefit, risk and operational load in mind, and which brings the widest range of protection with the least cost and business disruption.

A general framework

As with most things when you have academics, corporations and governments all involved, the concept of a cybersecurity stack is somewhat fluid. On an organizational level, the security stack encompasses everything from password security to antivirus and HIPS/HIDS, from firewalls to physical security, security policies, education and backup strategies.

From the broadest level on down, these can be divided as:

1. Policies, procedure and awareness
2. Physical security
3. Perimeter security
4. Internal security
5. Host/endpoint security
6. Data security.

THE CONCEPT OF A CYBERSECURITY STACK IS SOMEWHAT FLUID

It starts with the endpoint

Each layer in this general cyber security stack can be broken down into sub-stacks. Of these sub-stacks, the first place of focus should be the endpoint protection stack. The SANS Institute found that nearly 50% of organizations are aware they've had endpoints compromised in the past 24 months. Once compromised, the endpoint can yield tremendous amounts of information, including access credentials to critical organizational systems and data.

Given that endpoints are the main entrance point for advanced attacks, and attackers continue to develop ever more sophisticated methods, various types of technologies have evolved around the endpoint and the network that surrounds it.

Each approach has its own strengths and weaknesses:

- Signature based malware prevention – Very effective at blocking basic malware but easy to evade.
- Exploit mitigation – Makes a vulnerability more difficult to exploit. Some technologies can be evaded by script-based malware.
- Network sandboxing – Some malware can detect sandboxing and avoids malicious activity until tagged as benign. Once executed on a real system, it starts its malicious activities.
- Application control – Exploits that use legitimate operations are not stopped (e.g. a malicious Word macro). Malware can also spoof a trusted application.
- Behavior analysis – Attackers that understand the rules defining suspicious behavior can design exploits that get past them.
- Endpoint detection and response (EDR) – Speed is critical – an exploit can cause serious damage before detection kicks in.
- Containment – This is the most challenging from an attacker perspective but can impact business efficiency from the user perspective.

Theoretically, the most comprehensive defense would incorporate all of the above techniques to ensure that the endpoint is covered from all potential threat vectors. In reality, dealing with the configurations, CPU drain, collisions between products, maintenance and vast quantities of data generated (including high rates of false positives) would be far too costly and degrade business operations to the point of almost causing as much damage as an attack. Not to mention the fact that the worldwide shortage of security personnel would make the task impossible.

Moreover, each of these techniques still has limitations and, even in combination, attackers may slip through the cracks long enough to cause harm.

So how should security teams decide which products to deploy?

THE LONGER IT TAKES TO DETECT AND CONTAIN A DATA BREACH, THE MORE COSTLY IT BECOMES TO RESOLVE

The leaner, meaner endpoint stack

Endpoint security technologies are generally added independently and haphazardly, in response to the latest threat or regulation, with little planning as to how they might best work together or how they may affect an organization's overall business goals.

Recently, a CISO told me he cannot identify the contribution of a specific HIPS agent his company added years back, one of seven agents; its value in the risk mitigation equation long forgotten except that it is required for regulatory compliance. There needs to be a better equilibrium of benefit and risk, a full understanding of the costs and implications.

The longer it takes to detect and contain a data breach, the more costly it becomes to resolve. The 2016 Ponemon Cost of Data Breach Study found that breaches that were identified in less than 100 days cost companies an average of $3.23 million, while breaches found later cost over $1 million more ($4.38 million).

Forrester rightly predicted that in 2016 cybersecurity would swing back to prevention. Take the case of ransomware – by the time an attack is detected, it is already too late.

An optimal endpoint stack should start with an effective and efficient prevention stack that catches the bulk of attacks for the lowest cost. Augment traditional signature-based approaches with memory protection and exploit prevention that prevent the common ways that malware gets onto systems. Combine new technologies like Moving Target Defense to handle advanced threats with existing "good hygiene" products like anti-virus. For all its flaws, AV is still the most effective prevention for run-of-the-mill malware.

With such a lean, effective prevention stack companies could possibly do away with HIPS, personal FW, tedious repetitive patching prompted by new vulnerabilities and other techniques that do little to improve security efficacy, but a lot to increase inefficiency of workstations and their users.

Supplementary components should be added according to specific organizational needs, always weighing benefits against costs. Businesses that are under frequent attack should consider EDR and sandboxing detection techniques, especially given that malware is most likely already in the network.

If this is done right, security teams will have fewer agents to maintain, a lower level of compatibility issues, less CPU drain, fewer false alerts and lower remediation costs.

Ronen Yehoshua is the CEO of Morphisec (www.morphisec.com) with more than 20 year of technology management and venture capital experience. Prior to Morphisec, Ronen was a partner at Cedar Fund, an international venture capital firm with over $325M under management. In this strategic, hands-on role, he lead investments and resided on the boards of several companies in seed and growth stages.

2nd ANNUAL SUMMIT

GLOBAL CYBER SECURITY LEADERS

7th – 8th NOVEMBER, 2016 | STEIGENBERGER AM KANZLERAMT | BERLIN

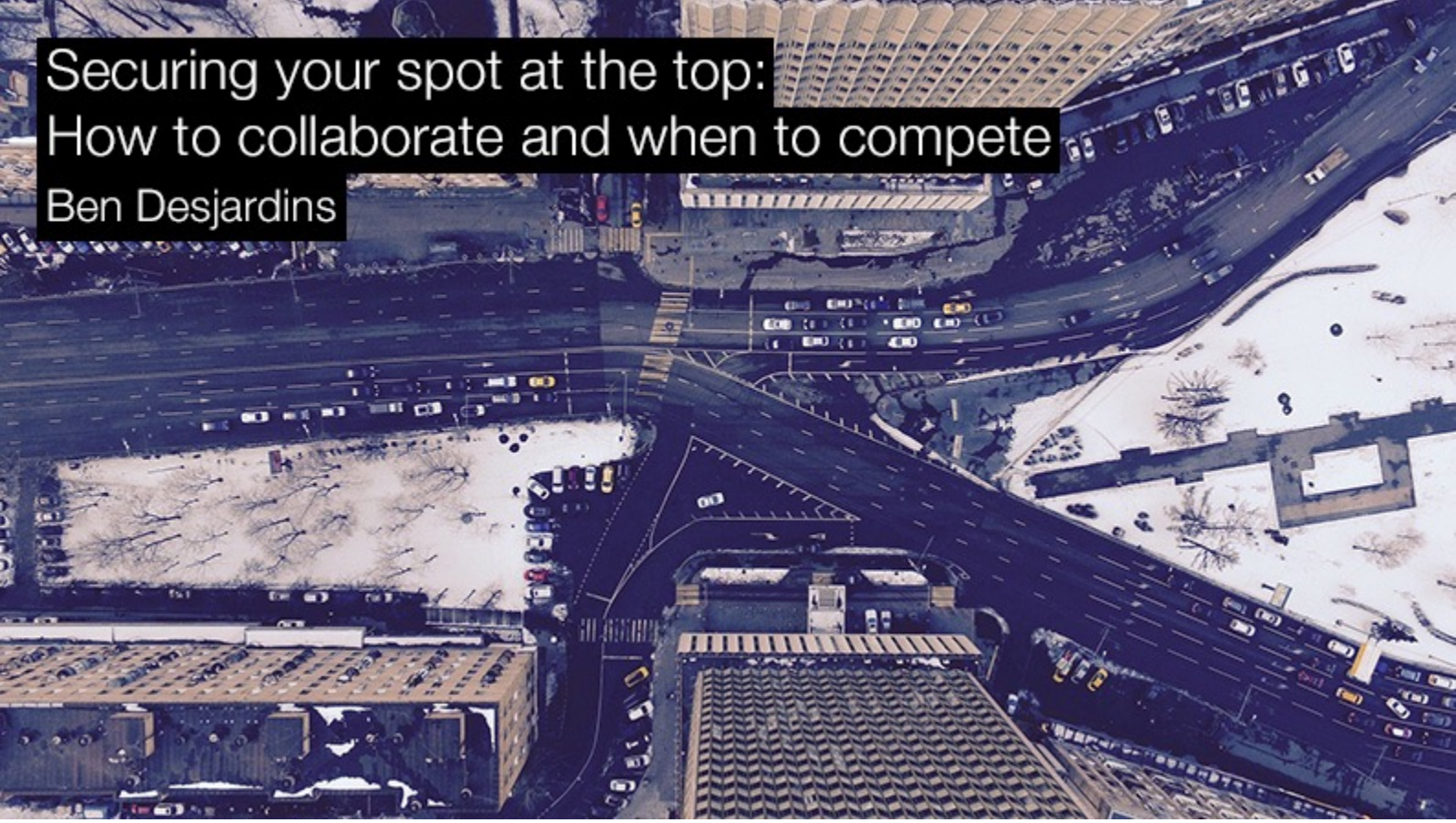
6 Cyber Challenges and Key Summit Themes

- Optimizing Crisis Preparedness
- Leveraging Cloud-Based Security Solutions
- Developing Trans-Organizational Security Cooperation
- Mitigating Human Aspect Vulnerabilities
- Integrating Next Generation Authentication
- Predicting Threats with Intelligent Analytics

20+ international Speakers include:

Thomas Tschersich, Deutsche Telekom AG, Germany
Daniel Selman, UK Ministry of Defence, UK
Scott Stewart, Stratfor, USA
Stephan Gerhager, Allianz Deutschland AG, Germany
Lakshmi Hanspal, SAP Ariba, USA
Volker Kozok, Bundeswehr, Germany
Kim B. Larsen, Huawei Technologies, Denmark
Kelvin Brooks, City of Atlanta, USA

Use code GCSL5HNS for € 500 discount!



Securing your spot at the top: How to collaborate and when to compete

Ben Desjardins

The IT manager tasked with understanding today's complex vendor landscape is in an unenviable position. The rapid proliferation of new types of cyber security threats and general IT dynamics has, in turn, driven a near equal proliferation of products and services aimed at helping manage the associated risks.

Keeping up with the categories of products and services that now make up the security vendor landscape is challenging enough, not to mention keeping abreast of the strengths and weaknesses of individual vendors.

On some level, the vendors themselves complicate this process through their efforts to differentiate around unique features or capabilities. Not all of this is disingenuous. The pace with which cybersecurity threats emerge and/or evolve creates both the need and the opportunity for vendors to innovate new capabilities that create true separation from other players in the market.

This specialization is, to a large degree, a necessary response to the continued innovation on the threat side of the equation. We see constant and clear evidence that traditional security products (firewalls, intrusion prevention/detection systems) continue to serve a key role but alone can't ensure protection from attacks of increasing scale and complexity.

However, leading vendors are not only pushing their own technologies in pursuit of new solutions, but also committing active teams to finding these opportunities through collaboration with other, sometimes competing, vendors. Expanded use of open APIs by a variety of technology companies, in conjunction with movements toward SaaS and cloud computing, have made a strong case for the necessity of third-party collaboration and integration.

In the security arena, this collaboration between vendors most commonly takes the form of API integrations that allow for the exchange of threat, vulnerability, or general security event data across products. In particular, most now expect vendors to support integration with major players in the Security Information and Event Management (SIEM) space. Enterprises and service providers often leverage SIEM platforms to deliver a consolidated view of relevant security information for correlation of events and to provide a "single pane of glass" view into their environment.

Keys to successful security vendor collaboration

There are some important considerations for vendors looking to collaborate, which also reflect some of the characteristics of collaboration that end users should be looking for from their vendors.

It's imperative to find opportunities where complementary capabilities address real-world use cases or scenarios. There are a number of trends within IT at any given time driving changes to the dynamics of how products and services are being used. Occasionally, these become disruptive trends that render good products or services suddenly vulnerable to obsolescence if they can't evolve.

One such trend would be the DevOps model, where application development, testing, and release of new applications or application updates occur more rapidly.

Even in the most disciplined application development environments where secure coding is part of the SDLC, every change to an application can introduce new vulnerabilities.

Suddenly, in this environment, application security scanning tools that were built to operate around more defined, spaced development cycles find they need to not only speed up their operation, but also tie into complementary products or services that help security teams act on results more quickly.

Every day we see clear evidence of the increasingly automated nature of the cybersecurity threat landscape

One way vendors can extend this concept further is to seek out technology collaboration that creates opportunities for automation in security operations. Every day we see clear evidence of the increasingly automated nature of the cybersecurity threat landscape.

The result is faster, larger, more complex attacks that can rapidly move from target to target seeking vulnerabilities to its tactics, techniques, and procedures.

As a result, forward-thinking security teams recognize they need collaboration and integrations that do more than add another product's data to a SIEM or other platform for consolidated human decision-making. Fight bots with bots and leverage unique combined technology capabilities to allow for faster response. Then focus the human skills on deeper interpretation and longer-term remediation strategies.

If we apply this to the DevOps example above, this might look something like a technology integration that takes the results of dynamic application testing and automatically feeds it into an application security product (such as a Web Application Firewall) for automated policy deployment in response to newly identified vulnerabilities.

Steps for IT pros to leverage or spur collaboration

There are some basic tactics that enable IT professionals to get more from potential collaboration within their stable of security vendors.

Focus on addressing your critical requirements, but know the categories to help you compartmentalize and quickly compare vendors

First, really understand the unique requirements of your network, applications, and business. With all the buzzword bingo in the security space, it's easy to get bogged down and become convinced you have to address something that either isn't a problem for you or poses little risk.

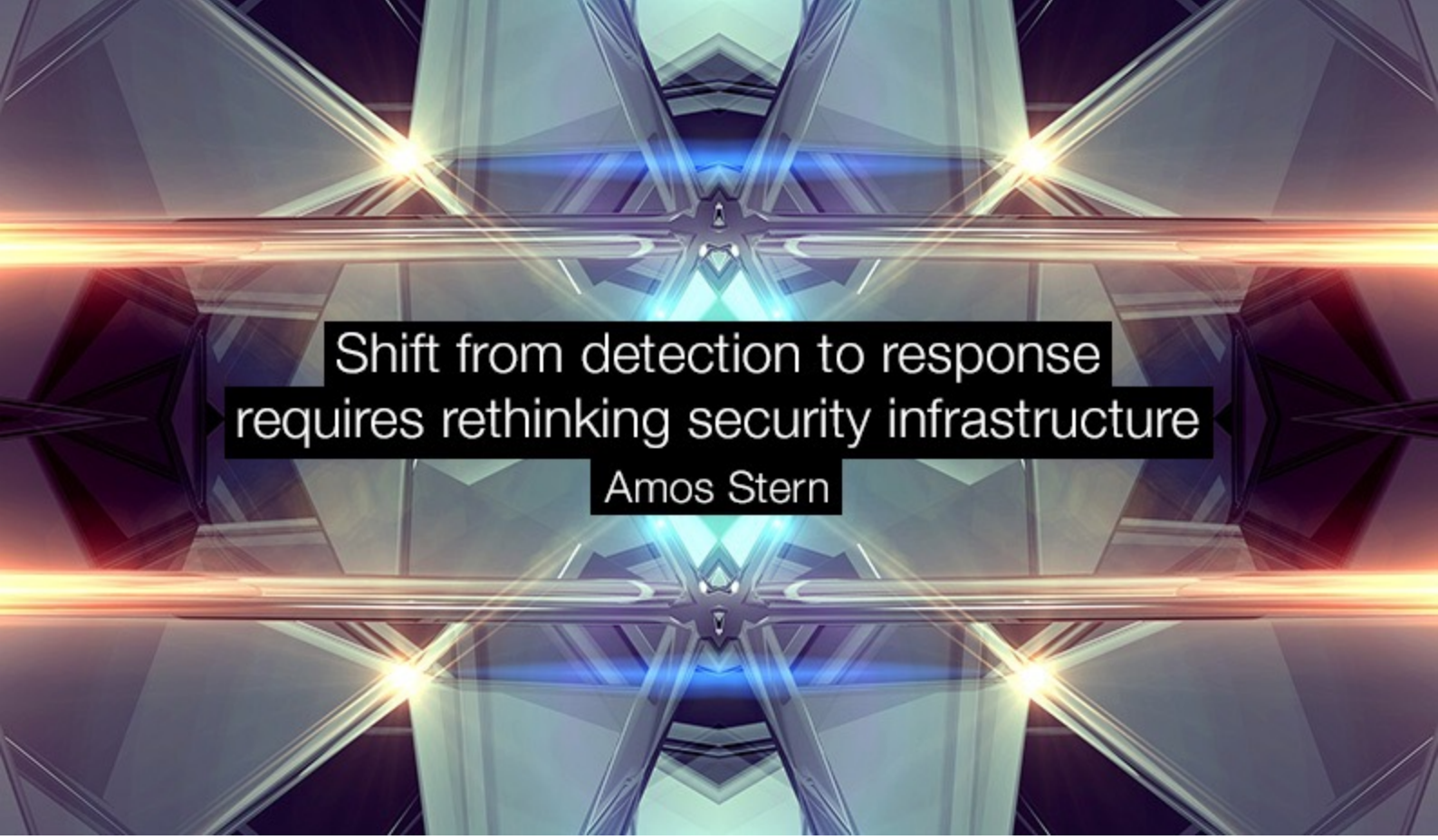
An example of this emerged in our 2016 Global Application & Network Security Report, where 35 percent of respondents listed Advanced Persistent Threats as the biggest danger, yet only 23 percent of respondents had actually experienced any such attack.

Another pitfall to avoid is becoming overly focused on the security headlines and assume those are critical requirements for protection. We see this often with customers exploring protection options from DDoS attacks. The seemingly daily headlines about multi-100 Gigabit-per-second attacks push many to focus primarily on total mitigation capacity of cloud vendors, but in so doing they overlook the potential damage of smaller or encrypted attacks.

The final step is to familiarize yourself and get comfortable with one of the existing security product/service taxonomies. That's not to suggest you should become rigidly fixated on the idea that all solutions need to fit neatly into one or the other for consideration.

Focus on addressing your critical requirements, but know the categories to help you compartmentalize and quickly compare vendors. It can also help you understand which categories are being successfully integrated for specific unique use cases and where your organization can flourish among the competition.

Ben Desjardins is the Director of Security Solutions at Radware (www.radware.com).



Shift from detection to response requires rethinking security infrastructure

Amos Stern

The world of corporate information security is locked in an ongoing battle, with hackers always one step ahead. In order to be successful, security operations teams need to rethink security infrastructure in their shift from detection to response.

Security teams traditionally turn to detection and mitigation tools in their attempts to overpower their pursuers. The tools used to detect, respond, prevent and predict attacks are numerous and complex.

Today, the typical security team employs a cocktail of detection tools, threat management tools, mitigation tools, threat intelligence tools, log management tools, and so on. The assumption is that the more tools the team uses, the better the chances of simple and straightforward containment will be. But a cursory look at the numbers behind recent breaches such as Anthem or OPM tells another story. Despite the plethora of tools found in security departments today, security teams are still locked in the battle – and they are not winning.

Because today's skilled analysts have to contend with so many tools, updates and processes, they often miss the big picture: they see the trees (each siloed element as its own entity, unrelated to every other aspect) while missing the forest: the overall picture of their security infrastructure, and how each aspect feeds into and relates to the others. As distinguished engineer and CTO of Security at IBM Europe Martin Borrett says, it's “hard to be successful when organizations have an average 85 tools from 45 vendors.” With a diversified and growing attack surface spanning IOT, mobile and cloud infrastructures, the number of tools needed to secure all these new platforms increases, introducing even more complexity and noise.

To truly see the context and connect the dots between all events, security teams must shift their focus away from point solutions and start viewing all aspects as part of one cohesive unit. For example, teams must start connecting external threat intelligence with alert data and internal assets to fully understand and contextualize threats across time and source. Is the team agile enough to see the individual aspects as one whole? Do they see the underlying story or do they just see the individual trees?

Remaining zeroed-in on this elaborate patchwork of point solutions essentially blocks teams from getting a clear picture into what is actually taking place within their security environment and can be damaging in a host of ways.

Loss of time

In a breach, every moment counts. A study conducted by the Ponemon Institute states that it takes companies in the financial sector 98 days from breach to containment (on average). Companies in the retail sector take 197 days on average to resolve them. This dwell time is staggering, leaving organizations vulnerable to threat actors.

The time it takes to put together the storyline of a threat can make all the difference between emerging from a breach with the integrity of data still somewhat intact or a complete loss of data.

Team efficiency

In the sea of alerts, logs and tools, security teams often feel like they are drowning. The same study found that a typical company receives 50,000 alerts per month, of which approximately five percent are real.

The rest are false positives, a result of fragmented and independent tools working in disunity with the others. But they all must be examined, as even one unprocessed alert can spell disaster as it did in the Target breach in 2014.

The underlying story behind the string of events that led up to the breach and ultimately, the loss of data of over 110 million customers, was there for all to see if they had been able to see events within context.

Target's varied and complex security environment contained so many individual aspects that when their malware detection platform alerted them to a high level threat, it went unnoticed, amid all the background noise.

The reality is that an alert from one detection tool could be deemed insignificant, yet when put together with information from other tools and alerts it could, in fact, be critical.

Loss of revenue

According to an annual study conducted by IBM and the Ponemon Institute, the average loss per year due to breaches for a large company is $4 million, a figure that is just slightly higher than it was in 2015, but a full 29 percent higher than it was just three years ago in 2013. And this isn't even the full cost. According to the study's author, "the biggest financial consequence to organizations that experienced a data breach is lost business." The true financial blow of a breach might not be fully felt for years.

To highlight all this, IBM's study shares with us this important gem: the longer it takes to identify and contain an attack, the higher the costs. And as the total cost of cybercrime crosses the $3 trillion mark, spending goes up proportionally. According to Steven Morgan at CyberSecurity Ventures, "as cybercrime rises, so does cyber defense spending — it's the nature of the beast."

Closing the gap

While point solution tools are effective in their own target domain, each on its own is incomplete, leaving analysts to do the complex dirty work of stitching together the real story of what is taking place. In this environment, it is nearly impossible to find context and easily correlate between events, and there is no underlying infrastructure, nothing to unify events.

In such a fragmented environment, with its multiple point solutions, alerts and logs, it is no small wonder that those alerts fall through the cracks, that incidents go uninspected and that threats remain unresolved.

Security teams today simply do not have the time or ability to deal with all the hundreds of moving parts that go into trying to contain the next big breach. Adding more tools, hiring more analysts, these are all just Band-Aids slapped onto the wound.

As long as corporate security continues down this path, the game of cat and mouse will continue and the bad guys will continue to emerge victorious.

Learning to see the whole story

A new paradigm is needed. One that takes all the disparate security sources and puts them into one unified picture, one single pane of glass, illuminating the relationships between them, focusing on what is significant and removing what is not, ultimately giving teams the tools they need to look at huge volumes of data and understand their significance at a glance.

So what is needed to help security teams actualize this new paradigm?

Provide end-to-end visibility: Security teams should implement software and tools needed to create a connective tissue that puts all events, alerts, logs and accumulated data into crystal clear context.

Streamline operations: Give teams the necessary training to organize workflows, process events and train new employees better, thus lowering overhead and using existing resources more efficiently and thoroughly. With tools that use existing resources more effectively, teams can take on entry-level staff and on-board them faster and more efficiently.

Put information sources into context: Identify and contextualize all incoming intelligence from all the numerous, difficult-to-access sources within organizations. Out of context, this intelligence is useless, living in its own silo.

Build a flexible and adaptive security infrastructure: As new data sources and requirements emerge, teams need to ensure their security environment is built to be able to incorporate new data sources and tools effectively as they evolve in a complementary manner.

Connect the dots: Collecting the data is not enough; it is the process of distilling intelligence out of it that will drive the value that SOCs need in order to evolve and compete in today's competitive security environment.

Understand that breaches will occur no matter what, so stop focusing solely on preventing breaches. They will happen.

Final note

Understand that breaches will occur no matter what, so stop focusing solely on preventing breaches. They will happen.

What matters most is how and how fast your organization responds to the threats. Using the right methods to locate and contain breaches reduces loss, cuts damage and reduces dwell time from months to minutes.

The parts and processes of your security infrastructure tell a story. When seen as individual units, the story is confusing, fragmented and difficult to decipher. Put those same events in context and a whole new world of insight and meaning becomes abundantly clear.

Amos Stern is the CEO at Siemplify (www.siemplify.co). He brings a unique technical and business background that includes leadership of the Cyber Security department within the IDF Intelligence Corps as well as directing sales and business development for Elbit's Cyber & Intelligence Division.

IP EXPO Europe 2016

ipexpoeurope.com - London, UK / 5 - 6 October 2016.

With six top IT events under one roof, 300+ exhibitors and 300+ free to attend seminar sessions, IP EXPO Europe is a must-attend IT event for CIOs, heads of IT, security specialists, heads of insight and tech experts. Cyber Security Europe at IP EXPO Europe offers invaluable security insight for both IT managers and security specialists. Hear from the experts how you can build stronger defences against cyber-attacks, and recover more quickly if your systems are breached.

Global Cyber Security Leaders 2016

cybersecurity-leaders.com - Berlin, Germany / 7 - 8 November 2016.

Meet with other cyber security leaders and learn from Texas Instruments, Allianz Deutschland AG, PayPal, Bundeswehr, City of Atlanta, Huawei Technologies, UK Ministry of Defence, Uber, Deutsche Telekom AG and many more, on how to establish an effective Cyber Security Strategy, address the human factor in cybersecurity, and improve your threat intelligence and cyber security response plan.

Is your business still HIPAA complaint after the 2016 federal changes?

Clyde Bennett

The US Department of Health and Human Services' Office for Civil Rights (OCR) warned healthcare professionals and their business associates of its intention to launch a series of random HIPAA compliance audits throughout 2016.

This announcement caused some panic among businesses unsure of their ability to pass a compliance review. Many organizations are unclear as to who's bound by HIPAA compliance standards and what aspects of their business will be evaluated during an audit.

Any organization that transmits electronic Protected Health Information (ePHI) is required to comply with all HIPAA parameters. These rules work to protect the security and confidentiality of patient data and the failure to adhere to these standards could put a business at risk for both substantial fines and potential lawsuits.

Covered entities and their business associates need to understand what's required to meet HIPAA standards and how their organizations could be affected if a random audit were to occur.

Understanding what is changing and what an audit entails will help ensure if businesses meet HIPAA compliance standards.

What has changed?

Before 2016, the OCR was only investigating non-compliance situations after a complaint, tip, or media report had been filed, thus 98% of closed privacy cases were the result of a complaint. The Health Information Technology for Economic and Clinical Health (HITECH) audit act became effective starting in 2010, but the OCR has yet to implement an audit program that will proactively evaluate the compliance status of covered entities and business associates.

A 2015 report released by the Office of Inspector General found the OCR's oversight of HIPAA compliance to be lacking.

Now, the OCR plans to strengthen its review efforts by implementing a second phase of audits that was scheduled to occur in 2014, but encountered a number of delays.

In this new round of assessments, providers with fewer than 15 physicians and healthcare business associates will be subject to audits. A business associate is any person or group that generates, stores, receives, or transmits PHI on behalf of the covered entity with which they're affiliated. A covered entity is any health plan, healthcare clearinghouse, or healthcare provider that electronically transmits PHI.

However, it's important to note that some states define these roles differently and businesses should check with their legal counsel or state trade association to determine the state's specific rules. In Texas, for example, covered entities are classified as any organization in possession of PHI, meaning business associates are subject to the same regulations imposed on covered entities. While the odds a practice will be randomly audited are slim, it's pertinent that an entity with access to PHI be vigilant about consistently evaluating and modifying its HIPAA security and compliance strategy, thus avoiding damages to its bottom line and reputation.

Business associates are required to implement training for their employees and all instruction efforts must be documented

The HIPAA Omnibus Rule

The Final HIPAA Omnibus Rule was established in 2013 to revise previous HIPAA definitions, clarify procedures and policies, and include business associates and their contractors within the HIPAA regulations. While the rule has been in effect for a few years, the OCR's lax investigation efforts have allowed some businesses to continue operating without adjusting their policies or procedures to meet the Omnibus Rule's standards. Covered entities should address the following elements of their organization and make any updates to former documents and procedures to ensure they will be adequately covered in case of an audit.

Business associate agreements

All business associate agreements should be revised and updated to include the standards outlined in the HIPAA Omnibus Rule. Whereas before, covered entities shouldered compliance responsibilities, now business associates are equally liable if a data breach or security error occurs on their end. Business associates must sign a Business Associate Agreement before their services are used by a healthcare provider and are subject to the same penalties and fines as a covered entity.

Privacy policies

The Omnibus rule includes several HIPAA definition changes and a provider's privacy policy should be updated to reflect these adjustments. Policies should include the amendments made in regards to deceased persons, the rights of patients to access the ePHI, and access request responses. They must also take into consideration the new restrictions regarding the disclosure of information to Medicare and insurance providers, the distribution of ePHI and school immunizations, and the use of ePHI for marketing, fundraising, and research efforts.

Employee training

An organization's employees can be either a risk or an asset to its network and information security. Sufficient training should be held to inform staff of the definitions and procedures changed as a result of the Omnibus Rule. Business associates are required to implement training for their employees and all instruction efforts must be documented.

How to prepare for an audit

For any organization, managing HIPAA compliance can be daunting. A business and its employees should understand what a HIPAA compliance audit entails and what steps should be taken to adhere to HIPAA standards. When an organization is audited, they will be evaluated on aspects like patient privacy requests rights for PHI, individual access to PHI, administrative, technical and physical safeguards, the use and disclosure of PHI, HIPAA Breach Notification Rule policies and changes to PHI.

If an organization is subjected to an audit, it will likely be required to supply a plethora of documents to the OCR. An organization has 10 business days to supply the requested information and if it does not have the proper documentation and procedures in place when the audit occurs, it will likely be unable to supply the necessary information in the allotted time.

Generally, an audit will require an organization to provide records of its compliance efforts dating back several years. If this information is unavailable or nonexistent, the company could incur a number of legal and financial penalties. Businesses bound by HIPAA regulations should hold regular security reviews to assess the ability of the organization and its technology to meet compliance standards. In addition, changes made to suit these regulations should be regularly documented and updated to prove a remediation plan is in effect.

It's vital an organization's security review be held and updated at least annually

When performing a security review, businesses should ask themselves:

- What written policies and procedures are in place to address HIPAA regulations?
- Is there an established incident response plan to address a breach if it occurs?
- Are regular risk assessments being performed and documented?
- What policies are in place to address data security?
- Are security and use policies for BYOD and mobile devices in effect?
- Are business associates complying with HIPAA standards?
- Is there a regular training program in place to educate both old and new employees about HIPAA compliance regulations?
- Do patients receive a Notice of Privacy Practices and where is this notice available? (on-site, online, etc.)

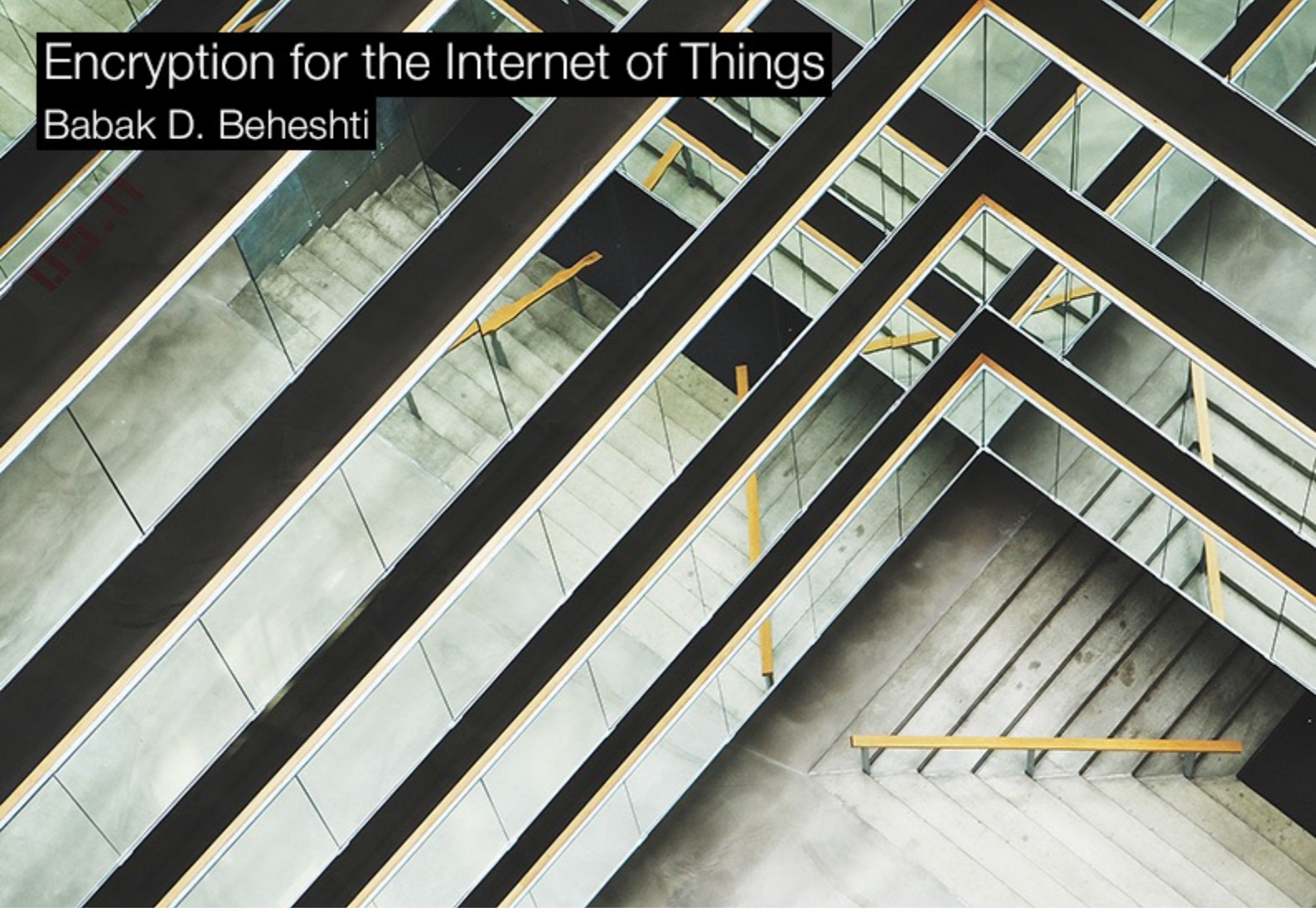
It's vital an organization's security review be held and updated at least annually as businesses often restructure processes or add additional technology to their IT environment. Such changes can leave holes in the organization's security strategy and render it vulnerable to a data breach.

While much of the HIPAA legislation remains unchanged in 2016, the OCR is bolstering its efforts to monitor and remediate PHI security risks throughout the nation. And as more organizations will be prone to an audit or investigation, it's important that business understand HIPAA so they can remain compliant and protect their clients.

Clyde Bennett is the Chief Healthcare Technology Strategist at Aldridge Health (health.aldridge.com).

Encryption for the Internet of Things

Babak D. Beheshti



For as long as there has been recorded history, humans have had the need to encrypt content-sensitive messages to prevent them from being read by anyone except by the intended recipient.

Early signs of encryption have been found in Egypt dating to ca. 2000 B.C., when non-standard hieroglyphics were used to hide secret messages. Archeologists have uncovered documented cases of secret writing in ancient Greece (Scytale of Sparta), as well as the well-known Caesar cipher in ancient Rome.

In the modern age of electronic communication, we have moved on from letter-based encryption schemes of the ancient past to digital schemes, all based on mathematical concepts and algorithms that not only obscure the original content of the message (plaintext), but also have properties that make them resilient to attacks by unintended recipients looking to decrypt the encrypted message (ciphertext).

Cipher schemes can be categorized into two groups: Symmetric Key, and Asymmetric key cryptography.

In a symmetric key cipher, the “key” (the unique digital pattern) that was used to encrypt the plaintext is identical to the key needed to decrypt the ciphertext by the recipient. This inherently requires the secure transportation of the key from the sender to the receiver. This produces a paradox in which our own cipher system needs another cipher system to transport its key.

Asymmetric key (or public key) cryptography schemes use an entirely different set of mathematical algorithms and concepts to create a situation where the key used to decrypt a message (the private key) will never have to leave the recipient’s sight.

On the other hand, the recipient openly publicizes his/her public key. Any party can encrypt a plaintext using this public key, but only the recipient has the ability to decrypt it with the

private key. The pair (public key and the private key) constitutes the key in these schemes.

In reality, the computational complexity of public key schemes is far more than that of symmetric key schemes, making them impractical for fast, and in particular real-time, massive data encryption/decryption. "Hybrid" systems are most prevalent today (for web based commutations), in which the symmetric key is initially securely exchanged using public key crypto, and subsequently the bulk data cipher uses symmetric key schemes.

Modern symmetric key ciphers can be either stream ciphers (in which one bit at time is encrypted), or block ciphers (in which a block of bits are encrypted at a time). The important factor to remember is that in the traditional web-based cipher, the computational power of the CPUs at either end of the communication link has been sufficiently large that these cipher schemes does not tax the performance of the CPUs significantly. Encryption time is used to calculate the throughput of an encryption scheme. In 2010, three scholars published their comparison of the performance of several key symmetric ciphers using a 2.4 GHz CPU. The throughput of the encryption scheme was calculated by dividing the total plaintext in megabytes encrypted on the total encryption time. The table below captures the approximate values.

Cipher	Throughput (MB/sec)
RC2	3
DES	4
3DES	3
AES	3.5
Blowfish	25
RC6	7

The Internet of Things (IoT)

The definition of the Internet of Things evolves around the central concept of "a world-wide network of interconnected objects." More things are being connected to address a growing range of business needs. In fact, by 2020, more than 50 billion things will connect to the Internet—seven times our human population.

IoT devices that connect to one another can range from a high-powered server to coin-sized (or even smaller) smart devices that collect information from their surroundings (via sensors) and transmit them wirelessly to their designated destinations.

Examples of IoT applications include wearable health and performance monitors, connected vehicles, smart grids, connected oil rigs, and connected manufacturing.

IoT security

Inadequate security will be a critical barrier to large-scale deployment of IoT systems and broad customer adoption of IoT applications. Since the data collected and transmitted via IoT devices can be private and often extremely sensitive, encryption of all transmitted data is a requisite feature of most applications.

The challenge in implementation of cipher systems in IoT devices comes in the low end of IoT devices where, by design, these devices can be very constrained as far as computational power is concerned.

Remember that a coin-sized device that must run on its internal battery power for periods upwards of one year has very low computational power, often a very low speed processor, little memory, and finally, often no hardware support for crypto algorithms.

Earlier in this article we saw the performance of symmetric key ciphers on a laptop with a 2.4 GHz CPU. What throughput do you think the same algorithms will yield in a small processor with little memory, say with a total computational power of 1/100 of the laptop used above?

Consider an Intel Core i7 5960X , manufactured in 2014, which has a performance of 238,310 MIPS at 3.0 GHz. Compare this to an Atmel AVR XMEGA MCU embedded processor that delivers 32 MIPS at the maximum clock speed of 32MHz. This is a performance difference in the order of 7500!

It is becoming clear that IoT devices need a new set of "lightweight" cipher algorithms that, while providing adequate security, are able to realistically run on low end devices. There are many such algorithms designed for specific application domains. Fortunately, all of these algorithms are public and significant studies are done on their performance and security. As a small set of example ciphers, a few such lightweight ciphers are introduced here. DESL and DESXL are lightweight versions of the DES cipher that are used in mobile applications. CURUPIRA-1 is proposed for applications in sensor networks. HIGHT is another lightweight cipher that is proposed for RFID devices, as well as sensor networks. XTEA (eXtended TEA) is a block cipher invented at the Cambridge Computer Laboratory, and the algorithm was presented in an unpublished technical report in 1997.

The table below gives the comparative analysis of the lightweight cipher algorithms available in the literature:

Cipher	Block Size (Bits)	Key (Bits)	Throughput (MB/s)
DESL	64	56	50
DESXL	64	184	50
CURUPIRA-1	96	96	120
CURUPIRA-2	96	96	120
HIGHT	64	128	25
XTEA	64	128	25

As can be seen, one can achieve real-time performance of encryption/decryption on constrained IoT devices using available lightweight ciphers.

In conclusion, as Premnath states in his the IEEE Wireless Communications Letters, since IoT devices typically exchange tactical data, as opposed to strategic data, it is more practical to achieve data protection for a time span ranging from real-time to a few days, as opposed to several years or decades.

HP performed a study in 2015 in which it reviewed ten products in the most popular IoT market segments. The study found that 80% of these devices raised privacy concerns; 90% collected at least one piece of personal information via the device; and 70% didn't encrypt communications to along their path to the destination.

As the public becomes more exposed to scandals of private data exposed due to ill-designed security features in their IoT devices and products, it will be more difficult for IoT device designers and manufacturers to avoid putting security and privacy as a central and paramount feature of their products.

Babak D. Beheshti is the Associate Dean of the School of Engineering and Computing Sciences at NYIT (www.nyit.edu). He has over 20 years of experience in R&D for embedded systems and wireless technology, and has successfully managed joint R&D programs with Asian, European, and U.S. companies including Siemens Mobile, Nokia, Samsung, KDDI, and LG. Beheshti has been an active member of IEEE since 1991.

Preparing for new EU cyber-security rules and regulations

Ross Brewer

Recently, the European Parliament signed off on its first ever set of cybersecurity rules. The Network and Information Security (NIS) Directive spells the end of more than three years of political bickering, and requires critical national infrastructure operators - such as banks, healthcare, transportation, energy and digital service providers - to ramp up their security measures and report major data breaches.

The directive is poised to establish the first set of baseline cybersecurity and breach reporting responsibilities in the European Union and will specifically require the implementation of measures that are proportionate to today's cyber risks and will minimise the impact of modern-day security incidents.

This will work in tandem with the EU's General Data Protection Regulation (GDPR), which will also force companies to tighten up their security with the threat of hefty fines and the small breach disclosure window.

However, while the GDPR requires notification of a breach only when there is a risk to personal data, the directive takes things one step further, mandating operators to notify authorities whenever there is an impact on the provision of its service.

The directive ultimately aims to improve security defences and knowledge sharing of today's cyber threats.

It's fair to say that hackers are using much more sophisticated techniques to gain access to data, which is making it much harder for companies to defend themselves. APTs, ransomware and stolen credentials are becoming increasingly common ways for hackers to get their hands on confidential information.

Furthermore, there's the insider threat to consider as people from within an organization continue to pose a risk to network security, whether malicious or unintentional. It is generally agreed that no organization is safe and threats will find a way onto the network, but they can be stopped before any damage has been done.

A big problem within the critical national infrastructure industry is that much of its infrastructure was developed and implemented prior to the proliferation of the Internet. As such, many SCADA devices used by critical national infrastructure industries employ very basic, easily defeated authentication methods, transmitting data in clear text, with many cyber assets operating on old and vulnerable code bases.

Examples of just how vulnerable SCADA systems are to attack include the recent Ukrainian power grid hack, which led to the first large-scale electricity outage, and the attack on a Ukrainian airport, in which suspicious malware was found on a computer at Kiev's main airport, Boryspil. Stuxnet and Flame are also two infamous forms of malware that have been used to hack into SCADA systems. These attacks highlight the growing threat to critical national infrastructure and SCADA systems, but also just how determined and capable hackers can be.

Gaining control of a SCADA system could, potentially, have a hugely damaging impact on a country and the increasing connectedness of infrastructure finds control systems being even more vulnerable to cyber-attacks, but also increases the knock-on effect an attack can have on other infrastructure sectors and capabilities. The situation is not likely to improve – as hackers will continue to target systems that require little effort on their part, yet have a large widespread impact.

What we often find is that those managing critical national infrastructure are relying on security strategies that are out of date and becoming increasingly obsolete. It is a dangerous misconception to think that using point-based perimeter tools, such as anti-viruses and firewalls are sufficient, especially when it comes to these industries that have such a huge impact on a country's economic stability and development.

Today's hackers are becoming increasingly persistent in their approaches and using extremely sophisticated tactics to exploit existing vulnerabilities. Sticking with basic security solutions may have worked in the years before cyber-attacks became one of – if not, the – biggest threat to national security, but this is no longer sufficient. If hackers are finding new, innovative ways to get into IT systems, then logic would dictate that companies need to find new, innovative ways of protecting their IT systems. Unfortunately, avoiding a breach completely is unrealistic, but there are ways to take control and mitigate any subsequent damage.

Given the notion that computing environments may already be compromised, the critical national infrastructure industry needs to move their processes and priorities towards detecting when compromises occur, and responding to them as quickly as possible. While that does not mean that threat prevention itself is obsolete, it simply means these defenses cannot be relied upon to protect against determined hackers. The time between detection and response is when systems are at their most vulnerable, and without a strategy in place to effectively and efficiently deal with the problem, the consequences could be far reaching.

Critical national infrastructure needs security intelligence, which ensures that all systems are continuously monitored so any type of compromise can be identified and dealt with as soon as it arises. Indeed, critical national infrastructure operators tend to be controlled across a variety of geographic locations, therefore, having a centralized system that can provide full visibility across all IT network activity in real-time is vital for the management of security.

Critical national infrastructure will continue to be a top target for hackers, and we cannot afford to have any sector not know if they can stay safe. Only by taking an approach capable of monitoring and analysing network activity in real-time can sophisticated attacks attempting to control critical national infrastructure and, more specifically, SCADA systems, be effectively detected, remediated and correctly mitigated before any significant damage is done.

Ross Brewer is the VP and MD of EMEA at LogRhythm (www.logrhythm.com). Prior to joining LogRhythm, he was a senior executive at LogLogic where he served as Vice President and Managing Director of EMEA.

IP EXPO® EUROPE

5-6 October 2016, ExCeL London

SIX IT EVENTS UNDER **ONE** ROOF

CLOUD EUROPE	CYBER SECURITY EUROPE	NETWORKS & INFRASTRUCTURE EUROPE	DATA ANALYTICS EUROPE	DEVOPS EUROPE	OPEN SOURCE EUROPE
Powering the Digital Enterprise	**Securing** the Digital Enterprise	**Hosting** the Digital Enterprise	**Insight** into the Digital Enterprise	**Enabling** Continuous Delivery	**Future** of Collaborative Code

IP EXPO Europe is Europe's number ONE Enterprise IT event for those looking to find out how the latest IT innovations can drive their business forward

REGISTER FREE

ipexpoeurope.com