CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

Inside: highlights from...

infosecurity EUROPE

05-07 JUNE 2018, OLYMPIA LONDON

IN THIS EDITION:

Question:

It's June 12, 2018, a historic day for the world.

Are we at a peaceful crossroad? Or will Cyber War continue, unabated?

JUNE 2018

MORE INSIDE!

CONTENTS

CONTENTS (Cont')

@MILIEFSKY

From the Publisher…

Are we at a peaceful crossroad or will Cyber War continue, unabated?

Dear Readers,

Today, we launch this special edition of our e-Magazine on a very historic day, June 12, 2018, when World Leader US President Donald J. Trump and Kim Jong-un, the Supreme Leader of North Korea Leader of the Workers' Party of Korea will meet in Singapore and begin the long-awaited peace process. Normally, we focus our entire magazine on best practices in cyber defense. With the potential of 'tearing down this wall', the wall being that of more open borders between South and North Korea as well as North Korea's gaining more open access to free trade and a more normalized voice on the world stage, by promising to de-nuclearize, how will that impact cyberspace? Will this mark the quiet beginning of more normalized relations regarding the ongoing Cyber war?

Think of the NHS WannaCry outbreak – that absolutely and obviously was an act of Cyber war, not Cyber-crime. Children and adults who needed operations waited 3 or more extra days due to the downtime. This was the weaponization of malware into an intranet DDoS attack guised as ransom-ware or a 'ransom-worm.' Do you believe, as we do @CyberDefenseMag that now is the best time to begin the dialog on forming a #GENEVA #CONVENTION on #CYBER #WAR? If so, let's spread this message to the World powers who have turned the 'citizens' of the globe internet – a great place for networking, communicating, of knowledge sharing and commerce into a warfare playground for cyber espionage, cyber terrorism and cyber warfare. Let's get them to focus their resources on defeating cyber crime instead of weaponizing the internet.

Thank you so much for your continued support! We're so thankful and honored to have you!

Gary S. Miliefsky, CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

Our Vision: To be the Global Leader of Cyber Defense Knowledge & Information

From the Editor…

We continue to grow, thanks to you. We attend more conferences now each year, so we can share the latest news on what's happening in the world of cyber defense with you. We are printing our global editions of our magazine in October for the IPEXPO Europe 2018, launching cyber defense TV and our global awards for leaders in cyber defense products and services, for our sixth year in a row. Our team has just returned from InfoSecurity Europe 2018, so we have some news from this brilliant and well organized industry trade show. We also have new mobile apps now & more coming soon…

To our faithful readers,

Pierluigi Paganini

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

PRESIDENT & CO-FOUNDER
Stevin Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR-IN-CHIEF & CO-FOUNDER
Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING
Sarah Brandow, VP of Marketing
sarahb@cyberdefensemagazine.com

Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451
SKYPE: cyber.defense
http://www.cyberdefensemagazine.com

PUBLISHER
Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
http://www.cyberdefensemagazine.com/about-our-founder/

WE'RE CELEBRATING

6 YEARS OF EXCELLENCE!

Providing free information, best practices, tips and techniques on cybersecurity since 2012, Cyber Defense magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV AWARDS

SEE US IN OCTOBER AT…

IPEXPO europe

SPONSORS

Are Your Data Transfers PCI DSS Compliant?

We'll help you get ready for the June 30 deadine.

If audited next month, would your file transfers pass the latest PCI DSS requirements?

GoAnywhere MFT uses **TLS 1.1 and TLS 1.2** to secure file transmissions over public and private networks. Our **Security Settings Audit Report** tests 60+ settings in your GoAnywhere environment against PCI standards - and gives you recommendations to fix those that failed.

See the Report in Action. Request a Demo.
www.goanywhere.com/demo

GO ANYWHERE®
Managed File Transfer

REAL-TIME CONTINUOUS DIAGNOSTICS & MONITORING

SHINE A LIGHT ON THE DARKEST CORNERS OF YOUR NETWORK

STIGs & Configurations

Continuous audit of policies & controls.

Threats & Vulnerabilities

Real-time discovery of Threats & Risk.

Asset Discovery

Automatic inventory & tracking of assets.

User & Entity Behavior

Monitoring of risky & unsanctioned activity.

Looking for the information you need to **Identify Risk**, **Direct Remediation**, and **Document Results**?

Look no further...

Get meaningful, actionable, and repeatable data, in real-time. AristotleInsight® is the world's first Continuous Diagnostics & Monitoring (CDM) Platform to bridge the gap between security frameworks and real-world IT Technologies.

Get the information you need, when you need it, with AristotleInsight.

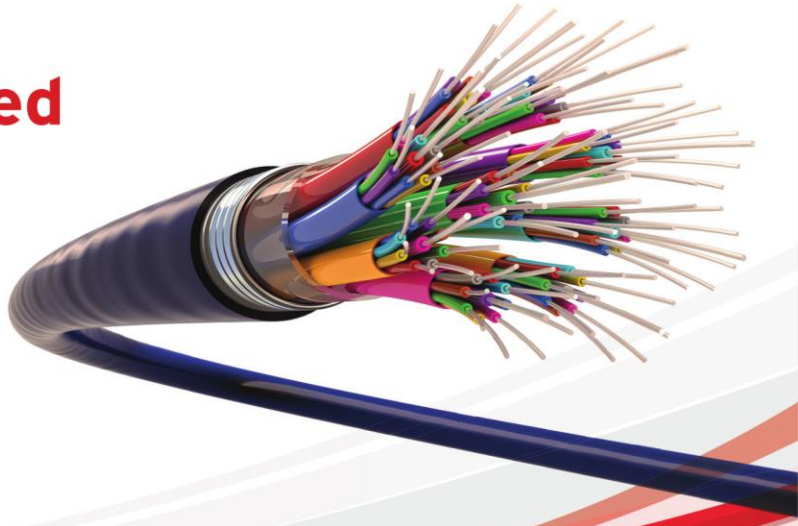
AristotleInsight®
— Identify | Remediate | Document —

AristotleInsight.com | Call us at 866.748.5227

TREND MICRO

POWERED BY XGen SECURITY

Detect and prevent breaches at wire speed



Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.

NSS LABS RECOMMENDED

Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber

Hacking Experts

Providing security solutions, training and professional services to enhance cyber security knowledge. We make cyberspace safer for businesses.

TRAINING SERVICES

HACKER HOUSE™

AS SEEN IN

Forbes Bloomberg FOX NEWS CNN WIRED SKY NEWS The Register MOTHERBOARD

CYBER SECURITY EXPERTS LEADING DEFENCES AGAINST THE DARK ARTS

PENETRATION TESTING SERVICES
view >

RED TEAM AND ADVERSARY SIMULATIONS
view >

INFRASTRUCTURE SECURITY
view >

WEB APPLICATION SECURITY
view >

HARDWARE SECURITY
view >

WIRELESS SECURITY
view >

MALWARE ANALYSIS

MOBILE SECURITY TESTING

BLOCKCHAIN SECURITY

ARTICLES

HOW GDPR COSTS COULD WIDEN THE GAP BETWEEN SMALL AND LARGE BUSINESSES

WILL THE GAPS WIDEN FURTHER BETWEEN SMALL AND LARGE FIRMS

by Reza Moaiandin, Founder, Cyber Scanner

In every line of business, there are always factors that can make breaking through to greater success seem insurmountable. While the causes change, the impact on smaller businesses never does. Online businesses currently have a new issue to tackle when it comes to the oncoming storm of General Data Protection Regulation.

THE CREATION OF A WEIGHTED MARKETPLACE

Sometimes the costs of running a business mean that you end up with an uncompetitive marketplace. The way most people understand this is by looking at large supermarket chains. If one brand can buy a hundred times the stock than another – and therefore can lower the price of each individual unit through deals to buy in bulk – then the smaller brand has no way of competing.

It cannot cut its prices until it grows past a certain point, and it cannot grow past that certain point because of higher prices. The latter is stuck in a catch 22 situation, while the market leader look more and more impossible to unseat or even challenge in any kind of fair manner. This is one way in which you end up with a stifled, uncompetitive marketplace.

However, we don't tend to think that way about the costs faced by online businesses – but we should.

WHAT'S FACING ONLINE BUSINESSES

Just because an online business doesn't have the same financial demands as physical stores, that doesn't mean there aren't costs. This makes it possible for larger, more established businesses to weather expenses that a smaller business cannot, therefore knocking those businesses out of their industries. This results in lost livelihoods, less innovation and less choice for consumers.

The looming threat on the horizon in this instance is GDPR, otherwise known as General Data Protection Regulation. If, like many currently facing this issue, you're wondering what that is, it's a set of regulations in EU law that's intended to give people control over their personal data. And in case you were wondering, no, Brexit won't make any difference to this legislation or when it comes into effect.

This is an issue which has obviously become a very hot topic in light of the recent Facebook data breach. It's a terribly complicated set of regulations – far too lengthy to go into any detail here – but in the simplest terms possible, its intention is to protect your personal data and your privacy.

So, new regulations, and ones which have good justification – how much trouble could they possibly cause?

THE REALITY OF THE REGULATIONS

A moment ago, we mentioned that the regulations were far too complex to go into detail here, and this is no exaggeration. Based on estimates derived from 1000 senior executives across Europe, in a piece of research known as Finding the Missing Link in GDPR Compliance, it is estimated that many businesses will spend an astonishing 172 hours a month on GDPR data searches. In other words, it requires another member of staff working full time purely on this issue.

And if you fail to meet these regulations, then the fines can be devastating, going up to over £20 million or 4% of annual turnover. This could potentially spell the end of one in five European businesses, according to Petter Nordwell, Director of Marketing at Sophos.

WHO IS REALLY THE HARDEST HIT?

It's important at this point to make clear that these regulations do go after the largest businesses harder, with tougher fines and penalties for example. Not only that, but a bigger company usually means more data, and therefore a bigger challenge to be met.

However, it will still likely impact smaller businesses more. One major issue is that small businesses simply don't seem to be taking this as seriously as they should, cutting it very fine to the May deadline. 90% of small businesses were not fully prepared by the end of February 2018, according to the FSB, with many completely unaware of the issue.

Furthermore, there's the simple reality of whether or not they can afford to put aside the amount of work hours and the costs associated with that in order to deal with the issue in time. This is where the resources of a large business really give them an advantage.

Large, small and medium businesses are all facing this challenge. However, smaller businesses may be going in the most unprepared, or not prepared at all. They might find themselves pushed out of business in the face of tough regulations and the weight of the competition, who have better resources at their disposal.

About the Author

Reza Moaiandin is Co-Founder & Technical Director at SALT.agency and Cyber Scanner. He has over 16 years' experience in software engineering, Reza has been involved in cyber security for nearly 10 years. Originally, Reza worked on security bugs on phpNuke, and moved onto writing complex algorithms for phishing detection, during his last year of university Reza designed an artificially intelligent algorithm that detected phishing websites faster than Google.

Reza can be reached online at our company website https://cyberscanner.com

ON THE CLOCK

WHY TIME IS CRUCIAL IN SECURITY EXECUTION

by Brad O'Hearne

DISCLAIMER: As with all security operations, always act in accordance with the highest standard of legality and ethics, making sure you have the proper authorization for any security exercises in which you engage.

Suppose for a moment that the relevance of time was removed from all human endeavour. How would that change the nature of athletic races? What if it no longer mattered how long it took an Olympic bobsled team to reach the bottom of the track, just that they reached it? Consider the field of medicine: what if the time required to discover a treatment for a fatal disease held no detrimental impact to those desperately needing a cure? What if military operations resulted in equal casualties and outcomes regardless of the timing?

Grasping these scenarios is difficult to fathom, because in our world, their significance derives from the speed of execution accompanying the effort. Without the defining aspect of time, efficiency and speed would cease to be relevant as well. Only the ability to complete a challenge would be important. So, if a few beer-swilling gents plucked from a Saturday barbecue were able to make It across the pool without drowning, they'd be equally deserving as Michael Phelps for an Olympic gold medal in the 100 m freestyle. Everyone suffering from a terminal disease would live indefinitely until a cure was available. Or each side in a military conflict would wait for all troops and weaponry to arrive and position in the battlefield before the first shot was fired.

These imaginations are clearly ridiculous, because in the real world, mere ability is not enough: time matters. The fastest wins the race. The cure discovered quickly saves the most lives. Militarily, perhaps General George S. Patton said it best: "A good plan violently executed now is better than a perfect plan executed next week."

Yet when it comes to security implementation, the sole presence of capability commonly remains the focus, as opposed to speed of execution. Particularly amongst management, security programs are evaluated through inquiries such as:

- Is a vulnerability management program in place?
- Is there an intrusion detection system in place?
- Is there an incident response policy?

Questions of this nature typically feed checkbox-type evaluation, absent of a qualitative analysis based on merit. Thus, both solid and awful security programs simultaneously have the possibility of resulting in the same answers to these questions. Viewing a security program through these have-it-or-don't lenses can encourage a mindset that improving security is the byproduct of increasing capabilities, i.e. defining more policies and adding more security tools to the mix. This is a sibling of the false perception that

the most money and resources necessarily results in a superior security program. While having abundant resources and a full toolbox is no doubt a desirable luxury which can help tremendously if employed strategically, it guarantees nothing. If it did, security news headlines would be dominated by under-resourced, fledgling companies. But they aren't – the largest companies and governments in the world, with comparatively massive security budgets and headcounts, can't keep out of the limelight.

Organizations of any size and budget can significantly improve their security posture by shifting their focus from stockpiling security tools and capabilities to focus instead on the speed of execution of a few key abilities.

THREAT INTELLIGENCE

Every day, new vulnerabilities and threat vectors are discovered in operating systems, common services, third-party component libraries, etc. Likewise, waves of attacks often follow trends (such as the recent spate of cryptocurrency-mining malware distributed by botnets). It is crucial to have awareness of these developments in as close to real-time as possible. Reports of new vulnerabilities often hit the news media well before they are catalogued in public vulnerability databases. It can take much longer for vulnerabilities to appear in updates to industry vulnerability scanners, which it would seem many rely on as their means to stay current.

Recently, I came across a particular vulnerability where the time between public disclosure and appearance in vulnerability scanner updates was around ninety days. If relying on security tool vendors to keep pace, this example gives potential attackers three full months lead time before even having awareness of whether the vulnerability exists in organization apps and systems – this doesn't include analysis and remediation time.

If you have the opportunity to employ a commercial threat intelligence tool, that can be a helpful time-saver. But if not, all is not lost. For the past several years, I've daily monitored a number of security-related web-sites, RSS feeds, and listened to a number of weekly security podcasts to keep current. It has consistently paid off – I am nearly always ahead of both those around me and vendor tools. Furthermore, acquiring this knowledge immediately when available has allowed me to quickly investigate other implications of these vulnerabilities to apps and systems before external exploit attempts kick into high gear.

GOAL: REDUCE TIME TO BECOME AWARE OF NEW THREATS TO YOUR APPS AND SYSTEMS. NARROW THE TIME GAP BETWEEN PUBLIC DISCLOSURE OF VULNERABILITIES AND POSITIVE IDENTIFICATION OF IMPACT TO YOUR APPS AND SYSTEMS.

Once a vulnerability has been determined to have impact, analysis and remediation will follow. Typically, an organization's vulnerability management program will have defined remediation time windows based upon severity. Time windows can vary widely across organizations. I've seen expected remediation times for common severities defined anywhere along the following spectrums:

- Critical severity: ASAP to thirty days.
- High severity: a few weeks to over sixty days.
- Medium severity: sixty days to six months.
- Low severity: ninety days to no commitment at all.

Those time ranges are diverse enough that they really call into question the primary motivation. In my observation, the approach to defining remediation time windows often derives from what efforts are considered nonintrusive and can be absorbed comfortably. While desirable to set goals that can be feasibly accomplished, if remediation arrives too late and fails to thwart attacks, those goals are at best a placebo, which eventually will fail.

Furthermore, there's a big difference between defining remediation time windows, and consistently remediating within those time windows. The definition is irrelevant if actual remediation times fall outside of those windows.

If I had to give an organization only one piece of security advice, it would be to become exceptionally efficient at consistently remediating vulnerabilities within tight time windows. The ability to remediate vulnerabilities quickly is the difference between preventing an attack, and having that vulnerability exploited (and all of the aftermath which may follow, including complete organization compromise). Preventing attacks, breaches, and destructive impact is the objective, and vulnerability remediation time windows should be defined to that end. If not successful defensively, a vulnerability management program is prioritizing style over substance.

GOAL: SET TIGHT VULNERABILITY REMEDIATION TIME WINDOWS. REORGANIZE OPERATIONS TO BECOME EXTREMELY EFFICIENT AT CONSISTENTLY REMEDIATING VULNERABILITIES AS QUICKLY AS POSSIBLE.

INTRUSION DETECTION & RESPONSE

With many companies still trying to figure out how to respond to new vulnerabilities when disclosed, to what degree have companies successfully organized tactical intrusion detection and response operations? Even if they have such teams and programs, do they have any concrete appreciation for their actual execution while under live attack?

I'd speculate that the majority of organizations probably have, at best, a network monitoring tool and perhaps a SIEM for intrusion detection; and some kind of policy and designated personnel in the event that indent response is required. These are necessary parts of the equation, but devoid of live simulations and rehearsals, nothing can ultimately be concluded about the ability to deal with a real attack.

Going back to the original three examples: how well could an athletic team be expected to perform in a game if they never practiced or scrimmaged? How well would a doctor perform in the operating room if never involved in a prior surgery? What could be reasonably expected from a platoon of soldiers who had never rehearsed coordinated troop movements and war games? Yet in security, there seems to be a perception that operations can be played by ear when an attack occurs, and a favorable outcome will result.

During a live attack, the answers to the following questions hang in the balance:

- Will the attack go unnoticed, or will it be detected?
- Will the app or system be successfully exploited, or will the attack be thwarted?
- If the app or system is exploited, will the attacker gain a foothold, or will they be identified and locked out?
- How long will an intruder foothold persist before it is detected?
- What undesirable impact will intrusion have against apps, systems, and data?
- How quickly and to what degree can the organization recover from destructive impact?

The answers to the above questions are highly dependent upon the speed of execution of both intrusion detection and intrusion response. The attacker most likely has performed the attack before, and has scripted their intended actions to some degree. They know they are working against time and detection. Unless your organization can efficiently execute quicker than the attacker, you will lose.

GOAL: CONSTRUCT A COORDINATED PLAN FOR INTRUSION DETECTION AND RESPONSE. PUT THE PLAN TO THE TEST UNDER LIVE ATTACK CONDITIONS, TIMING THE SPEED OF DEFENSIVE OPERATIONS AND ULTIMATE SUCCESS MILESTONES. ANALYZE THE OUTCOME, AND REVISE STRATEGY TO COUNTER WEAKNESSES. RUN SIMULATIONS AGAIN, TRYING TO LOWER THE AMOUNT OF TIME IT TAKES TO NULLIFY THE ATTACK.

SURVIVABILITY

There are more holistic organizational benefits which come from executing security operations swiftly. Some may consider it liability, others may refer to it as reputation, or call it PR. But it really includes all of the above: it is the ability for an organization to favorably survive a serious security incident. The speed at which security operations are executed says something about an organization's attitude toward security. When vulnerabilities are remediated slowly, and when there's no dedicated effort to detect intrusion or respond to an incident with urgency, it communicates a lack of priority to the organization.

When assets and potentially private user data hangs in the balance, it is important that actions document responsible security handling. Actions should be explainable, and defensible if necessary. How security operations are conducted should be evidence that the company places a high priority on security. Should these actions become public, their reality should serve as a PR asset, enforcing a message to the public that an organization takes security seriously. Otherwise, lax policies and procedures, or actions inconsistent with adequate policies and procedures, may have the opposite effect, and serve to demonstrate neglect. An organization's mishandling of security operations can become a bigger damage control problem than the actual security incident in play.

CONCLUSION

In security, it isn't enough to have policies and procedures defined. It isn't even enough to execute on those policies and procedures. Battles against attackers are won by whomever presses their initiative first. What determines the effectiveness of a security program is the ability to execute at speed. As security professionals, we are always on the clock.

About the Author

Brad O'Hearne is a 25-year career software architect / developer, application security expert, and independent security researcher.

He resides in Gilbert, AZ and enjoys cycling, soccer, reading, and spending time with his family.

He is available for consultation and can be contacted at brado@bighillsoftware.com.

5 THINGS EVERYONE NEEDS TO KNOW ABOUT CYBERSECURITY

PRACTICAL WAYS TO PREVENT A CYBER-ATTACK

by Kevin Cassidy, CEO, ClearFocus® Technologies

What do you think of when you hear the word "cybersecurity"? For some, just the name sounds ominous and somewhat overwhelming. Years ago, it was simply called IT Security, and all you needed was a good firewall and antivirus protection software to protect your company's information. But in recent years, the information security landscape has changed significantly, as the adversary has dramatically stepped up methods for attacking a company's vulnerable IT infrastructure. So, before you move on to other work priorities, please read the **5 Things Everyone Needs to know about Cybersecurity** below:

1. Everyone is at risk.

It's news we hear almost daily: another prominent company has fallen victim to a cyber-attack. Large, well-funded companies with sophisticated cybersecurity programs like Target, Sony, Equifax, Anthem, and eBay, have all experienced security breaches in recent years that have compromised sizable amounts of sensitive information. Large companies are often on the radar for hackers, but did you know 61% of data breach victims are businesses with under 1,000 employees?[1] In fact, according to a recent survey, 80% of organizations have been negatively impacted by a cyber-attack in the past 12 months.[2] So, if you haven't suffered a cybersecurity breach yet, you've either been incredibly well prepared, or very lucky, since most malware indiscriminately searches for vulnerable companies across the internet.

2. Cybersecurity is all about defense.

We will always have cyber threats, as the adversary continually looks for new methods and ways to infiltrate your organization. The best way to prevent a cyber-attack is to build a strong defense, by systematically and continually addressing your company's cyber vulnerabilities. A cyber vulnerability can be software that is not patched, a misconfigured firewall or even a weak password. There are several cost-effective cloud-based vulnerability monitoring solutions that can continually identify and help resolve your company's existing vulnerabilities. For example, vulnerability management software can inform you about patches you absolutely need to apply today versus less critical patches. In fact, the Wanna Cry ransomware virus that crippled many European banks in May 2017 could have been avoided by applying a critical Microsoft patch issued in March 2017. So, in order to build a strong defense against a cyber-attack, you need to continually and systematically address your cyber vulnerabilities.

3. *What you don't know can hurt you.*

Many companies, large or small, do not have a complete inventory of all the devices and software running on their network. As a result, vulnerable assets continue to operate on networks unnoticed, and more importantly, unsupported. IT professionals dutifully patch systems and upgrade software, only to miss a device or software that has a serious vulnerability that could lead to a security breach. To prevent rogue devices from compromising your company's network, you need a comprehensive and current inventory of all devices and software running on your network. There are many affordable tools that can scan a company's network(s) and discover all devices and software running on it. So, don't take the risk of not having a complete inventory of devices and software running on your network. What you don't know *can* hurt you.

4. *End users are the weakest link.*

End user behavior causes most cybersecurity breaches. In fact, according to a recent survey, 1 in 14 users are usually tricked into following an illegitimate link in an email or opening an attachment that leads to the installation of some form of malware.[1] Think back to the 2016 Presidential Election, when the Democratic National Committee suffered a significant breach of sensitive e-mails because of a single spear-phishing e-mail sent to John Podesta, Chairman of Hillary Clinton's U.S. Presidential campaign. The e-mail led Mr. Podesta to click on an illegitimate link to change his Gmail password, which ultimately compromised his e-mail. Recently, 65% of professionals have identified phishing and social engineering as the biggest threat to their organization.[3] Since most cyber-attacks begin at endpoint devices like desktops and mobile devices, you really need to protect your network from end user behavior. You can tighten up this weakest link in your cyber defense through training and awareness, and by implementing next generation endpoint security to isolate and sandbox any malware that an end user might unintentionally introduce to your network.

5. *Information in the cloud is still at risk.*

Many people believe that putting their information in the cloud shifts responsibility to the cloud provider for information protection. They often may fail to consider that end users access information in the cloud from their desktop or mobile device, from the company's network, or even worse, from a public network, where they are connecting their company's cloud resources to any security vulnerabilities on their device or network! For example, a single compromised password can provide legitimate access to the cloud and exploit cloud resources. Also, depending on the type of cloud service, some cybersecurity responsibilities still fall on the company to secure. According to Gartner, *"The cloud will require a different approach to security; on-premises security habits and designs won't work well for information stored in the cloud."*[4] Therefore, it is highly recommended that companies take a comprehensive view of their company's

cybersecurity and extend security boundaries to include cloud resources. No matter where information is hosted, all company information assets should be monitored and secured.

[1] 2017 Verizon Data Break Investigations Report.

Retrieved from: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[2] 2017 AT&T Global State of Cybersecurity Survey

Retrieved from: https://www.business.att.com/content/whitepaper/cybersecurity-report/v6/index.html

[3] 2016 UBM Cybersecurity Trend Report

Retrieved from: https://techbeacon.com/resources/cybersecurity-2016-trend-report-ubm-ponemon-study

[4] Gartner: Is the Cloud Secure? January 23, 2017, Contributor: Kasey Panetta

Retrieved from: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

About the Author

Kevin Cassidy is the CEO of ClearFocus® Technologies, a company that provides Next Generation Cybersecurity and Secure Cloud solutions to solve today's challenges and prevent tomorrow's problems. Kevin has provided IT leadership for Fortune 500 companies, government agencies and small businesses for over 30 years, with a focus on solving systemic enterprise IT and security problems. Kevin started ClearFocus® in 2012 to provide cybersecurity and secure cloud solutions for the federal government and commercial enterprises. Kevin can be reached online at (email: kcassidy@clearfocustech.com, LinkedIn: https://www.linkedin.com/in/kevin-cassidy-9733983, Twitter: @KevinFCassidy) and at our company website http://www.ClearFocusTech.com

SHOULD HACKING COURSE BE A PART OF UNIVERSITY CURRICULUM

Before continuing that course, let me tell you something about my own experience. At first, I did not know anything about the course (I just remembered basic Networking but nothing about hacking).

My course started with critical essential topics in networking. It was taught by an experienced Security Expert. Concepts of networking got cleared to me, and I felt like I have really learned something useful.

Remember, these concepts are not a part of official CEH course, but they were taught to us. I think that the Expert who taught us is a great person.

So, please study NETWORKING before pursuing CEH course because it is mostly not taught by the Experts as it is required.

After those concepts, the rest of our course was taught by a young Expert, who was only 22 years old at that time but he had excellent knowledge about hacking.

After that our relationship was more like friends rather than student and teacher.

There are 20 topics in official CEH course(v8). Each problem is a set of particular type of attack or something like that.

Now let's come to the topic what I learned and what are its advantages: -

- You will get to know how things in the field of Hackers work.
- Your misconceptions about hacking will be resolved.
- Your problems regarding hacking can be solved by the Expert.
- You will have a permanent routine for learning about hacking.
- You will understand that Hacking is not merely about getting unauthorized access to computers or FB accounts. It is much more than that. It is an art.
- You will get to know that at which subdiscipline of CEH you are good at so that you can further give more attention to that subdiscipline.

But all the above advantages depend on your teacher and Institute.

So, I would suggest that choose a good institute and probably choose the institute which is a part of any Security firm. It will provide you with proper labs and real Security Experts and not just random teachers who will teach you about theory more than practical.

Now let's start with some benefits of hacking course in everyone's life. We heard from many people that why hacking sessions is being a part of University's Curriculum? Because as you know that today's world is full of technology now, and the most important thing that is everywhere in nowadays is "DATA."

In an ethical hacking course, we learn management and security of Data. So, yes! This field has great scopes in coming future.

BENEFITS OF HACKING COURSES IN UNIVERSITIES/ SCHOOLS:

Why do teachers need to teach hacking courses in Universities? After Parents, Teachers have all the authority to guide you with better vision and solve your issues. We have to clear brainstorm ways by which we can build the pipeline of cyber security professionals while developing the cyber curriculum in Schools or Universities to decrease the number and impact of crimes.

You know what, in today's world, we are facing so many problems in cyber security which makes our kids more coward and irresponsible. These three are common in them:

- The rash of crimes or violations;
- Un-professional security, most of them are barely qualified;
- Shortage of learning about cyber education.

By outlining these main problems, we can also develop a standard solution which is teaching the kids about hacking or provide them hacking courses in their regular university curriculum. Do not teach the wicked type courses, but simple proactive cyber security in a fun and interactive way. We need to start this today to increase the cyber security workforces of tomorrow. That's why every school and universities introduce a hacking course to make their tomorrow better.

Also, most of the kids can point and click, but they do not even know the proper ways of how the underlying technology works. In another side, most of them do not take advantage of basic techniques on how to manage to save themselves and their overall information online, before it turns into bad choices.

It further creates a complicating or confuses situation when teachers have lack resources, and they do not have enough knowledge of technology, then how can we suppose from them to teach the kids professionally? We are undergoing an intense storm of cases where we have a great need of hacking courses and complete knowledge, but we are getting failed because of lack of the availability of the sessions.

How can we solve these issues? If we really want to address those issues then we have to encourage the kids to learn about how the technology works and how can we save

ourselves with the help of hacking skills. And of course, we must include ethics and responsibility in that study.

Security experts can be a part of the solution by involving themselves in some local schools/universities to further help and educate the teachers and the students by offering in some programs like Cyber Patriot, NCSA Stay Safe Online and the ISC2 Foundation's Safe & Secure Online. The charges are less, and the advantages are many, mainly given today's death cyber security situations.

IMPORTANCE OF LEARNING HACKING COURSES:

Learn hacking skills to prevent any type of hacking, and this will also help to recognize network security vulnerabilities and patch security breaches before anyone can harm them. Hacking courses are way more important in this world of technology because we put everything on the online basis and due to a hacking skill; you may save your entire documents or other essential things in minutes before the crime takes place.

Learning about hacking can help the information security experts to perform the most robust potential security systems. It is much like to finding and repairing security vulnerabilities as it is blocking them. You can also study more about the techniques which hackers use to infiltrate systems, you will also be able to resolve the issues entirely; if you do not learn about how the black hat hackers could get into your systems, you are going to have a difficult time securing them.

Let's talk simply, like you have a computer network which looks like a yard with lots of fences to keep the people stay out. And you have planted something worthy inside the yard, and then it might be possible that someone may want to jump the fence and steal that good item before you know it. So, in hacking courses, you will have to learn about the daily checking for vulnerabilities in and around the fences so you can strengthen the weak areas before anyone decides to get in.

However, a successful ethical hacking needs being a mentor in every problem and its solution. Knowledge of how computer systems and programming languages operate is also necessary because if you get to know the details about how the actual system works, it's going to easier for you to think of ways to exploit the system.

HOW TO BECOME A PROFESSIONAL ETHICAL HACKER:

According to the technology world, choosing managers look for people who have the ethical hacking knowledge, or they do have degrees regarding information security and information technology, as well as IT certifications. It's likely to start your profession in ethical hacking or drive your work in the field as your experience improves. Hack training sites such as hackthissite.org can also help you to get you focus on your hacking skills despite your experience level.

Although, a Certified Ethical Hacker is an experienced professional who reads and knows about how to scan those weaknesses and vulnerabilities in targeted systems and how to uses the same data and tools as an infamous hacker, but in a lawful and authorized manner to value the security presence of a target system.

The actual purpose of this course is to help you learn an ethical hacking methodology that can be used in a stabbing testing or any other moral hacking situation. Imagine, you step out the gate with ethical hacking skills that are immensely in demand nowadays, also, the internationally recognized Certified Ethical Hacker certification! This course provides you with EC-Council Certified Ethical Hacker exam 312-50. Some of the primary purposes of the hacking course are given below:

- Build and rule minimum criteria for credentialing professional information security experts in ethical hacking projects.
- Notify the society that credentialed people meet or pass the minimum standards.
- Strengthen ethical hacking as a different and self-adjusting profession.

About the Exam:

- Number of Questions: 125
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Test Delivery: ECC EXAM, VUE
- Exam Prefix: 312-50 (ECC EXAM), 312-50 (VUE)

This is the worlds most developed a certified ethical hacking course with 20 of the most popular security fields, any person will ever need to know if they are planning to beef up the information security position of their organization. In 20 comprehensive modules, the course covers 340 attack technologies, commonly used by hackers.

This course also provides the most superior hacking tools and techniques which also used by hackers and information security professionals alike to break into an organization. Also, remember that "To beat a hacker, you need to think like a hacker."

About the Author

Meesha Saleem is an SEO and Inbound Marketing Specialist, he is currently working for an online firm which provides the services of tuition teacher. He specializes in search engine marketing and online reputation management, having managed online marketing campaigns for clients from large enterprises to small businesses.

PROTECT YOUR BUSINESS WITH LAYERS OF DEFENSE

DEFENDING YOU NETWORK FROM MALICIOUS ATTACKS TAKES MORE THAN A PLATFORM'S NATIVE SECURITY FEATURES

by Troy Gill, Senior Security Analyst, AppRiver

Businesses flock to the cloud. As they do, they often forget to maintain a firm security posture and in turn expose themselves to attacks that could cripple their organization.

Take Office 365 for example. The platform has spam filtering, but users should be weary of putting all of their cyber faith in just one filter. While native filtering may be enough to keep some of the distracting and annoying barrage of spam in check, there are other areas where it may fall short.

As the bad guys are getting smarter at tricking users, phishing attacks and malicious email are getting more sophisticated and nuanced. Those who consider security as an afterthought can be exposed to problems that an innovative security company would catch. Now with all of the sophisticated techniques hackers are employing, users cannot rely on native filtering alone to secure them against today's advanced phishing and malware attacks.

Ransomware is one of the many modern threats we are all faced with, and it is one that can cause major operational and financial hardships. Businesses as well as public entities such as local and state government agencies are being held captive to ransomware attacks with un-nerving frequency. Many companies have learned that a robust backup system is no longer optional, it is a must. And with many different strains of ransomware in circulation and many more popping up on a consistent basis, organizations should take every precaution possible to prevent this threat. Because email is the most prevalent infection vector for ransomware, preventative measures should be focused there first and foremost.

The same level of attention should also be given to the web gateway as well since it is another popular attack vector. Organizations will want to be careful not to overlook the low-hanging fruit such as practicing the principle of least privilege and making sure all software and operating systems are kept up to date. These measures can help mitigate risk with ransomware and also the many other forms of malware (including file-less attacks) that are abound these days.

Along with the increase in malware, we also are seeing a big increase in phishing activity. **Business Email Compromise** or BEC has become an over-the-counter name because of its prevalence and, unfortunately, its successfulness for the perpetrators.

BEC attacks started picking up in October 2015 and have been gaining steam since. Estimates place anticipated losses well into the billions in 2018. These phishing-based attacks often use very clever social engineering to dupe unsuspecting users into paying a phony invoice or making a wire transfer at the request of the attacker masquerading as a company executive. The wealth of information about company employees available online (through websites and social media) has given the attackers a larger toolset to be able to craft these attacks in a much more personalized and convincing manner.

These type of attacks routinely net the attacker anywhere from tens of thousands to hundreds of thousands of dollars per attack. While some companies have been lucky enough to realize what happened in time to contact their bank and claw back the funds, that is often NOT the case, and the losses can be quite devastating. Everyone should take extra precautions with wire transfer payment practices and institute two-factor authentication as a matter of policy. And, of course, make sure that your email security provider has taken specific proactive measures to combat these types of attacks.

Another disturbing trend in 2018 has been the continued rise of attacks being launched from legitimate but compromised email accounts.

A popular type of attack that we have been seeing with increased frequency is **Conversation Hijacking Attacks** or CHAs. This begins with the attackers gathering login credentials for whatever email providers they can - Office 365, Gmail and Yahoo are all frequent targets. Once the hackers have access to the user's email account the attacker uses "REPLY" to a prior ongoing email conversation and adds the malware file of their choice.

The attacker usually includes some vague language such as: "Can you review this document?" – the malware attached is most often in the form of a macro-embedded word document. To the recipient being targeted, the message comes quite naturally as they were just having a back-and-forth exchange with an individual they likely know and trust. Though most users know they should be highly skeptical of an attachment in an unsolicited email, this scenario looks to disarm the "user awareness" aspect of security. What's more, these attacks can be launched against contacts within the same domain which could have equally devastating results.

In today's age of targeted attacks, one thing is certain — these attacks are here to stay and will present even more of a threat going forward.

The threat landscape is in a state of constant transformation. Make sure that your security providers are paying attention around the clock and adapting quickly to the ever-changing threats. For sure, attackers will continue to find more innovative and rewarding ways to make quick and sizeable profits – just don't let it be at the expense of your organization!

About the Author

Troy Gill, Manager of Security Research - Senior Security Analyst at AppRiver.

Troy is primarily responsible for evaluating security controls and identifying potential risks.

He provides advice, research support, project management services, and information security expertise to assist in designing security solutions for new and existing applications.

Troy can be reached online at https://www.linkedin.com/in/trgill/ or https://www.appriver.com/

HOW DECEPTION TECHNOLOGY HELPS CIOS MEET THE CHALLENGES OF CYBER SECURITY

by Nahim Fazal, BAL - Cyber Threat Intelligence, CounterCraft

World War II. Intense tank battles are taking place in North Africa and Allied forces are pitched against the might of Rommel and his formidable German tank divisions. It is a battle that is being lost due to the superior equipment that the Germans posed and the Allied command needed to introduce a new tactic to help them even up the battlefield. They turned to deception. The Allied powers started to make extensive use of agents to encourage the Germans to believe that attacks would take place at certain times and places. They never did. This tactic proved extremely useful in exposing chinks in the Germans' armor, as well as their techniques to deploy tank formations. It didn't end there. The most extensive phase of the deception program came in 1942 when the Allies managed to deceive the Germans about troop movement and location. The deception was multi-layered, involving radio signals, agents, and the deployment of fake infrastructure. This was done to combat German aerial reconnaissance. The deception campaign convinced Rommel that the Allies were going to concentrate their attacks in the north, when in fact the attack came in the south.

What the battle demonstrated is the capacity and complexity of a successful deception campaign. However, some tend to reduce it to nothing more than a simple honeypot. Deception is not to be dismissed, and to be truly effective, it needs to be multifaceted and multi-layered, just as it was against Rommel and his forces. The battle of El Alamein demonstrates just how powerful deception can be in manipulating an adversary into revealing his tools, techniques and procedures, ultimately delivering intelligence that can be acted upon to frustrate and defeat a threat. The concept of deception and how it can be used to strengthen defenses and identify internal and external threat actors is relatively new. In this article, I will demonstrate how CISOs and their security teams can use it to significantly increase their ability to identify and deflect potential attackers. This is not just about security; organizations spanning every sector are currently embarking on ambitious digital transformation programs. In the first instance, the foundations for successful transformation require consumers to trust organizations with their data, and in order to ensure this, robust frameworks are being introduced to enforce this. You don't need reminding the recent entry into force of EU GDPR (General Data Protection Regulation). But let us take a step back and examine where we are today when it comes to network intrusion and detection.

DATA BREACHES

There is no escaping the fact that the frequency and impact of newsworthy data breaches is on the up. Reflecting on some of the big breaches reported so far in 2018, the list is littered with well-known brands such as Verizon, Uber, Deloitte, Equifax or Dun & Bradstreet. In each case, it was customer information that the threat actors sought, found and extracted, affecting millions of end users. What this demonstrates is that the current technology sets deployed to prevent data breaches are simply not able to do so. Unsurprising, when we factor in the ever-evolving threat landscape, the diversity of the threats, and the budgetary and resource constraints that most organizations face. The costs associated with data breaches are staggering. Aside from any liability that may have existed under GDPR had it been in force, this figure alone should be a compelling reason for organizations to examine alternative and more advanced technology to help minimize the risk of incurring the financial loss and reputational damage that come with a data breach.

CHALLENGES

So, the first key problem that CISOs face is how to effectively defend their network parameters, that in 2018, are probably a complex mix of multiple different technology stacks, and likely distributed across the globe. This scenario alone makes the job of a SOC team infinitely more complex. Factor in the number of existing security tools that are firing of alerts on a regular basis, and the task of identifying real APT or zero-day threats becomes almost impossible. These types of sophisticated attacks have the ability to silently slip under the radar of existing network security measures and go undetected. And external threats represent just one aspect of the challenge; we must consider the additional risk of insider threats too. There will be employees with detailed knowledge of the corporate network and where critical data assets are located within this network. Their behavior wouldn't trigger any legacy security tool sets because it would fall within the normal range of expected behavior. The 2017 Verizon Data Breach Investigations Report identified a 75:25 split between breaches carried out by external perpetrators and internal threat actors, for those included in the study.

Some organizations have resorted to using threat intelligence in an attempt to become better informed and better equipped to identify the vast array of threats out there. The problem with this, however, is the poor quality and generic nature of the threat intelligence collected, that together render it very difficult to act upon. This is where distributed cyber deception platforms offer value.

To summarize, the key pain points for CISOs are:

1. The inability to detect corporate network breaches in a timely manner
2. Effectively detecting the insider threat
3. The inability to detect advanced attack techniques that leverage APT and zero-day threats
4. Too many false positives associated with current technology
5. Regulatory demands for effective breach detection and investigation
6. Targeted, client-specific threat intelligence
7. Equipping the SOC team with the tools they need to be more efficient
8. Missed alerts

With each pain point identified above, there is an associated cost and the potential for a data breach running into hundreds of millions of dollars. These issues simply can't be ignored. At board level, leadership teams increasingly expect to see a cohesive strategy that details how the risk of regulatory fines and costs associated with data breaches will be managed effectively.

DECEPTION TECHNOLOGY

It must be said that not all deception technology is equal. There are many different approaches to the steps required to identify threat actors, and through the use of deception, prevent a breach by moving them out of the production environment and into the deception platform. CISOs should look for some, if not all of the following characteristics (please note this is a starting point rather than an exhaustive list).

EVENT MANAGEMENT & ALERTING

The deception platform should produce zero false positives; therefore, the event alerting should be concise, clear and feature-rich. This means detailed intelligence on what triggered the alert, who triggered the alert, and the ability to track the source of the alert right through all of the deployed deception assets. Attack graphs are particularly useful to SOC analysts in this instance, that help to address missed alerts and the volume of false positives generated.

AUTOMATED COMPLEX DEFENSE RESPONSES

To effectively reduce the workload for the SOC team, the deception technology should include automated functionality. Automation allows the deception environment to be manipulated in response to the attacker's actions. This targeted intelligence informs incident response processes with the level of sophistication needed to save time, money and resource. Consequently, the SOC team is empowered to operate more efficiently, their time freed up to focus on real threats targeting the wider network.

COMPLEX RANGE OF DECEPTION HOSTS

In order to effectively identify threat attackers within your network and keep them engaged in the deception environment, the deception platform must be capable of deploying a diverse and rich range of deception hosts. Fully functional operating systems covering both Windows and Linux should be a baseline requirement to support this. In addition, routers, Wi-Fi access points and even mobile devices should all be considered for use as deception assets.

Remember that the richer and more complex the deception environment, the more likely you are to root out not only external threats, but those that lay inside your network too. But it should not stop there. One of the final key points identified earlier was the lack of client-specific intelligence. You need to know who is attacking, how are they attacking, and what data sets are they after - if that is in fact what they want. This means any deception technology should be able to deploy external deception campaigns in order to collect detailed information on what comprises the threat actors targeting your organization. You cannot create a cohesive security strategy unless you can answer some basic questions; am I being targeted by low level threat actors relying on third party tools and automation, or am I in fact being attacked by APTs using bespoke toolkits and crafted malware?

CONCLUSIONS

CISOs should be actively researching deception technology during the course of 2018. The rationale behind this a powerful mix of regulatory guidelines and the increasing probability of attackers breaching your network.

There are significant business benefits to be leveraged through the use of such technology, including, but not limited to;

1. Faster detection of threats at a lower cost
2. Enhanced detection of advanced threats
3. Collecting specific threat intelligence on if and how you are being targeted
4. Developing a cohesive security strategy based on objective data sets
5. Reducing false positives and not missing alerts
6. Reducing the overall the cost of detection
7. Potential to reduce your overall security spend
8. Delivering rigorous management information on how effectively the cyber risks are addressed

Ultimately for a CISO, a deception platform will vastly reduce the probability of your organisation suffering a data breach, regardless of the source. It will provide you with informed data analytics that quantify and qualify your risk exposure to threat actors, and provide you with detailed intelligence on which attack surfaces and tools might be used to target your organisation. These data sets will not only inform where you should be focusing your limited security resources, but also demonstrate to the board how effectively managing cyber risk, and what you're doing to improve your organisation's overall security posture.

About the Author

Nahim Fazal is the Business Area Lead - Cyber Threat Intelligence of CounterCraft. He has over 12 years developing and delivering innovative cyber threat solutions, having honed his cyber threat intelligence skillset within multinational financial services organizations including RBS and HBOS. At CounterCraft he is responsible for aligning the cyber deception platform with the unique needs of a broad range of industry verticals across the globe. Nahim can be reached online at LinkedIn and at our company website https://www.countercraft.eu/

HOW TO ENSURE SHARED RESPONSIBILITY FOR INTERNET SECURITY

Today, we discuss something that's relevant in today's context-shared responsibility as regards internet security.

Today we have systems and devices, plus many online activities that we share with those close to us. It could be a couple sharing a system or devices and connected activities; it could even be two or three roommates who do such a kind of sharing. In such a situation, one among two people sharing system or devices could be less careful, less cyber-savvy as regards online behavior.

The result could be damaging; there could be data exposure or device damage or money loss, which could affect the other, more careful partner as well.

A recent study conducted by Kaspersky Lab says that 82 percent of people who are in a relationship share a device with their partner. 77% of those in a relationship share online accounts, which would include social networks, banking accounts etc. While this helps improve relationships, this also leads to certain issues.

The Kaspersky study says that 90 percent of people sharing a device tend to behave insecurely, like using the same password for multiple accounts, connecting to an unsafe WiFi network, downloading files from unknown websites or leaving a device unattended in public.

45 percent of the respondents covered in the survey feel vulnerable to cyber threats, especially owing to the actions of their less cyber-savvy partner.

28 percent have encountered problems on their devices and online accounts since they had been sharing them with their less cyber-savvy partner.

The Kaspersky study points out that among the issues that shared devices cause, the prominent ones are those caused by cyber threats.

Devices get infected with malware and people also lose their money. Another interesting finding is that it also leads to arguments and fights between couples.

There are certain things that could help sort these kinds of issues. Let's discuss those, one by one…

- The day you decide to share your device or accounts, discuss and then set ground rules about device usage. There should be clarity as regards the time each partner would spend on a device and also regarding the usage of any accounts associated with it.
- Once rules are finalized, make sure the partners stick to the rules. There should be no over usage or inappropriate usage, which could directly affect the relationship.
- If you need any help, ask for it. If your partner needs any help, provide it with all promptness.
- If you don't have sufficient knowledge about internet security and online threats, ask your partner and make sure you do all that's needed to keep the device and accounts secure.
- Make sure you have a strong and separate password for each online account.
- Exercise caution while entering account details on any website (make sure the website is safe), while connecting to a Wi-Fi network, while downloading files from websites and while clicking on any link (never click suspicious links).
- Always use the necessary security software to secure your device and also to secure your online activities. Always go for a multifunctional, multi-device security solution from a trusted provider.

About the Author

Julia Sowells is a security geek with almost 5+ years of experience, writes on various topics pertaining to network security.

THE IMPACT OF USABILITY ON PHISHING

PREVENTION EFFECTIVENESS - THE PHISHING THREAT

by Andrew B. Goldberg, Chief Scientist, Inky Phish Fence

Phishing emails can take many forms; from massive email blasts valuing quantity over quality, to spear phishing and Business Email Compromise (BEC) attacks custom-tailored to maximize probability of success. Regardless of form, all phishing emails are designed to trick the recipient into taking some action that hurts them or benefits the attacker.

Phishing is currently a massive threat, and growing larger. According to Symantec, over half of all emails are spam and IBM claims that the number of spam emails increased 4x in 2016. In 2016, 1 in every 131 emails contained malware and over two-thirds of installed malware was delivered via email attachments.

While the phishing threat is a well-known, and common focus of cyber security training, phishing attacks are still very effective. On average, 30% of phishing emails are opened by their intended recipient, and 12% of recipients will click on a malicious link or open a malicious attachment from a phishing email. As a result, an estimated 95% of successful cyber attacks targeting enterprises start as a spear phishing email.

The potential business impact of clicking on a phishing email can be significant. Obviously, phishing emails can be a vector for malware infections or a source of data loss, but financial and regulatory risks are also potential concerns. On average, a successful phishing attack costs an organization 1.6 million USD, which is a pretty big hit to take just because someone clicked a link or opened an attachment. With the introduction of the General Data Protection Regulation (GDPR) in Europe, the impact of a data breach has increased with stiff penalties for the loss of sensitive customer or employee data.

With all of the available cyber security training out there, it seems like phishing emails should no longer be an issue. The majority of phishing emails rely on commonly known attack vectors like malicious links and attachments containing malware. These types of attacks can be easily prevented by users willing to take the time to carefully inspect each link and attachment before clicking or downloading. However, no one has the time to put this amount of effort into each and every email that they receive. Here, we'll talk about the tradeoffs between usability and security in preventing phishing attacks, and how anti-phishing software can be designed to improve security without harming usability.

USABILITY AND PHISHING PREVENTION

Usability is commonly considered to be the enemy of security. In general, being secure means taking extra steps to avoid falling for different attacks. This takes time and effort which could otherwise be spent on other tasks. This is especially true of phishing where the best ways to prevent against most phishing attacks are commonly known, but cyber security guidance is rarely followed. This is because the sheer volume of emails that the average person receives in a day means that dealing with each one properly would take up a significant amount of time that could be used to actually do one's job.

In this section, we'll discuss the results of human factors and usability studies. Each one has a direct impact on phishing prevention, and can be used to design more effective and efficient anti-phishing software.

MENTAL MODELS

Everyone has a way they view the world and their own preconceptions about "how the world works". In general, it's easier to make decisions that fit with our worldviews. Since generally employees are busy and tired, this means that when they are faced with a decision, they're unlikely to think it through and more likely to just "go with their gut".

This can have a serious impact on cyber security in general and phishing in particular. Phishing emails are specifically designed to look as legitimate as possible. This means that by default, most people will believe them and click on malicious links or download infected attachments. Most anti-phishing training is focused on getting people to take the steps necessary to protect themselves against phishing attacks (verifying senders and links, not enabling macros on documents, etc.). However, since this takes time and effort (which employees have in short supply), phishing is still an effective strategy for attackers. A key aspect to a phishing protection strategy is destroying the appearance of legitimacy of phishing emails (through warnings, etc.) so that users make the correct decision by default.

FITTS'S LAW

Fitts's Law is a scientific law based on the study of human movement. It states that the time it takes for a human to move to a given target is proportional to the distance to the target (from the starting location) and the width of the target. For example, it may take roughly equal time to accurately touch a narrow, near target and a wide, far target but it will take longer to pinpoint a narrow, far target. This has been demonstrated to be true for both hand and eye movements.

Fitts's Law is directly applicable to usability in general, and cyber security usability in particular. Since anti-phishing protection software isn't perfect (some legitimate emails look a lot like spam and vice versa), the use of warning banners and reporting buttons are common anti-phishing techniques. Based on Fitts's Law, these banners and buttons should be sized and placed to minimize the effort required for a user to read or click on them.

EYE-TRACKING SCANNING PATTERNS

Eye tracking is a common area of research in usability and ergonomics research. Everyone wants to know how people instinctively look at a page so that content can be placed for maximum impact. Based on this research, several common scanning patterns have been identified.

The F-shaped scanning pattern is a common one for web content. Users typically read the first few lines of an article, a line or so further down, and skim down the left side of the page. The read sections form the shape of the letter F (hence its name). Other common patterns include layer-cake (reading only headings), spotted (skimming the page briefly looking for links, bold, etc.), and committed (reading all content on a page).

Knowledge of scanning patterns is useful for improving usability for anti-phishing products because it helps to determine the optimal place to put warnings and other informative content. In general, most scanning patterns involve reading the top of the page (which is why warning banners are commonly placed there). Differentiating warnings and reporting buttons by size, color, bolding, etc. improves the probability that they will be noticed by users. In phishing, where a single click can cost a company millions, improving the visibility of banners by any possible means is important.

IMPROVING PHISHING PROTECTION THROUGH INCREASED USABILITY

Usability is commonly considered to be in direct conflict with security. The only truly secure computer is one that's unplugged and locked in a vault somewhere with the key thrown away. And, even then, there is still the possibility of safecrackers or tunneling. Regardless, you can't achieve perfect security without rendering a system unusable, which means that some tradeoffs must be made to achieve a balance where a machine is capable of doing its job in an acceptably efficient manner while not decreasing security any more than is strictly necessary.

Protection against phishing emails is one of the most well-known areas where usability has to be weighed against security. Most phishing attacks are based on commonly

known methods that can be defeated with a little bit of effort from the recipient. For example, malicious links don't work if the recipient visits the target site directly (either by typing in the URL or finding it via a web search engine) and then navigates to the relevant page using internal links on the site. However, most people don't want to take the time and effort to do this for every email, so standard phishing attacks remain effective.

Effective anti-phishing software will provide increased protection to users without negatively impacting the usability of their email. It is not uncommon for people to receive hundreds of emails in a day, so even small delays add up. In this section, we'll discuss a few ways that anti-phishing software can improve security without negatively impacting user productivity.

PAINLESS PHISHING REPORTING

When an end user identifies a potential phishing email, their default response is to ignore or delete it and move on with their day. By identifying the potential threat and avoiding it, they protect their organization against the attack with minimal disruption to their workflow.

However, while it is good that a particular user is sufficiently well-trained, vigilant, and paranoid to identify and respond to the potential threat, the same may not be true of all potential targets within the organization. To reach the target's Inbox, the phishing email needed to evade all of the organization's defenses and may have reached the Inboxes of other members of the organization.

In order for an organization's network security team to respond properly to the threat, they need to be aware of it. Someone needs to report the phishing email and quickly. According to a study by Verizon, the average time between a phishing attack's launch and the first person clicking on a malicious link within the phishing email is only 82 seconds. The sooner that the network security team can respond to a threat, the better an organization's chances of mitigating it before damage is done.

In order to convince end users to report, rather than simply deleting phishing emails, it is key that reporting be quick and easy. Including an obvious "Report Phishing" button or link within an email or email client that takes care of forwarding the email to the security team and deleting it from the user's Inbox is a great solution. It's important to take into account Fitts's Law mentioned above: the button should be placed and sized so that reporting an email does not require any more time or effort than deletion or marking as spam. By making reporting as easy as deleting, an organization can improve its protections against phishing attacks.

INFORMATIVE THREAT BANNERS

A banner across the top of an email indicating that the email is suspicious is a common method of protecting against phishing attacks. However, how effective is a generic banner that is attached to any email regardless of the suspected threat type and threat level?

As mentioned above, it is more difficult for humans to make decisions that are in conflict with their view of "how the world works". If an email is obviously spam, a warning banner makes sense to the user for that email since, in their world, this email is suspicious and should be marked as such. Over time, their worldview includes the fact that their anti-phishing program distrusts certain emails based on certain attributes like embedded links. Since the program only tells them something that they already know (that a spam email is suspicious) and nothing more, the warning become background noise.

However, if an email is a well-crafted phishing or spear phishing attack, the target is more likely to believe in the authenticity of the email. If they've grown accustomed to ignoring warnings since they only appear on obvious spam (and possibly wrongly on legitimate emails), they're more likely to dismiss the warning as their anti-phishing program being overzealous and making another mistake.

In order for anti-phishing warnings to be effective, they need to resist users becoming desensitized to them. The best way to accomplish this is to design them so that they provide useful information to the user, and reduce the cognitive load of trying to determine whether or not an email should be trusted. Rather than just saying that an email is suspicious, an anti-phishing program should tell the user why that label is applied and provide enough information for the user to make a decision on their own. If an email contains malicious links, the program should say so, and warn the user not to click on them.

If an email looks like a Business Email Compromise (BEC) attack, explain what a BEC attack is and why this email looks like one. Rather than acting as an oracle labeling emails as malicious or not, an anti-phishing program should provide users with the information to make the decision whether or not to trust on their own. These banners should also be placed in a way that maximizes the probability that the user will see them while just scanning the page (based on the human factors research presented earlier).

TRANSPARENT PROTECTION

One of the primary threats with phishing emails are malicious links. It is not uncommon for phishers to take a legitimate email from a company and then change the links from the legitimate site to a site under their control. Since all visible parts of the email are legitimate, the look and feel of the email matches the recipient's expectations of an email from that company and they are more likely to accept it as fact. An untrained user would be very likely to click on the links or buttons in the email.

Checking the validity of links within emails is a central part of most anti-phishing training. Using mouse pointer hovering, a user can confirm that a link's target is in-line with their expectations, i.e. a link pointing to a web page under a domain belonging to the message sender. Phishers know this and take advantage of the fact that the recipient is likely in a hurry and not scrutinizing links carefully (if at all). By registering similar-looking, like arnerica.com instead of america.com, or plausible, like company-customercare.com, domains, phishers can increase the probability that a malicious link will be accepted as legitimate.

Common cyber security guidance for dealing with malicious links is for recipients to visit the supposed sender's legitimate site (by typing in the URL or using a web search engine) and then navigate to the target webpage using internal links on the site. However, this is time-consuming and most people will just click the link if it looks good to them.

One way that anti-phishing programs can improve security without impacting usability is to make protection against malicious links transparent to the user. Using fuzzy string matching against domains known to be targeted by phishing and contextual clues from the email or a URL blacklist, a program can determine if a domain is not legitimate. An inline anti-phishing solution can then rewrite the malicious URL to the benign equivalent and guarantee that a user's click will not take them to a phisher's site. By testing both at time of receipt of the email and time of opening, the program can use the most updated information and provide real-time protection.

CHOOSING USABLE PHISHING PROTECTION

The main takeaway of this article is that users are efficient (i.e. lazy) and are prone to falling for phishing schemes because phishers take advantage of this fact. Most phishing attacks are based on techniques with a known defense; however, properly defending against phishing takes time and effort, which can be used on other things. The key to effectively protecting against phishing attacks is making doing the "right" thing easier than doing the "wrong" thing.

In this article, we discussed usability research and how it relates to protecting against phishing attacks. Humans are predictable (a fact that phishers take advantage of) and anti-phishing products can take advantage of this fact to improve their protections. By designing warning banners and reporting links to maximize visibility and usability, an effective anti-phishing solution can improve the level of protection that it offers.

Beyond suggestions based on usability research, three concrete methods of providing highly usable phishing protection were also addressed. In order to maximize protection against phishing attacks, it is important to choose a phishing protection product that provides all of this functionality. By removing as much of the burden as possible from the user, effective anti-phishing software increases an organization's security and the efficiency of its users.

About the Author

Andrew B. Goldberg , Chief Scientist at Inky Phish Fence.

He is leading development at Inky, an enterprise communications security platform, working to protect corporate email from new breeds of sophisticated phishing attacks.

Andrew can be reached online at @inkymail, and at our company website https://www.inky.com

ONE IN FIVE ANDROID APPS HAVE NUMEROUS KNOWN SECURITY FLAWS

by Tae Jin "TJ" Kang, CEO, Insignary, Inc.

Study Finds One in Five of 700 Most Popular Android Apps Have Numerous Known Open Source Security Vulnerabilities

IDC estimates that Google's Android operating system has an 85% market share, while Apple's iOS declined by almost four percent. Paid apps, subscriptions and in-app purchases through Google Play Store are estimated to have reached $20.1 billion in 2017, a 34% increase. While Apple's App Store saw a slightly larger increase in growth, and had almost double Google Play's revenue, it is Android apps that are used by the majority of mobile device users.

There has been a great deal of speculation regarding the quality of apps developed and sold for the both the iOS and Android platforms. More than 90% of the software developed and in use today contains open source components. This is interesting because the number of known security vulnerabilities reported through the Common Vulnerability Exposures (CVE) database shows that 2017 was a record year, with more than 14,700 reported. We should also note that reported vulnerabilities for 2018, are on a pace to beat last year's milestone.

KNOWN SECURITY VULNERABILITIES ARE LOW HANGING FRUIT FOR HACKERS

Whether software code is proprietary or open source, it harbors security vulnerabilities. Because of its transparency, open source code tends be better engineered than a comparable piece of proprietary code. And thanks to its flexibility, open source code is extensively used. This means that a security vulnerability in a piece of open source code is likely to exist across a multitude of applications and platforms. Consequently, open source software vulnerabilities become a "low hanging fruit" for hackers to target and attack.

While updated versions of open source components are available without security vulnerabilities, in-house software development teams and third-party developers are hard-pressed to effectively track all open source software components in their internally developed and externally sourced code.

BINARIES DO NOT LIE

In order to determine how "secure" mobile apps are, our R&D team sought a proxy. It was determined that the binary code – the exact software downloaded and installed on Android smartphones and tablets – would be examined for open source software components known to harbor known security vulnerabilities. The binaries were chosen because they are the actual code being "shipped" and while software vendors and third-party developers might have an idea about what open source code elements are in their source code, a binary file does not lie.

ABOUT THE STUDY

During the first week in April of 2018, our research and development team scanned the APK files of the 700 most popular apps by downloads on the Google Play Store. The team selected the 20 most popular apps in each of the 35 main Android app categories, including "Games," "Productivity," "Social," "Entertainment" and "Education," among others.

Following are some of the key findings:

- The binary scans indicate that the Android apps available on Google Play Store by the top software vendors contain versions of open source components that are known to contain known security vulnerabilities. Out of the 700 APK files scanned, 136 contain open source software components known to harbor known security vulnerabilities.
- 57% of the APK files with reported security vulnerabilities contain vulnerabilities that are ranked as "Severity High," meaning that the deployed software updates remain vulnerable to potential security threats.
- 86 out of the 136 APK files with security vulnerabilities contain vulnerabilities associated with openssl.
- 58 out of the 136 APK files with security vulnerabilities contain vulnerabilities associated with ffmpeg and libpng. The prevalence of these open source components can be attributed to the abundance of images and videos in mobile applications.
- Interestingly, three of the APK files scanned contain over five binaries with security vulnerabilities. The majority of APK files with vulnerabilities contain one-to-three binaries with security vulnerabilities.
- 70% out of the top 20 apps in the "Games" category contain security vulnerabilities.
- 30% out of the top 20 apps in the "Sports" category contain security vulnerabilities.
- This study demonstrates that 1 in 5 APK files does not utilize the correct, most up-to-date versions of the OSS components available.

In the majority of cases, the open source community has created new versions of the components to address nearly all discovered security vulnerabilities. Software developers and vendors can employ these versions to prevent data breaches and subsequent litigations that can cause significant corporate losses. Interestingly, during discussions with various vendors, Insignary encountered a few developers who expressed a preference in manually applying patches, line by line.

Though this ad hoc approach to addressing vulnerabilities may be used by others, it appears to be the exception, rather than the rule. Additionally, while this method may work, it is still recommended that Android app developers scan their binaries to ensure that they catch and address all known security vulnerabilities.

Our findings suggest two possibilities for the failure to use the correct component version by Android app developers. Either they are not aware of the open source software vulnerability issues, or they do not have a process or a tool that accurately finds and reports open source components that are known to contain security vulnerabilities.

The market for smartphone and tablet apps appears to be on a steadfast trajectory. However, if apps vendors are unable to employ the latest, vulnerability-free OSS versions in their firmware, the possibility of data theft and business disruption could be significantly debilitating. We encourage all apps vendors to redouble their efforts to patch known security vulnerabilities. We encourage the app stores to make stronger efforts to ensure that the apps they sell are less hacker-friendly. Finally, we suggest consumers seek to leverage sites or services like – like no-cost TruthIsIntheBinary.com – that allow them to test the apps they are considering or purchasing, for components that are known to have known security vulnerabilities, prior to installing them on their mobile devices.

About the Author

Tae Jin "TJ" Kang is a technology industry executive and entrepreneur. He is the president and CEO of Insignary. In addition to founding a number successful technology startups, Mr. Kang has held senior management positions with global technology leaders that include Korea Telecom and Samsung Electronics, among others.

Mr. Kang can be reached online at tjkang@insignary.com and at our company website www.insignary.com

HOW ARTIFICIAL INTELLIGENCE BASED MACHINE LEARNING WILL AFFECT IT SECURITY

By: Rabih Itani, Regional Business Development Manager - Security, Middle East and Turkey at Aruba, a Hewlett Packard Enterprise company

Artificial Intelligence (AI) has been a hot topic of discussion in many industries for a while now, with healthcare, retail and hospitality, to name but a few, starting to speculate on the massive opportunities its development could bring to how their business is run, and how customers interact with those businesses. Many articles are already predicting the demise of human workers as a result of AI making inroads into our lives because we are on the verge of true artificial intelligence. But when it comes to the biggest challenges facing business, these technologies are yet to have their big breakthrough. This may all change as we progress into this information age, and for me, the first proof point will be IT security. Having grown into one of our biggest international threats of 2018 with attacks spanning the globe and affecting every country including Middle East ones, a new defense is being developed that will allow companies to tackle the latest threats as soon as they appear on the network. This new defense is based on machine learning, a key component of a security framework that can move as quickly as those who are looking to breach the network. Machine learning is a fundamental part of an AI system. Machine learning enables AI to detect patterns in all sorts of data sources and create behaviors based on recognized patterns.

HOW DOES MACHINE LEARNING IMPROVE SECURITY?

IT teams today are faced with a moving security target. From the devices used by employees to do work, to the locations, we work in and the people, we send data to, our activities change day by day. It is important to understand, keep up with and protect against these moving goalposts.

As is clear nowadays, security is number one on the agenda for CIOs around the world, as they move to protect their organizations against the malevolent attackers who are looking to breach the network and, typically, steal personal data. This can be a tall order for most IT staff that cannot predict the subtle changes that might take place within their network day to day. These could include hundreds of new devices signing up to the network, from employee-owned mobile phones to older temperate sensors, newly connected as part of an IoT strategy.

The scale of the challenge is often just too vast when asking human IT teams to manage the data being shared by incoming and existing devices, which can easily reach into the thousands for a large enterprise. This is where machine learning comes

into its own. Using machine learning for UEBA (user entity and behavioral analytics), IT managers can create standard profiles for each device on the network. Sales managers get access to Salesforce anytime anywhere, finance teams get access to Financial Information Systems using specific devices at specific locations, and so on. The profile of each user becomes quickly personalized, and as soon as a user or entity behaves in a way that strays outside of their profile, the machine sees it, and raises the risk score of that user or entity and may accordingly send an alert, which in many cases will require the user/entity to re-authenticate. In the case of a malevolent attack, the intruder will be isolated from the rest of the network, to limit any potential damage that might have occurred.

Machines are capable of analyzing millions of individual packets of data plus thousands of system logs and possibly business context data (such as HR records), making a truly individual approach to security possible, which is more than can be said for the ability of a human IT team. With the machine doing the brunt of the monitoring work within the network, the human agent need not intervene until an entity risk score gets above threshold. This automatic monitoring offers IT staff exceptional time savings, which means they can get on with tackling other IT issues throughout the organization.

SECURITY'S POSITIVE IMPACT ON THE WORKFORCE

With AI based machine learning introduced in the workplace, security teams stand to benefit greatly. The technology isn't here to replace the human element in security operations; it will augment the human's intelligence, allowing staff to make better decisions based on the quality of the actions being proposed and the forensics data being furnished. Permissions, for instance, won't be automated by artificial intelligence; it will flag the request to a human agent, who can use the information gathered, and knowledge of the actor, to make an informed decision. These developments could ultimately change the range of jobs on offer within IT security. Security staff will move from being the operational proponent within the network, to making the decisions that could determine the security of the network. On the other hand, the Security Manager might become the Policy Manager, determining the various policies and credentials necessary to access business networks.

Whilst the approaches of human workers might change during the course of the roll-out of this technology throughout enterprises, their work will be no less important. They will still need to build security into the core of the network, regardless of the technology already in place. As the world moves into a state of 'data as commodity', the network is still the most important infrastructure to maintain and keep safe as it is the first line of defense. It's time to start thinking about these developments as they become more prevalent because human IT staff need all the help they can get when combatting increasingly intelligent threats.

BEING PREPARED TO KEEP YOUR E-COMMERCE STORE'S DATA SAFE

The recent cases of data breach and cyberattack are clear signs of a growing need for better information security. It is no longer acceptable for businesses to take data security lightly, especially when you take customers' data and other sensitive information into the equation. The security measures available are advancing too, but the final decision still lies with businesses and entities storing sensitive data.

E-commerce sites have been the target of cyber attacks for obvious reasons. Aside from customers' personal information, many e-commerce sites also store credit card information – or tokenized versions of the customers' cards – and these are valuable for attackers. If you run an e-commerce store, it is important that you know how to be prepared to keep your data safe at all times.

SSL SECURITY AS A FOUNDATION

One of the first things you need to do when starting an e-commerce site is adding Secure Sockets Layer or SSL security. SSL provides the necessary protection for data transmissions to and from the server. With an SSL certificate in place, all data transmissions can be encrypted, which means communications between the server and customers' browsers are fully protected.

Of course, SSL security is only one part of a very complex set security measures. With SSL security implemented first, however, e-commerce sites can also grow their credibility and start developing customers' trust early on. After all, customers will only complete their transactions when they see a verifiable SSL certificate appearing on the corner of the address bar.

SECURITY COMPLIANCE AS A STANDARD

The next step of securing your e-commerce site is meeting the security standards required by different entities. For sites that process payments on-site, for instance, PCI-DSS compliance is a requirement that needs to be met. The PCI compliance requires additional security measures to be put in place to further prevent different types of cyber attacks.

Live address verification is a good example of how most attacks can be prevented with the right security measure. Address verification alone can help e-commerce stores prevent the majority of frauds and faulty transactions, leaving only a handful to deal with. Fraudulent purchases can also be prevented using two-factor authentication supported by credit card issuers.

Other security standards are not to be ignored either. European-based e-commerce sites must now follow the General Data Protection Regulation or GDPR. The deadline for compliance is May of 2018, but businesses and e-commerce site owners are still miles away from fully adopting the security standards.

Probably, many small business owners wonder what is GDPR. The legal framework is designed to standardise data security and storage across the European Union. It applies to all sites that capture user data, including those that ask users to subscribe to their newsletters or fill out other types of forms.

CHOOSE THE RIGHT DATA TO STORE

The data and details you store also play an important role in determining the kind of security measures you have to put in place. A good approach is to avoid storing data that you don't absolutely need to store. The fewer details you have in your database, the less you have to worry about losing those details to unauthorised parties.

In the case of an e-commerce site, not all details are about the customers. Sites are starting to shy away from storing credit card details; it is usually the payment processors or gateway that stores those details, as they have much higher security standards to meet. Addresses and basic details about the customer may still be needed, but the majority of e-commerce sites don't have to go beyond that.

Instead of storing a lot of details that aren't always useful, it is actually better to focus on details that can improve the customers' experience whenever they shop on your platform. Of course, the platform itself needs to be properly secured.

A SECURE PLATFORM

Not all e-commerce platforms are created equal. Some require you to tinker with advanced settings and configure the server in a certain way to achieve maximum security. Others are designed to be secure out of the box. Both types of solutions have their own advantages and disadvantages.

The server you use is also a big part of the security equation. Unless the server is configured to offer maximum security, the thousands – if not millions – of customers' data you store in your database are always at risk. Proper backup routine, regular updates and security patches, and the way the server is configured are among the things you need to pay close attention to.

Even little details can greatly affect server security. Things like whether the SSH port (22) is left open and the way your server firewall is configured to ban IP addresses that show unusual activity are also details you want to attend to. These security measures add up.

REGULAR SECURITY AUDITS

There is one last piece of the puzzle that every e-commerce store owner needs to understand, and that is the fact that information security is not a one-time thing; it never is. Complying with security standards and having the best setup today doesn't necessarily mean you no longer have to worry about cyber attacks indefinitely. In fact, one of the primary reasons why more cyber attacks are successful these days is this type of negligence.

Information security is something you need to do regularly and continuously. This means doing regular security updates, keeping up with the latest standards, and checking for potential security holes to patch. Even standards like PCI-DSS get updated regularly.

The threats are changing too. Ransomware, for example, is a well-known type of malware that has been around for years. However, recent ransomware attacks are based on a new strain of malware. The attackers are getting smarter and updating their tricks, so you need to stay one step ahead and update your security measures too.

Be prepared, however, and you can worry less about losing your customers' data to attackers and other unauthorized parties. You know you have the best security measures in place and you can rest assured knowing that those measures, combined with your security policies, are providing the best protection for customers' data.

SYNTHETIC IDENTITY FRAUD AND SOCIAL ENGINEERING ARE GROWING CONCERNS AND ON THE RISE

By: Christina Luttrell

With customer not present identity fraud becoming an increasingly prevalent issue, major shifts in the fraud landscape have had far-reaching effects across multiple industries. Businesses are feeling the pressure to successfully fight fraud by employing greater preventative measures, while at the same time maintaining a positive experience for customers. For the past five years, the team at IDology has surveyed fraud and cybersecurity professionals across a variety of industries, enabling us to provide useful insights and report on current fraud trends. This year, our research validated a sharp rise in companies reporting an increase in fraud—a 58 percent jump over 2016, some of which can be explained by the substantial amount of high-profile breaches that have flooded the dark web with the personal identity information of millions of Americans.

This may also be attributed to the swiftly growing number of synthetic identity fraud cases, which was ranked highest by respondents as the category of fraud that their industry is least prepared for. We also discovered an increase in customer-not-present fraud, caused by the ripple effect of EMV chip adoption, which continues to push thieves to shift their focus and fraudulent activity online and away from physical point of sale retail locations. And notably as fraudulent activity is increasing, so is the need to reduce friction in customer interactions, especially onboarding new customers. Nearly half of the companies we surveyed listed a seamless, effortless user experience as a top priority and key competitive differentiator in today's marketplace.

A Closer Look:

> **Synthetic Identity Fraud**. Major breaches have provided criminals with more identity data to utilize as they constantly shift strategies to evade detection. They're using more sophisticated schemes that are harder to detect, such as synthetic identity fraud (SIF). SIF is a combination of real and fabricated information that criminals use to create a new identity, which is then used to open accounts, gain credit and then "bust out" of accounts with fraud. SIF cemented a sizable footprint in this year's survey, with 31 percent of businesses confirming its increase and 58 percent sharing that they are "extremely" or "very" worried about it. In particular, 50 percent of financial institutions reported that SIF is widely prevalent,

compared to 38 percent across all industries, making financial services the hardest hit.

Social Engineering in Call Centers. While widespread adoption of EMV chips on credit and debit cards boosted transaction security in retail POS locations, billions of dollars in counterfeit card fraud are being redirected to more vulnerable channels such as the call center. In the last 12 months, call center fraud levels increased for 40 percent of businesses surveyed.

Call centers are an ideal target, particularly for account takeover activities. Caller ID spoofing, which occurs when a fraudster calls into a contact center and appears to be calling from the victim's number makes this especially easy for criminals. By nature, customer service agents are helpful and in the business to make and keep customers happy. In doing so, they can unknowingly give up small bits of personal information that can lead to future fraud. Preying on this weakness, fraudsters attempt to trick or "socially engineer" unsuspecting agents into sharing information. This was reported as the most prevalent type of fraud by 69 percent of survey respondents.

A BALANCING ACT

IDology's Fifth Annual Fraud Report confirms that fraud is growing in prevalence, methodologies and sophistication, and challenging businesses to approach identity verification in new ways. However, increasing fraud prevention measures should not come at the expense of providing a slower or more frustrating experience for legitimate customers. In call centers, this includes preventing social engineering before it happens by employing big data innovation such as technology that accesses mobile network operating data in real time to determine the legitimacy of the caller's device and phone number. By checking the validity of the mobile number and call status in real-time, genuine customers can be greenlighted to the call center for assistance while suspect calls can be routed to fraud specialists.

The threat of synthetic identity fraud demands an intelligent, multi-layered approach that pulls together an array of location, activity, device, digital and other identity attributes to validate customers. Another key layer of defense is sharing data across industries and companies through a fraud network that gives security experts insight into trends and evolving, well-developed scams. Emerging technology and collaborative networks must continually evolve to stay ahead of fraudsters while ensuring that legitimate customers have a secure, fast and positive experience.

Christina Luttrell is the senior vice president of product, client solutions and marketing for IDology, a leader in multi-layered identity verification and fraud prevention.

WARNING SIGNS FOR MANAGING CYBER SECURITY

In 1997, the NSA attacked the Department of Defense information infrastructures and attempted to breach their network. The attack was codenamed Operation Eligible Receiver 97 and was intended to test the defense capabilities of the DoD against a cyber attack. Results from the exercise were alarming. The NSA took complete control over many of the Department of Defense information infrastructures and gained superuser access to critical systems. The exercise highlighted the unorganized and poorly governed computer infrastructures of the DoD and armed forces.

After two years of hearings and review, three recommendations were made; recommendations that cybersecurity professionals are well aware of today. These are Configuration Management, Patching Vulnerabilities, and the implementation of Controls. Though best practices were not formally codified, compliance frameworks were developed and these may be reviewed. They are Security Technical Implementation Guides (STIGs), the National Vulnerability Database (NVD), and the controls within NIST 800-53. Surprisingly, while the recommendations were made over twenty years ago, many organizations still struggle with implementing them today.

All professionals know benchmarks and accountability are a hallmark of good management. A project may not proceed until the target is formally described, processes are implemented, and milestones are validated. Unfortunately, for many professionals in the cybersecurity field, the tools and process have been developed over the years in a hodgepodge manner.

Certain beliefs and procedures are implemented because “that’s how it has always been done.” There are even occasions when milestones are merely guesses. For example, how many times have you heard the question, “What percentage of CVEs do we have patched?”, answered with, “Probably 75%.” This inability to provide consistent or accurate data creates an unmanageable cybersecurity process.

THE DEVIL IS IN THE DETAILS

While all plans start out logical, over time the complexity of implementation, requirement of changes, and opinions of others can introduce problems. This article describes a technique used by managers to notice warning signs and determine if there is a problem with their cybersecurity processes. By reviewing the metrics they receive, managers can determine the health of their group. Likewise, inconsistencies in the security metrics may be used to justify reviews or upgrades to tools and training for parts of the process. What is needed to find the warning signs? What every manager looks for: reliable, consistent, and usable data (RCU).

Reliability ensures security teams are utilizing real data. Organizations operating without real data often misunderstand their current security posture or rely on guesses. For example, an understanding of vulnerabilities can only be accomplished when there is an understanding of asset inventory and IP leases. Many organizations use DHCP servers to discover these IP leases, but this number will vary over time and is inaccurate. If a manager learns developing reliable data by his team member is difficult, they know an underlining tool or process is incomplete. With a focus on reliability, the security process becomes based on reality.

Consistent data ensures security professionals are able to view data, return at a later date, and analyze the same data. More importantly, it allows different members of the team to get the same results. If a manager determines security metrics are inconsistent, they know there is an issue with the organization and retention of data by the team. Maintaining a detailed history of changes is crucial for an accurate security ledger detailing what security risks an organization has, what procedures are in place, and ultimately reporting to the board.

Usability allows data to be used in different ways. This is the measure of the flexibility that a security team has in determining problems, forensically exploring issues, and developing a novel and unique procedure. If a manager suspects the metrics developed by their team are silo-ed, or limited in scope, they know there is an issue with team members being too regimental in their performance.

Access to actionable items that apply to multiple security functions differentiates organizations from an inefficiency where time is being spent searching through data instead of being used to remediate issues. For example, when looking at configurations, usable data clearly shows when drift has occurred along with who caused it. This allows security teams to efficiently discover who was responsible for changes and what the reasoning was. Linking data from behavioral information into usable metrics for security functions, such as configuration management, helps organizations manage cybersecurity.

THE RED FLAG OF POLICIES

Organizations will often attempt to manage cybersecurity with specific policies. These policies will cover various IT functions such as USB usage or local admin rights. Unfortunately, these policies can take on a life of their own and specific answers to the compliance of policies will be met with statements such as “We’ll have to ask IT” or “ We won't know until the next audit.”

When following the principles of RCU, answers to the coverage of policies will be nearly instantaneous. The continuous checks provided by RCU determine if specific policies are utilized rather than simply existing. A manager can quickly tell their organization is at risk if their team is more focused on whether the policy is being followed rather than if there is a policy in place.

Reliable, consistent, and usable data is important for the security process as a whole. For example, conducting an audit every six months does not follow the principles of RCU. In order to be reliable and consistent, data needs to be analyzed continuously. Security events that occurred six months ago will not be relevant or usable for security professionals. When organizations have reliable, consistent, and usable data to manage security processes, their processes become more efficient and robust.

As an example of utilizing the reliability, consistency, and usability principle to configuration management, organizations have immediate answers to questions such as:

- How are devices configured?
- How are they supposed to be configured?
- Who made changes and when did they make them?

The answers to these questions provide valuable information for not only configuration management, but for all security functions.

The recommendations from Eligible Receiver 97 are critical to any organization's security posture, but there is far more to consider before implementing a process.

The processes implemented must provide reliable, consistent and usable data so a robust and dynamic security team is supported. Managers watching for simple indicators can determine if their group is working in a productive manner.

FINDING THE WARNING SIGNS WITH ARISTOTLEINSIGHT

AristotleInsight is a big data security platform designed to implement the three principals of security metrics: Reliability, Consistency, and Usability. The Continuous Diagnostics and Monitoring platform for Configurations, Vulnerabilities, Privileged User Management, Asset Inventory, and Threat Analytics continuously provides reliable, consistent, and usable data organizations need to implement their cybersecurity process.

Utilizing the revolutionary UDAPE® technology, AristotleInsight collects reliable data from the process level across all devices on an organization's network.

A unique Bayesian Inference Engine sorts through the kernel level data to highlight actionable items that help security teams identify risk, direct the remediation process, and document results. This helps security teams save time and better manage their cybersecurity posture.

If an organization is building their security process, AristotleInsight is the perfect solution to collect data that is reliable, consistent, and usable. For organizations with a mature cybersecurity process in place, AristotleInsight is an effective hunt tool.

To learn more about AristotleInsight: Visit - www.aristotleinsight.com

Email - info@provecompliance.com Call - 866-748-5227

About the Author:

Josh Paape is an Online Marketing Specialist at Sergeant Laboratories, a leader in security and compliance solutions that allow businesses, governments, and healthcare institutions to comply with regulations and stay a step ahead of criminals. As a graduate of the University of Wisconsin - La Crosse, Josh has experience marketing products from a variety of industries. As a contributor to CDM, he hopes to spark new thought and discussion topics in the information security community.

Connect with Sergeant Laboratories: https://www.sgtlabs.com

Sergeant Laboratories Blog: https://www.aristotleinsight.com

LinkedIn: https://www.linkedin.com/company/sergeant-laboratories-inc

Twitter: @Sergeant_Labs

IOT ENVIRONMENT COMPROMISING CYBER SECURITY

IT'S HIGH TIME TO EXPLORE WHAT IOT IS OFFERING CYBER-CRIMINALS, NEED TO DEFEND.

By N Subash Reddy, Cyber Security Research Fellow, Mindmajix

Digital revolution has got its roots into every sector and is spreading till date. Automation helped every possible sector in adapting new innovations in serving their customers quick and effective. People started believing digitization will make this world a better place to live, and hence accepted every change happened with the integration of technology. Increase in the technology has made information available on the internet and this is where researchers are challenged in securing data.

IOT AND ARTIFICIAL INTELLIGENCE TODAY

As the number of internet users is increasing every day, the number of devices getting connected to each other got proportionally increased. This resulted in expecting 30 billion devices gets connected with IoT by 2020. Internet of Things (IoT) and Artificial intelligence are currently the buzzwords for every industry. IoT has improved the quality of life with its smart devices. Artificial intelligence has already proved its importance in all major business sectors like healthcare, education, automotive, agriculture, etc., to provide qualitative service. With the positive and overwhelming response to Artificial Intelligence, researches are in progress to integrate it with IoT, to make it easier in decision making for some devices (smart home appliances, self-driving cars, etc) connected in IoT.

CYBER SECURITY IN IOT

What is IoT?

Internet Of Things (IoT) is an environment that connects computer software embedded devices to get connected with each other to communicate or data exchange.

Why IoT?

IoT helps in understanding the importance of getting connected. *Can we imagine our lives without smart phones today?* Great if your answer is "Yes". But most of the people

end up with the answer “No”. The same is going to happen with many other IoT devices further, as they make our life comfortable. For example, smart refrigerator as a part IoT can help you in monitoring temperatures and adjust according to climate around, thus reducing human intervention. Next level of IoT enabled devices like Air Conditioners provides access with smart phones when connected.

Limitations of IoT

With the huge network of devices connected, providing security to all the devices can difficult which enables chance of cyber crimes. IoT not only helped many common people, but also it has got features enhancing thoughts of cybercriminals in stealing the information available.

CYBER SECURITY – CYBER ATTACKS

Cyber Security is enabling and ensuring every device that gets connected through internet/Wi-Fi/Bluetooth or any other medium has got security features installed in defending any type of unauthorized/phishing attack in the network. Device manufacturers are advised to focus on security. Recent reports claimed that there was 70% increase in cyber attacks in the year 2017 using IoT devices.

Cyber attacks registered came up with different strategies while working with IoT.

- Targeting IoT Devices:

  Criminals target IoT devices to executing malicious unwanted instructions. These criminal are good at computer and scientific knowledge to understand the execution of IoT devices and deploy code into them.
- Using IoT tools:

  Less secured devices in the IoT are chosen by cyber criminals to attack. IoT devices are used as tools and deploy botnets to execute Distributed Denial of Service (DDoS) kind of attacks on the network. Mirai botnet is an example of such attack.
- Extracting Data:

  Most of the devices in IoT have got some personal information stored. FitBits, smartphones, automated home appliances, etc., have records of your daily activities, when all the pieces of information put together reveals majority of the identity which is used by hackers in information theft.

EXAMPLES OF CYBER ATTACKS

- AI program installed on the server outside US has got its instructions to debit half-a-dollar from bank accounts, and customers in general ignore for such a small amount. Executing the same instruction for millions of time can fill hackers account. All this happens in the network without leaving any hint to the banks and customers.
- Using SWIFT network to steal 80 million dollars from Bangladesh bank.
- Petya Ransomware and NotPetya Malware.
- Email dumps prior French Presidential elections in the name of EMLEAKS.

These are very few among many cyber attacks happening around the world.

IOT AS PLATFORM FOR CYBER CRIMINALS

Bromium's recent study, there was $1.5 trillion revenue generated through Cyber Crimes. According to this research, cyber crime became professional in its executions and is considered to be self-sustaining system adapting platform capitalism model. New techniques need to be invented in combating with sophisticated attacks expected by cyber criminals further.

Other key points to be considered from the research:

- Cybercriminal platform owners make more money than their employees
- Criminal sites found using services, ratings, customer support, etc.,
- Services and products range from $200 to $30000 with different hacking/attack operations.
- Reinvesting 20% of their revenue in business development.

Another report on accelerating cyber criminal revenue states that attacks like phishing, file hijacking, ad clicker, screenshot manager, DDos made by WannaCry, ZCryptor, Petya kind cybercrime resulted in reputational, financial and downtime loss.

Cybercrime-as-a-business will be the next big challenge to defend in the world of technology.

AI'S ROLE IN CYBER SECURITY

Machine learning helps in identifying intrusion or unauthorized attempts made on network, thus making it easy in anticipating and understanding the kind of attack from the hacker. These kinds of analytics made by AI will help in defending attacks before it is too late.

Research from MIT came up with news that automated threat detection technique successfully predicted 85% of the cyber attacks in the year 2016. And it is also mentioned that the system can update itself with latest data in making new techniques in defending attacks. This gives a sigh of relief in identifying threats.

"Experts came up with another theory saying AI which is used in identifying threats can also be used by hackers in making advanced attempts in breaching into the networks."

CYBER SECURITY RECOMMENDATIONS FOR IOT

1. Minimal Research
   Make sure the device you are about to use with IoT has got enough security provided by the manufacturer.
2. Avoid default credentials
   When the device is deployed, focus on customizing credentials with proper key combinations
3. Update Passwords
   It is recommended to update/reset passwords after regular intervals or when there seems to be any suspicious activity observed.
4. Disconnect outdated software devices
   When the device is not capable of updating its software with latest versions, it is sign for security breach, and is suggested to disconnect it from the network.
5. Avoid being online when not in use
   Devices that are not in use for long period are to be disconnected, and even if the devices are in use, make sure you disconnect and reconnect it to ensure security.
6. Update Firewalls and Routers security
   Most of the routers used at home are always open; this has to be secured with built-in firewalls.
7. Segment your home networks
   It is recommended to segment your home networks in order to avoid access to the whole network when intruder gets an access to one of the devices connected. In general all the devices are set up with same password, which is not recommended.

8. Mobile Security

   Of all the devices connected to IoT, smart phones carry lot of valuable information when compared to other. High priority is given to secure mobiles to safeguard vital information.

According to Gartner, by 2020 there will be 60% of the companies that rely on the internet will suffer from failure of defending IT Cyber attacks.

FUTURE OF CYBER SECURITY

Future of cyber security is directly associated with the advancements made in technology and how secure is information when shared on internet. With the innovations in technology, it is recommended to educate common audience to be aware of information and safety. Getting connected to the internet should not be the first step in losing control over the data. Shielding devices before enabling it to share information is made as important as wearing seatbelt while driving. Artificial intelligence with IoT research has to be backed up with market leaders in order to make sure they come up with sophisticated solutions in defending similar kind of innovative hackers growing with the same proportions.

About the Author

N Subash Reddy, computer science post graduate from JNT University - Hyderabad, India. He is currently working as senior content strategist for Mindmajix. He is also into research about cyber security and artificial intelligence. His writings focus on latest technologies, tutorials, best practices, and innovations. Prior he was web developer familiar with most of the web and UI technologies. You can connect with Subash at LinkedIN, Twitter and Facebook.

ARE WE SOLVING THE RIGHT PROBLEM?

By Mac McMillan, CEO and President of CynergisTek

If you do not live and work within the cybersecurity profession, it won't take much research to find out just how far behind we are in having enough qualified cyber warriors. A quick Google search will yield scores of articles decrying just how bad this workforce shortage is, how it's getting worse, and some even offering creative solutions. In most cases, these "creative solutions" amount to little more than gimmicks or futile attempts to find a different way to say what everyone else had already said: there just aren't enough cybersecurity professionals to go around. All too often we seem to focus too much attention on the number of professionals and not the quality of the talent, which again is missing the mark in my opinion.

The interesting aspect of this workforce shortage is it's nothing new. Nearly four decades ago in the late 80s, before some reading this were even in the business and I was managing a large security team, I learned this first-hand. Back then cybersecurity wasn't a term and computer security wasn't even a real career field yet, and there was no such thing as a pipeline of cybersecurity professionals. We had to create them by drafting talented and experienced network engineers from IT, send them to multiple training courses in security, and then invest the time necessary for them to gain experience. They were literally several years in the making. At that time, the workforce problem was a lot simpler so the shortage was not as pronounced. That, however, is not the situation we find ourselves in today, nor will it be where we will find ourselves in the future.

Healthcare has been transformed by information and technology much like most other industries. Healthcare is now capable of doing amazing things by harnessing information through automation and advanced analytics. From predictive disease management to better patient engagement, deeper and more dynamic research, more accurate diagnosis, more precise surgical procedures, and on and on. Society has benefited immeasurably by what technology and information have done and will do for healthcare. Well over 90 percent of providers use an electronic health record, along with hundreds of other systems and applications that automate just about every process in the hospital today. Every practitioner relies on multiple devices to do their jobs and every patient has his or her own health-related apps or devices. Information is shared, repurposed, de-identified, studied, used a thousand different ways, and with countless others. Information transfers back and forth between systems, in and out of organizations, to and from individuals in a constant maelstrom of activity.

Patient information is concentrated in huge databases, spread over thousands of systems, transmitted and processed at increasing speeds. Who actually thinks that one person, the CISO, is capable of knowing or managing all of the risks associated with this new paradigm alone? And there lies the problem for today and tomorrow…a single individual, or even a group of highly dedicated and capable individuals, is not going to succeed in today's digital environment. Just like healthcare itself, it takes a care team. Each team may have specialists and sub-specialists, for example, but every member of the security team needs to understand the basic concepts around cybersecurity. If you touch "the system" in today's healthcare world, you touch the patient.

As a society, we need to understand and embrace the fact that cybersecurity knowledge and skills are becoming a necessity, not a "nice-to-have." The acquisition of these skills and this knowledge needs to begin the minute we hand a child his or her first device and must continue throughout their connected lives. We need to understand that every individual who comes in contact with information technology has an inherent responsibility to know how to use it responsibly, and should understand the risk if they don't. Every person that works in information technology — be they network engineer, database administrator, code developer, system administrator, etc. — needs to have cybersecurity training and knowledge of cybersecurity related to what they do. For companies or healthcare organizations, it means shifting away from the notion that one person, the CISO or CIO, is going to protect their entity, or that cybersecurity is simply an information technology problem. The CISO today and in the future needs to be a visionary, an architect, and a business manager, as well as a cybersecurity generalist who understands the total picture and can apply security principles to orchestrate the right solutions for the business.

The CISO must be someone capable of working collaboratively with others within the institution to secure systems and data; someone who understands the nuances of the business as well as security. In fact, security is part of the business of healthcare, and every organization across the continuum care must understand their specific security requirements. If we are going to be an informational or technologically driven society, then we need to embrace the fact that cybersecurity is an integral component of designing, building, deploying, administering, coding, managing, and using an information system or device.

At the same time, we need to retool cybersecurity experts to focus on the higher, more advanced skills needed to address cybersecurity challenges. We need them to be the analysts, the researchers, the developers, the monitors, the testers, the architects, the policy designers, the consultants, and the program managers.

So how and where do we begin to fix this problem? One approach already mentioned is changing the culture to recognize that cybersecurity is a fundamental aspect of any information system. A core knowledge requirement for every user is way overdue. This should begin at an early age and reinforced through learning in schools, K – 12 and beyond. This is as much a personal issue as it is a business issue.

There are some excellent programs out there that promote learning around cyber defense like the Cyber Warrior program. This innovative program makes learning about cybersecurity fun and practical for kids, and provides a launching path for those who might be interested in further study and/or a career in cybersecurity. Each year the Cyber Warrior program facilitates sponsored educational programs and contests for student teams across the country involving thousands of young people learning and practicing positive cyber defensive skills. Thinking on a grand scale, every elementary, middle, and high school in the country ought to have the opportunity to provide this experience for interested students.

Next, we address it in our technical schools, colleges, and universities. Basic cybersecurity learning should also be incorporated into every college curriculum, as most higher learning environments include course work using a computer — plus, most students are in school to prepare for a job that also uses a computer. For some, this will be the first real immersion into an environment where their computer is something other than a platform for social media. The number of undergraduate, master's and doctoral programs in cybersecurity are growing, and both classroom and online curriculums are available, but we need to recruit more proactively and promote these degree programs. One way to do this would be to offer tuition assistance, career jumpstart opportunities, paid intern programs, etc. Curriculums should also become more specialized offering classes in specific skills such as cyber analysis, security engineering, secure architecture design and security management. We need to ready the next generation of cyber warriors to be more prepared to hit the ground running and capable of making an impact when they arrive in the workforce.

Starting cybersecurity education early can also address cybersecurity challenges that arise in office environments, as workforce members arrive with an inherent appreciation for cybersecurity principles already ingrained. Organizations can cultivate their own cybersecurity talent by providing basic cybersecurity training to IT staff, and recruiting within for younger IT professionals to fill the more tactical jobs in security. This will allow more senior cybersecurity professionals to focus on more strategic tasks and be more proactive. We also need to give security professionals more time to increase their knowledge and skills. Professional development and skill enhancement are key determinants of job satisfaction for most cybersecurity staff, yet nearly half report that they have precious little time for this pursuit.

To put that in perspective, in terms of importance, 66 percent of cybersecurity professionals in healthcare receive at least one recruiter call per week.[1] Cybersecurity professionals also need to feel what they do makes a difference and is appreciated and supported. Thought should be given to where these individuals report in the organization, the visibility both they and the security mission are given, and the resources and support the program receives. These are people who work in an incredibly dynamic field, have many different interesting paths, belong to a workforce segment with zero unemployment, and constant inducement to go elsewhere. In short you need them more than they need you.

Organizations need to also look at their strategies for recruitment and retention. Broaden the focus, or more appropriately stop focusing. Look at cross-training opportunities with motivated individuals, get involved with local schools and technical schools, sponsor cybersecurity events to pull in other interested candidates. Create a cybersecurity support ecosystem for staff by connecting with local government and professional associations like ISACA. Create diversity in assignments and opportunities to learn new skills. Commit to support for professional education, certifications higher learning. Give serious consideration for career progression and incentive programs tied to continuous learning and acquiring new skills. Pay attention to pay scales and geographic norms for compensation. Cybersecurity professionals want and expect fair pay, but more than anything they want to be challenged, they want to continue to learn, and they want to make a difference. Organizations that want to attract and retain high caliber cybersecurity professionals need to create this environment.

The solution to the workforce problem is not the minting of an army of cybersecurity professionals, as if we expect the supply of talent to catch up to the demand. We also can't wait for the military or colleges to produce what we need unless you have another decade to wait. If we want to solve this shortage now we need to think more strategically and more broadly with respect to where applicants for roles might come from, and we need to act tactically and get serious about designing and providing workplaces that will attract and retain cybersecurity professionals. In the short run we need to remember that this workforce has options and is highly sought after, and conventional recruitment and retention is not going to be enough.

Mac McMillan, CEO and President of CynergisTek

1. CSO Magazine, Cybersecurity Snippets, John Oitsik, Nov 28, 2017

SHINE A LIGHT ON APP SECURITY

By Min Pyo Hong, CEO and Founder, SEWORKS

Cybersecurity and protecting the network reside squarely in the corporate IT spotlight, yet there's a shadow area where it's time to shine a light: Application security. Too often it's the app client that's the weakest link and becomes the entry point for hackers and malware.

The view of many IT security professionals is that if the network servers are secure, important business assets are protected. What's often overlooked is that enterprise servers are constantly communicating with a wide variety of mobile and web applications, ranging from internal communication apps to those residing on employee's devices (who could be using them to access the company network -- without the knowledge of IT).

But apps don't store critical information so any damage is minimal, right?

Wrong. Apps may not store critical company data, but servers do.

Hackers may be able to eventually compromise the servers by access via unsecure apps. According to our analysis at SEWORKS, 85% of the top 200 free apps on Google Play can be decompiled. Do any of your employees have mobile fitness apps on their phone? When we analyzed the top 10 fitness apps on the market, we discovered all of the apps had at least some critical and medium security vulnerabilities. Moreover, they all had a possibility of getting decompiled, which could bring subsequent hacking damages.

APP SECURITY VULNERABILITIES

Let's take a look at a few possible security scenarios where apps may be vulnerable.

Copycat apps. A prime asset for any software company is source code. One well-known gaming company, Supercell, expended significant resources and money developing a story line, characters, graphics and more for Clash Royale, a freemium mobile tower rush video game. The game was soft-launched in 2016 in a few countries, but within 4 weeks, a copycat app showed up. By re-engineering the source code, rogue hackers based in China were able to bypass normal development costs and time by simply bringing to market an already developed mobile game. By the time the true game developers entered the market, the copycat app already had a toehold in these markets.

Malware expulsion. A hacker compromises an app, reverse engineers the source code and inserts a type of malware that infects the corporate network. The malware could be used for DDoS attacks. Or, servers could be cryptojacked and the CPU or GPU power used to illegally mine digital currency. A company may also unknowingly distribute the malware, infecting unsuspecting customers and prospects. Unfortunately, it's difficult to predict what damage malicious malware could do in the future, but it certainly could monitor activities, messages, phone calls, or photos.

S**ource code manipulation and payment fraud.** If hackers manipulate the software code of a company's payment system, from the IT security professional's view, payments are flowing properly. In actuality, the money is flowing to the hacker's bank account and there's no way to get the money back.

PROTECTING YOUR APPS AND SERVERS

In one of the largest data breaches in the United States, Equifax said in a statement that "Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application." Through the attack, criminals had potential access to files that contained names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers.

Warning signs that apps have compromised enterprise servers may be subtle. In the Equifax breach, the security team observed suspicious network traffic. We recommend employing obfuscation and encryption of core files and libraries. Closely monitor your security status on an ongoing basis. Analyze and modify source code or binary files for protection. If an incident occurs, you must be able to take action as quickly as possible.

For any internal apps, we recommend starting with the design phase and incorporating security testing throughout the development lifecycle. Additionally, IT security professionals should also pay attention to customer feedback and online reviews. For example, if complaints crop up that a device seem to be running slow, that might be a sign that an app has been compromised.

We can't stress enough that apps can be leveraged by hackers to access your enterprise servers and your sensitive data. It's time to widen your cybersecurity spotlight – your business could depend upon it.

COULD CRYPTOCURRENCIES BE A BETTER AND MORE EFFECTIVE WAY OF THE SOCIETY'S CONTROL?

By Milica D. Djekic

Our world is changing at a quite fast pace and sometimes we are not sure if we can cope with all those changes. One technology would replace another and something that we knew yesterday would become unusable tomorrow. The similar situation is with the cybersecurity phenomenon being known as a cryptocurrency. The first indications of such advancement would appear a decade back and some predictions would suggest that this technology would vanish from our lives so soon, while the other experts would claim that the cryptocurrencies are our future. The fact is that some countries as well as financial institutions would approve the cryptocurrencies as a legal way of paying indicating that we could go deeply into cyberspace in the coming times in case we decide on to rely on that monetary solution.

The best known cryptocurrency is a Bitcoin and through this effort – we would mainly talk about the Bitcoin as the well-investigated and developed way of electronic payments. So, what is the difference between the ordinary bank transaction and the Bitcoin blockchain payment? The banking would mostly count on trust-based systems, while the Bitcoin would deal with the cryptography. On the other hand, the banking assets are centralized, while the Bitcoin is a decentralized system of transactions. It's also good to mention that the history of Bitcoin transactions is called the blockchain, while the person doing sending and receiving of the Bitcoin payments is known as a miner and such an activity is called a mining.

In addition, we should mention that the cryptocurrencies are so popular on the black market offering a certain amount of anonymity to their users. Well, is dealing with the Bitcoins that safe for real? Some sources would suggest that if you do the online transactions, that webpage would get the information about your IP address. Also, it's quite questionable if you got any anonymity at all while using the downloaded crypto-wallets. In any sense, whatever you do in the cyberspace would get correlated with some trace that could get skillfully investigated applying a digital forensics. The role of this effort is to make a comprehensive overview about the future of cryptocurrencies as well as make some suggestions how we could take the advantages over a virtual payment.

As it's quite obvious – right here, we would mention the virtual payment as a way of the future cyber transactions. In other words, it's not the point to suggest that tomorrow would rely strictly on the Bitcoins or banking transactions, but probably on some sort of the virtual payment. As we would indicate before, some forecasts would indicate the quite cloudy future to the Bitcoins. Some more optimistic prognoses would say that the Bitcoin could become the first global currency being accepted worldwide. Anyhow, if we dream about some united global marketplace that would deal with the only one currency, we could suggest that could be the Bitcoin or something else. As we already said, the Bitcoin is the decentralized system and it's well used by the black market, so it would not be that simple to avoid that way of financial activities. Also, we would say that

such a currency is not so safe for the usage, so its developers should work so hard to overcome that obstacle.

On the other hand, if we want to make the global economy getting so united – we should think about the currency that would replace all current monetary systems and cause the breakthrough of the ongoing financial marketplace. At the moment, this idea could seem as the utopia to many, but we believe if the world decides on to take that course – we could count on the united global economy in, say, several decades ahead. So, the question here is if the cryptocurrencies or their improved versions are our future or we would wait for a banking community to invent some new ways of payment. Apparently, if we see our coming days as a time of not using the cash – we would defiantly vote for some sort of the virtual currency. This proposition could bring us a lot of headaches because there would always be the conflict of interests between the governments intending to apply such an idea and the money printing industry being so powerful stakeholder on the marketplace. In other words, we believe that the folks making the notes and coins would not that easily give up from their profit-making businesses.

Also, let's say that the virtual money got our future and someone would somehow convince the guys printing the banknotes to change their business and choose something that would also bring them the good incomes. What would happen then? Would we transfer our financial activities in the cyberspace and go to the bank only to collect our payment cards? In case, this gets our reality – we should think a bit about some legal regulations that would offer the better control of our societies. In this effort, our intend is not to push some idea on, but rather to try to make a rational discussion about the times that are coming on. It's always good to have the plan or strategy that would support you in directing your actions on. If our way to the future is correlated with the virtual currencies and if we estimate that we need some time on to obtain so, it's helpful to do some brainstorming in order to clarify what we truly want out of our tomorrow.

The reasons why we believe that the governments worldwide could realize it could be quite useful to remove the printed money is that such an action would offer the good savings to the majority of the international budgets. It's well-known that making the notes and coins is quite expensive and it could be pretty appreciated if everyone could reduce those costs. Also, there could be some geo-political interests that could make the world votes for the united virtual currency. From this perspective, it can appear as a distant future – but as we said it could be the quite obtainable one. Additionally, we should think how those actions could reform our societies so deeply.

One more open question being present here is that if we could make our world getting more secure once we apply such a scenario. Also, if we decide to deal with the virtual currency only – we should get aware of the need for more IT security professionals who would make our web experience being so convenient and safe. This is still the ongoing concern because there is the huge shortage for the cyber skills. In addition, we should think how to resolve some additional challenges such as giving the legal permission to individuals being in possession of those accounts and cards. If we prohibit to underage

to get the owners of any virtual currency account or payment card – we should dig deeply for the solutions regarding the organization and management of those societies.

At the end, all these questions are on the fire and we would not insist on our suggestion to get accepted anyhow. We believe that it's necessary to think hard about your future plans and strategies before you make any step on. In other words, if anyone makes a decision to lead his economy in such a direction – that would probably get obtained in the few decades on. At the moment, this is only a proposal and if anyone wants to tackle it – he would realize it could become the big challenge as well.

HOW TO GET PREPARED TO COPE WITH THE DEEP REFORMS OF A COMMUNITY?

By Milica D. Djekic

The cryptocurrencies have revolutionized the way we send and receive the payments. It's easier than ever to obtain the crypto-wallet and save your blockchain transactions there. The interesting thing with your crypto-wallets is that you need only the password in order to steal someone's money on. As we would discuss through one of our pervious articles, our future could include paying and getting money via digital transactions only. Some futurists would suggest that there would not be need for the cash at all. The point of this effort is to try to realize how the world in such a case would look like.

In other words, try to imagine all the social and economical consequences of not dealing with the banknotes and coins in the future. It would sound as someone's dream, but it's possible that at one point in the future – the world would become the united economic marketplace and people would use digital currencies only. As the starting point here – we could use so rational facts – why would anyone want to get the united world and what are the benefits of such a concept? In addition, you cannot expect that undeveloped parts of our planet could follow the fast progress of the developed economies. The answer to this remark is quite questionable! We can expect that the entire world would get digitalized in, say, several decades ahead.

In such a case, it's possible to think about some digital currency that would get used over the globe. Also, it's important to know that in the reality – the main trigger to the progress is the interest. If the governments of the world's leading countries make a decision to take that course on and if they estimate that could get beneficial to their societies – they would definitely do so. In another case, this idea would remain only a dream. We are aware of that many experts worldwide would vote for this concept, but we would not find any pros and cons that would explain why anyone would accept this idea on. On the other hand, we would read some reports suggesting that the cryptocurrencies are only utopia and they must disappear from the marketplace so soon.

Anyhow, we would get aware of that the cryptocurrencies would get well exploited on the black market and so many criminal and terrorist organizations would count on this

way of dealing. Also, it's well-known that some countries and financial institutions worldwide would legally use this sort of payments. In addition, some organizations would print on the cryptocurrencies' notes and make their coins in order to satisfy their clients. The main reason for doing so is that the money printing industry is so powerful and it could get quite trickery to make it gives up from its business. Well, someone would say that there will be no cash in the future, right? In such a case, the first assumption we need to bridge is that to prepare our communities to live and work without the printed money. This may appear as a challenge and certainly it is, so right here we would stress out how our societies could get ready for such a change. We would agree with the only one claim and that is the only certain thing in the future is the change.

In other words, if we seriously get dependable on the digital currencies and our governments decide to remove the cash from the usage – that could be the good reason to deeply reform our lives and businesses. Just try to imagine that you would deal with your digital wallet only and send and receive the payments using so. Also, you could get some support in some sort of payment card that you would use in order to make a payment when you go to a shopping. In addition, it's quite questionable if there would even be need for the payment cards because you could pay for some goods or services simply subscribing to their weekly or monthly offerings. Hope you can get how serious and deep this reform could be. On the other hand, if you make a subscription to your favorite shopping mall or restaurant and pay in advance for their offerings using a digital transaction, you could easily cancel your order once you decide to give up from so or if you make the smaller bill than you expected – they would return you such money or leave it on your account for the next occasion.

Also, there is the big concern with the underage group of persons. Many parents would not get happy to give the money to their teenagers believing they could spend them on drug, alcohol, weapons or some wild parties. If there is no cash and the parents get an opportunity to better control the activities of their kids and if the governments ban to the underage to open on any monetary accounts before their legal maturity – there could get less cases of the young delinquent crimes. This could be the good contribution to a public safety and security, but we are also aware of that many humanitarian organizations could report that there is less freedom for the people. In any case, we could try to think hard how to make a balance between the human rights and security needs. It's sometimes so hard to the decision makers to decide on what to do or how to deal in the certain situation.

The role of this effort is to offer a brief discussion about all pluses and minuses of the digital currencies' usages and also mention some suggestions regarding how our societies could cope with so inevitable changes. We all know that something new would happen in the future and we should get prepared to cope with those changes. The digitalization of the planet would undoubtedly require more IT security professionals and we know that there is some skill shortage in such an area. One day if we accept the global currency for real or, in other words, if we make the conditions for so – this world could be more appropriate place to everyone!

VIRTUAL PRIVATE NETWORKS: CHECKING, TRACKING AND BREAKING

By Milica D. Djekic

Many persons and organizations would try to find the ways to protect their internet connections as well as confidential contents using a diverse set of tools. One of the well-known methods to assure your IT infrastructure is using the Virtual Private Networks of VPNs. These sorts of defense would include the hiding of your private IP address and showing only the public IP address that would be different from the private one. In other words, it's about the simple trick to avoid to get stalked in the cyberspace. So many organizations belonging to the both – public and private sector – would recognize the advantages of this technology and they would greatly use it.

So recently, we would do the small testing trying to figure out how many people worldwide use the VPN. For such a purpose, we would apply the Shodan IoT crawler and we would find more than a million IP addresses that would get correlated with the VPN keyword. It's feasible that there are even more end users worldwide that would take advantage over this cryptographic solution. In other words, the VPN would encrypt your web traffic in some manner and the people trying to access your device from the outside could have the certain difficulties to do so. Indeed, the VPN is the good way of protection and so many researchers over the globe would recommend it to get applied by the IT security professionals.

On the other hand, that sort of the cryptographic assurance is so popular amongst the organized crime and terrorist groups. They would probably believe that they can do the good camouflage applying such a system. Also, they would so commonly use the alternative ways of security such as Tor browser in order to remain anonymous and safe. Right here, we would stay with the VPN solutions, because those technologies could get so popular in case of the bad guys. Indeed, the majority of those individuals would believe that they would get invisible from the outside once they set up their computers to deal with the VPN gadgets or download some of those software from the internet. The question here would be if they are safe for real using the VPN technology. The answer to this question would get provided further through this effort. At this stage, it's good to know that the VPN system as any other has some pros and cons and it would not offer an absolute security to anyone.

So, we would try to discuss if we are really safe when we use the VPN solution. So many criminals and terrorists would hide behind this technology and they may believe that they got some chance to trick their opponents. Indeed, would that be the case for real? The answer to this question is quite straightforward. In so many cases, the VPN gadget could serve as a good method of prevention from getting discovered on the web. Also, some people would consider that such a protection got good enough to prevent any sort of a cyber attack. In other words, the VPN in combination with the good encryption of data could get the perfect way to avoid to get targeted. On the other hand, we would do a simple research on the internet trying to realize if there is any possibility to discover the real IP address of anyone using the VPN protection. The results of our

investigation got so shocking! Namely, there are the considerable bunches of online tools that can support you in discovering if anyone is applying the VPN gadgets. In addition, we would know that the defense community would deal with so many professional tools and if anyone tries to use the VPN technology for the illegal purposes, he would so easily get proceeded. It's important to know that anything you are doing online would leave the trace and the skillful forensics investigation would sooner or later prove what it has happened in the practice. In other words, if the bad guys make a decision to hide behind the VPN or any other solutions – they should know that the Law Enforcement agencies would catch them quickly.

So, the VPN is a handy option for protecting your asset from the hackers and in so many cases, the good guys would apply this technology in order to encrypt their web traffic and hide their IP addresses being correlated with their physical devices. Also, if you choose to deal with the VPN – you should know that there are so many pluses of that advancement. The ordinary hacker would usually get some difficulties to discover anything about you, while the professional cyber criminal dealing with the wide spectrum of the hacking tools would see that task as a piece of the cake. As we already said, there is a plenty of the VPN tracking and checking tools being available on the internet and sometimes it's so hard to prevent any cyber incident. In addition, the bad guys would not be anyhow smart if they believe that the VPN gadget can resolve all their concerns. The fact is the VPN is the quite average method of protection and we would not recommend so for any serious applications. Further, this is the good news for the defense and intelligence community because those folks should know that the VPN is not any obstacle in combating the organized crime and terrorism. Apparently, the good guys should constantly and continuously get updated with the new and new education and training sessions in order to remain ready for any actions on. We believe that such an approach could offer us much safer cyberspace!

In conclusion, it may appear that the VPN is possibly the good method to prevent your devices being the part of a global network, but you should always keep in mind that the defense agencies got the capacities to handle any situation on. If anyone would try to protect his privacy applying the VPN gadgets, that would not be the problem. On the other hand, if we talk about the malicious actors trying to hide any illegal activities or even crimes behind the VPN technology – they should know they would be only the routine task to the Police Forces.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and. She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

SECURING YOUR CODE FOR GDPR COMPLIANCE

BUILDING A LONG-TERM PROGRAM

by Jeannie Warner, Security Manager, WhiteHat Security

INTRODUCTION:

The deadline for GDPR initial compliance was May 25, 2018, but the directives enforcing Privacy by Design are not a "once and done" project; The methodology used to create public-facing GDPR-compliant websites and applications demand a change in development and engineering practices. GDPR requirements are not bounded by network or application in scope; they are dedicated to the security and privacy of the citizens of the EU. Future lawsuits will likely focus on how well organizations are designing secure systems which allow for assessing, preventing and monitoring data privacy.

Every year, Verizon releases a **Data Breach Investigation Report.** In 2018 again, Web Applications top the list as the biggest vector for data breaches. It is not a trivial task to change the mindset of Developers and Architects, and to make major changes toward a secured Software Development Lifecycle (SDLC). The truth is, many Developers and Architects focus entirely on the functional requirements of a system or application as handed to them by product management. Non-functional requirements (NFRs) within the user experience are often considered architectural choices rather than mandates. The overall security of the application has, outside of PCI DSS, been relegated to short paragraphs here and there within security and privacy regulations.

Complicating this lack of specifics is a push toward cloud services and third-party plug ins, distributed data storage, microservice via distributed development teams, and insufficient architecture awareness of security threats, from both applications and the APIs that connect them with databases and services.

We need to bridge that gap by helping Developers understand that adding security as an essential NFR to every application will reduce churn, rework, and a large backlog of bug tickets. Management, both Engineering, Product, and Security, need to speak the language of the developer to offer up support for their daily tasks using Developer's language.

MANDATES FOR SCOPING YOUR SECURE SDLC FOR GDPR

The following are the mandates for scoping the GDPR Secured SDLC in terms of data privacy:

- ✓ Encryption and pseudonymization of personal data.
- ✓ The ability to restore personal data availability in the event of a security incident or technical issue in a timely manner.
- ✓ Ensuring ongoing confidentiality, integrity, and availability of applications which touch EU Customer data.
- ✓ Establishing a process for regular security testing and assessment of the effectiveness of security practices and solutions in place.

Nothing successful can be done without executive support, budget, and buy in. In support of these mandates, the following are high-level steps supporting your DevOps group both through management support and continuing communications plans and documentation:

1. Presumably your organization has created your GDPR Risk Register as you performed Gap analysis – you already determined which applications or vulnerabilities could not be scoped or addressed by May 25, 2018, but still may need review that the deadline has passed.
2. You need to set up a continual improvement and awareness program for long-term compliance.
3. Compliance/Data Privacy Officers need transparency into the newly compliant SDLC as part of their documentation on constant improvement. This includes process documentation and artifact creation such as:
    a. PCI DSS or other compliance-style formatted reports are always recommended
    b. Vulnerability detail reports which track age/longevity of vulnerability/risk
    c. SOC reports or other monitoring reports of threat activity for incident management
    d. Ticketing reports for status on remediation – the best KPI for process improvement is showing internal vulnerability remediation times dropping as Developers patch applications.

SECURITY AS AN ESSENTIAL NON-FUNCTIONAL REQUIREMENT

What is meant by essential and yet non-functional in the same sentence, one may ask? In Agile development terms, functional requirements include items such as Epics, Capabilities, Features, and Stories, all of which are dedicated to user, business, and market needs. Non-functional requirements define application attributes such as Security, Reliability, Performance, Maintainability, Scalability, and are handed to the developer by Solution Architects and Engineering. These are the constraints and restrictions on the application across the various product backlogs.

Application Security is an important part of GDPR compliance and needs to be addressed with exactly the same rigor and disciplines as Network Security. However, because GDPR has vague directives on the topic of applications as opposed to network assets, we can use the GDPR checklist for how to secure Databases combined with best practices in AppSec Security from PCI DSS, and expand those ideas, checks, and balances into a full application checklist for Developers.

PRIVACY BY DESIGN - SECTIONS OF GDPR THAT MENTION APPS

PRIVACY BY DESIGN

The GDPR states that organizations need to "Develop a strategy and playbook for "privacy by design" to incorporate privacy controls and impact assessments throughout the data lifecycle for new and changing data use initiatives"; That's extremely vague as pertains to applications - how does one set boundaries on what defines controls and impact assessments?

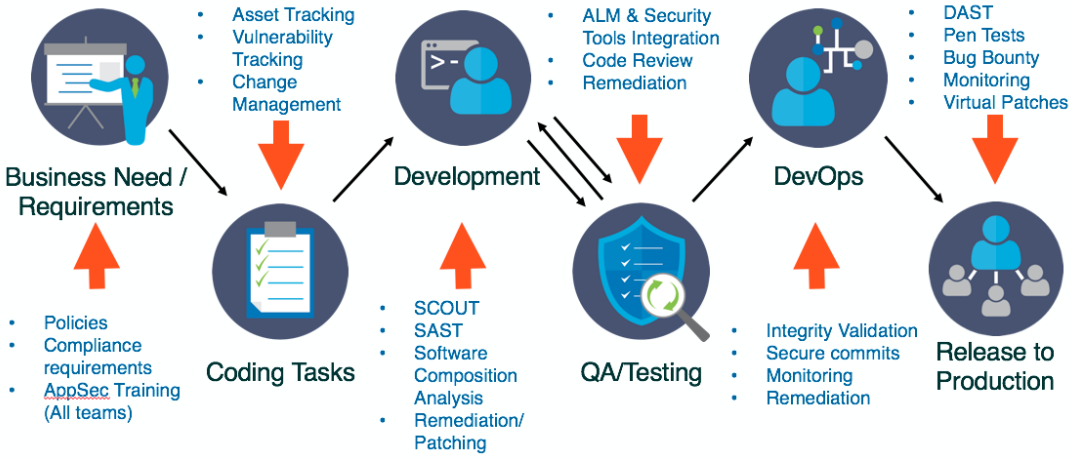
Application Security or AppSec needs to be bounded and defined so that every aspect can be weighed and examined. Each of the elements of the application need to be examined, both in UAT and production, as there can be vulnerabilities which are not made manifest until examined for business logic as well as pure data intake evaluation:

- ✓ Testable – NFRs must be stated with objective, measurable, and testable criteria, because if you can't test it, you shouldn't ship it.
- ✓ Independence – NFRs should be independent of each other so that they can be evaluated and **tested** without consideration of or impact from other system qualities.
- ✓ Negotiable – Understanding NFR business drivers can mean negotiation for what goes on a risk register vs gets fixed the very next release.

PRIVACY AND SECURITY CHECKS

Verify for Security early and often (See image of all SDLC stages, below)

1. Parameterize queries
2. Encode data
3. Validate all inputs
4. Implement identity and authentication controls
5. Implement appropriate access controls – authorization reviews
6. Protect data – least privilege & encryption
7. Implement logging and intrusion detection (monitoring)
8. Use secure frameworks and libraries (Software Composition Analysis)
9. Error and exception handling



For scope in this discussion, your NFRs matter most for web applications or sites where EU citizens have logins or accounts, or visit/distribute cookie information from which can be gleaned personal information, even via cookies, pursuant to GDPR scope.

Why do cookies matter in terms of data acquisition and theft?

This method of attack is not often mentioned in network security - A cookie is a token stored in a browser; however, it can be reverse engineered by the bad guys to trick a website into thinking it was the original cookie.

A SECURE SDLC FOR COMPLIANCE

Once you understand the scope of your ongoing GDPR compliance program and agree that Privacy by Design is integral to your Developer tasks, you need to create design your vulnerability scan, test, and verification plan for AppSec management throughout your Software Delivery Lifecycle (SDLC). This includes both your testing and production environments, because systems can behave with different values in pure code and test environments versus final staging and production.

To bake security testing into software development, you should take notice of how other testing is done. Unit and functional requirement tests are built custom for each application. In mature organizations, these may be abstracted, standardized, and even partially templated. Many organizations have entire teams dedicated to creating, running, and verifying the results of unit and functional testing.

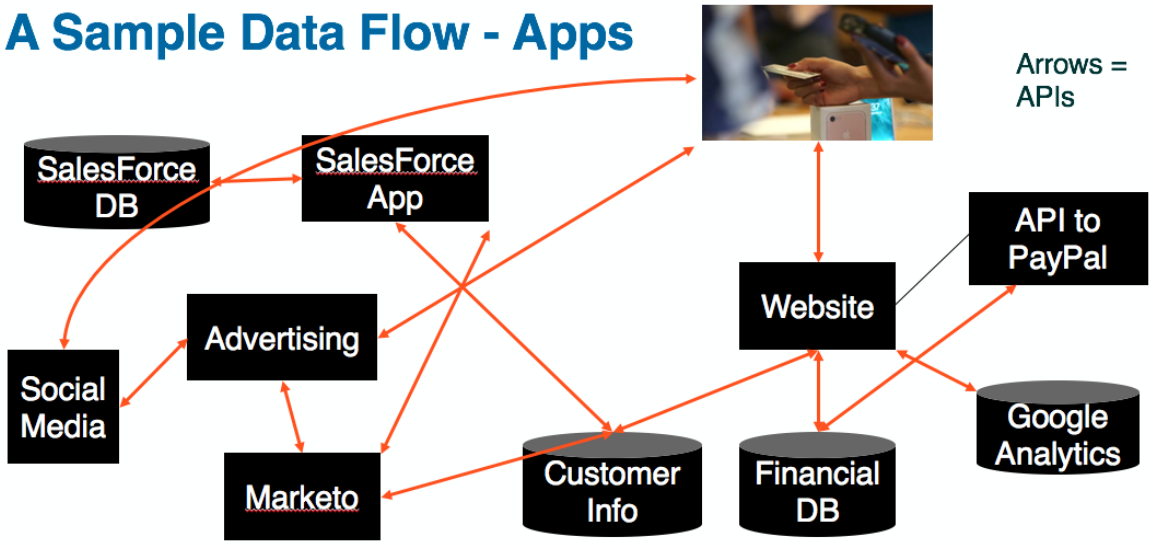
NFR security testing, like all other testing that takes place in the development process, must be generic (where possible) and specific (where necessary.) Ongoing risk discovery and management for the GDPR includes a need to:

- ✓ Focus on exploitable risks that exist in the application in its current released state.
- ✓ Scheduled scanning, scan points to the version of the code that is currently in release to customers or deployed in production (Master / Trunk / Released Binary).
- ✓ Findings from this concern should contribute to an organization's top line risk metric for the application.
- ✓ Bug tracking integration or other reporting that the organization uses to track risk reduction initiatives, document future design requirements, etc.
- ✓ RD&M is typically the correct starting point.
- ✓

All of this SDLC program design is pursuant to the GDPR InfoSec directive to "Identify existing security information protection controls and align security practices with GDPR considerations."

1. Identifying assets – many organizations have 100's applications they are not aware of, in terms of security.
2. You will need to work with architects and engineers to map the flow of EU citizen data through applications and databases. Use terminologies appropriate to the experience and understanding of the audience, i.e.:

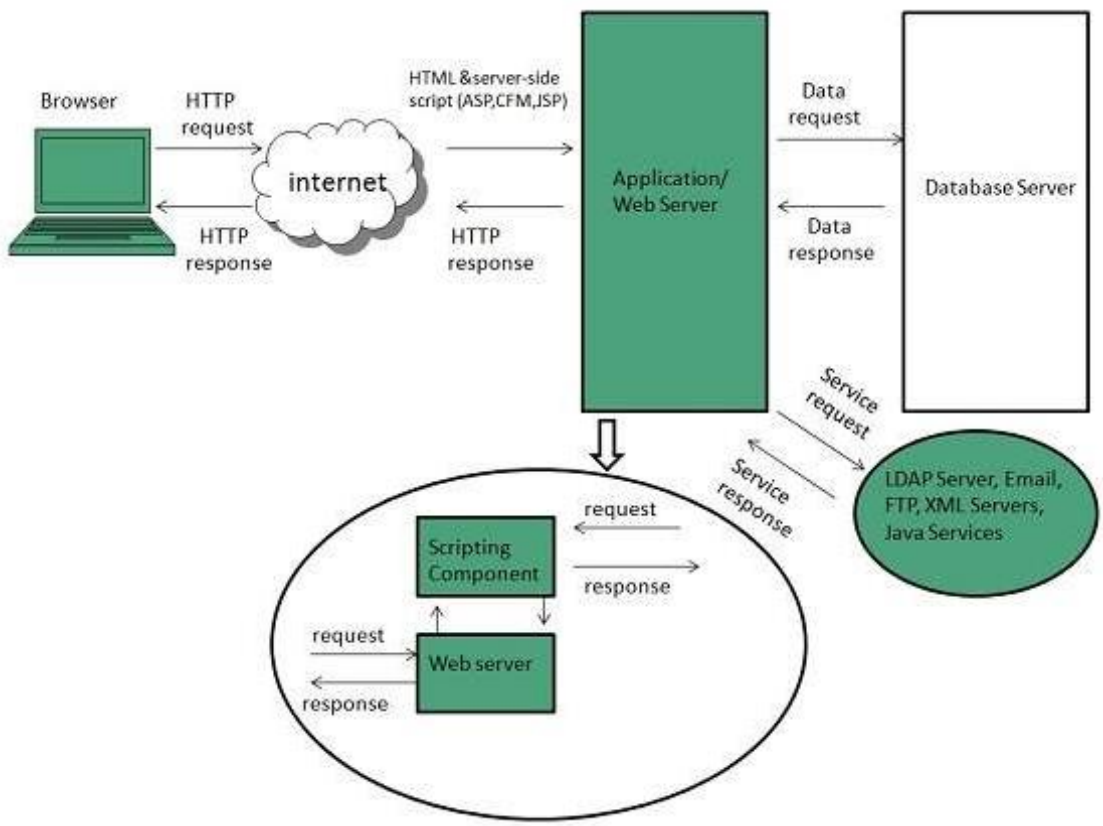
For Executives or Audit officers, construct models that illustrate broad flows of customer, partner, and prospect information through your various applications and websites. High-level labels are fine here, as in this marketing-department example:



For DevOps, Engineering, IT Security, your architectural decisions are more detailed and function-oriented as you write up NFRs and consider testing.

At each API arrow in either model, consider how much of a customer record is really needed to move, transfer, or store, and how secure each of those actions the information is going to be. Remember to test for worst case scenario, like

What could someone with Super User access do? What could a regular user do? Can a stranger get at the system through tricking the authentication to allow them access?



APPLICATION SECURITY PRODUCTS SUPPORTING GDPR COMPLIANCE

Choose your strategy for effective AppSec coverage across assets. Solutions include:

1. Static application security testing allows you to review code before it goes to production, to catch high- and critical-level vulnerabilities before risking exposure to the internet.
2. Software Composition Analysis, either built into the Static testing engine or as a second service, looks at third-party libraries and frameworks which make up an estimated 75-90 percent of all web applications. Because security seldom has insight into the developer tool set, this is an important function to help blend the two into a functioning DevSecOps cooperative.
3. Dynamic application security testing looks at the functionality of a web application. Dynamic application scanning helps you stays on top of all newly-discovered vulnerabilities and exploits as they become public. In an ideal world, set up constant daily or hourly production-safe scans. Keep your security team aware of both new functionality as it is added to a website, and any subsequent security vulnerabilities created by them.

4. API scanning can be handled in various ways, but for high-risk information streams and ERP systems you may want to do an evaluation to make sure that the information flowing between back-end systems is as airtight in security as the front-end systems. Usually API checks are performed as part of Dynamic scanning, but for instances where there is no UI associated, you may want to look at a stand-alone API logic assessment/security scan.
5. Don't forget Mobile applications! Mobile App security testing is mandatory for mobile sites which touch or store EU customer data. If your app, game, or other service is offered via phone in an app store, make sure it doesn't leak private customer info.
6. Bug Bounty programs – This is a useful add-on to your testing strategy or program; It is ad-hoc and requires internal validation of each finding by your development team and can incur higher costs in tracking and rewarding than simply operating a managed application security testing solution. Many companies maintain bug bounty programs in addition to a rigorous AppSec strategy, as it can allow for cutting-edge new vulnerability discovery if your risk tolerance is low and your IT security budget is high.

Consider Remediation vs Mitigation in risk: Backing up to the idea of Non-Functional requirements interfering with Functional requirements via legacy or third-party code, you may need to examine secondary protection for your web portal. The two best options on the market are:

WAF – Web Application Firewalls. If you have a network support team, they can often take over a WAF with minimal vendor training.

RASP – Runtime Application Self-Protection – this is an agent that is loaded onto the web application server to monitor runtime application commands and halt malicious user behavior.

Both of these options tend to cover the mandate for Logging and Monitoring – an important part of GDPR Incident Management. In organizations with no application-level logging and monitoring, it can be hard to find the actual vector of attack against an application.

DEVELOPER TOOLS & INTEGRATIONS

As you move toward the Privacy by Design model of securing your SDLC, it's best to integrate all your security checks into your Developers' current daily tasks and tools. The easier you can make application security testing for your teams, especially if the teams are geographically distributed or spread over multiple shifts, the more likely they are to perform regular security testing. Take note which developer environments and tool sets (IDE/ALM/CI/CD, etc.) are at work, and plug into ticketing.

PRIVACY INCIDENT MANAGEMENT

Build a scenario which engages DevOps on how to respond to emergencies, either identified internally or by someone outside your organization. GDPR says, “Align incident response processes with GDPR specifications and reporting requirements. Establish a triage approach to evaluating potential privacy breaches and incidents.”

As you conduct this alignment long-term, consider if your organization has sufficient AppSec expertise to execute this program, or whether you need program support or outside assistance as you create AppSec Champions.

1. Consider importing Dynamic scan results into WAF or RASP tools for your most critical applications to create virtual patches and prevent incursions rather than just report on them.
2. Import Dynamic scan results into SIEM or other VM/BI/GRC solutions to constantly assess and measure AppSec risk.
3. Finally, consider exporting Dynamic scan results into SOC monitoring infrastructure. SOC analysts love information and can always use AppSec training to understand how IDS/Network information can conflate with AppSec vulnerability data into a holistic security picture hour to hour.
4. Remember that any incidents or breaches of your web application security practices need to have a clear path leading back to your SDLC via ticketing systems and a review of your NFRs.
5. A Risk Register, started during your Design and Requirements phase in development, will serve your entire SDLC by allowing full transparency as well as tracking your improvement.

DON’T FORGET TRAINING AND AWARENESS

GDPR says, “Define and implement a training and awareness strategy at the enterprise and individual level.”

You’ve implemented GDPR training for sales, marketing, customer service – don’t forget engineering! Developers and IT Security Managers need training and education to understand the basics of risk analysis and threat modeling for applications as well as best practices in secure coding.

Close the loop of Security by Design by educating your DevOps team into avoiding bad practices from the beginning.

Resources for training and best practices on secure coding testing include:

- ✓ OWASP Secure Coding Practices -
- ✓ OWASP Application Security Verification Standard Project -
- ✓ WhiteHat's eLearning for Developers
- ✓ NIST – Systems Security Engineering (SSE) Project
- ✓ SANS – Security Web Application Technology

About the Author

Jeannie Warner, Security Manager at WhiteHat Security. She currently serves security manager at WhiteHat Security. She believes application security is the Next Big Thing in the security space. Her path to computer security started with DellNet Technical support, then into a Unix Helpdesk, followed by Network Ops. She went to work at IBM as they were building out their Security Operations Center in 2001, and after a short while became their tech lead. She moved on to security analysis and forensics from there, and eventually product and portfolio management. After IBM Security, she left for Microsoft's Security Research Center before returning to the Bay area to work for Symantec and Fortinet, with a brief stint off to Australia to run a global SOC operation.

Jeannie can be reached online at (Jeannie.warner@whitehatsec.com, @thetsmorgan, https://www.linkedin.com/in/jeannie-warner-cissp-5585851/) and at her company website https://www.whitehatsec.com/

WAKE-UP CALL FOR ENTERPRISE RESOURCE PLANNING USERS

A MAJOR INSIDER SECURITY THREAT STEMS FROM THE COMPLEXITY OF ERPS AND COMPLICATED SYSTEM SECURITY

by Jody Paterson, CEO, ERP Maestro

Cybercrime has become a top concern for the contemporary world. To protect themselves, many organizations have stockpiled solutions against outside attacks—while ignoring the more ominous threats right under their noses.

According to IBM's 2016 Cyber Security Index, 60 percent of cybersecurity breaches come not from an unknown outsider, but from the inside—at the hands of employees. Other sources cite higher numbers upwards of 75 percent. In Cyber Insider's 2018 Insider Threat Report, 90 percent of security professionals reported feeling vulnerable to insider threats.

Some attacks are malicious, with disgruntled workers taking revenge by disabling systems, committing fraud to embezzle money, or profiting by selling company or client data on the dark web. Many other breaches happen inadvertently, the result of worker error or inappropriate permission rights to information.

As a growing number of organizations use enterprise resource planning (ERP) solutions to manage their core business processes, they also have to safeguard against vulnerabilities that can come with ERP use. ERP systems, which provide a unified platform for accounting, human resources, purchasing, sales, and other departments, help businesses run more efficiently. The danger lies in the complexity of the systems, too much internal access to sensitive data and weak controls.

Since attention to internal cybersecurity has lagged behind the emphasis on external threats, companies have only begun to take internal risks more seriously. Increasing education and developing prevention programs are key components in correcting the inequity between the two.

A WAKE-UP CALL

Shockingly, there are companies that never analyze the permissions assigned to their ERP users. One reason for this is a tendency for companies to be reactive rather than proactive when it comes to internal risks, waiting until a costly or critical breach occurs instead of preventing incidents to begin with.

Conversely, all businesses understand the urgency in having a security system to prevent physical intrusion into facilities and to thwart external hacks into systems. They don't wait until a break in or breach takes place to protect valuable assets.

And yet, "privilege creep," in which an employee may gain increasing access as their roles and permissions change—even beyond what they need or should have—happens all of the time if not monitored. Another common problem is granting privileges that mirror existing user access when onboarding new users. Over time, a company can create their own worst permission-bloat nightmare.

Without regularly evaluating their ERP access and security, enterprises leave themselves incredibly exposed to inside cyber hazards.

PREVENTION IS MORE THAN JUST AN OPTION

There are steps an organization can take to guard against insider attacks, even of sensitive ERP systems. The first step is to acknowledge the problem and take internal threats seriously. Even small enterprises where "everybody knows your name," can be vulnerable—particularly so, if the intimate atmosphere creates a sense of complacency.

Secondly, prevention has to move to the forefront of internal cybersecurity. Once a company has acknowledged the real possibility of employee-based access violations, take steps to:

- Safeguard against mishaps and insider fraud with tight and agile controls. Double check who has access to what to avoid "privilege creep," making sure that each employee has only the access they need to perform their job. This important precaution is often overlooked—but it's the authorized access, not the unauthorized, that so often gets organizations in trouble. It's a daunting task to do manually, but it must be done if an automated solution is not in place.
- Understand the most common segregation of duties (SoD) conflicts. Is it possible for a single person to access all the processes involved in doing business in your organization? This end-to-end access is the linchpin of a security crisis. Analyze your SoD policies and procedures and redefine them where needed, then audit them continuously to ensure that they are being followed and are working.
- Educate users on security protocols. How security-aware are your employees? Your executives? Everyone in the organization, regardless of role, needs thorough training and regular refreshers on secure password protocols and proper use of ERP systems.

- Review your sensitive access monitoring controls at least once a year. Even the strictest controls can have "cracks." Checking for them, and for suspicious behaviors, is key to prevention and early detection of insider breaches. Have a system in place to continually monitor privileged users' activities—and to alert you to attacks. Track changes to critical data, as well, and set up audit trails on important transactions.

THE BIGGEST THREAT OF ALL

In the increasingly fast-paced world of business with global employees and many points of access in extremely large organizations, monitoring ERPs for internal security breaches isn't a nice-to-have option. It's a must-have.

When it comes to ERP security, the devil is in the details—often, in the ones you can't see due to lack of attention on them or tools to simplify spotting them. The biggest risk to any enterprise's security comes not from employee actions, but organizational inaction: the failure to act until after a breach occurs.

About the Author

Jody Paterson is the CEO of ERP Maestro.

He is a security evangelist, thought leader, speaker and KPMG veteran who is committed to creating smarter ways to keep companies secure on the inside and ease the burden of managing, monitoring and auditing access to critical business systems.

Jody can be reached online at jody.paterson@erpmaestro.com and at our company website http://www.erpmaestro.com

DECEPTION TECHNOLOGY—USEFUL TOOL OR JUST MORE BUSYWORK?

by Tim Roncevich, Partner, CyberGuard Compliance

INFOSEC PROFESSIONALS ARE LOSING GROUND IN THE WAR ON CYBERCRIME.

Cybercrime damages will total $6 trillion annually by 2021, doubling since 2015. Unfilled cybersecurity positions will reach 3.5 million by that time, more than tripling from a shortage of 1 million in 2014, according to the most recent Cybersecurity Jobs Report from Cybersecurity Ventures.

Forced to defend against an abundance of threats with a shortage of resources, understaffed teams and overworked workers are deploying deception technology as a defense against data breaches, hoping to proactively trap would-be cybercriminals.

Deception technology involves creating a fake network solely for identifying intruders. After you ferret them out, you can bar them from future access to your entire network.

Though deception itself has long been a cybersecurity tactic, modern technology has made it increasingly popular. In its early stages, deception technology was limited to "honeypots", whose simplicity, for the most part, relegated them to usage by smaller organizations. Attackers eventually learned to spot them because they didn't change, thus reducing their effectiveness.

Deception 2.0 technology mitigates advanced threats by detecting, engaging, and responding to the tactics, techniques, and procedures of those threats. Robust detection systems within your network provide stronger protection.

However, deception technology is not suitable for all organizations. If it isn't adequately supported, it could end up being busywork instead of a useful tool. Here are a few pros and cons of deception technology:

PROS

Fewer false positives: If someone is moving in the fake network, they likely do not belong. Following their activities can give you clues as to how they might attack your real network. Then, you can bolster your defenses by learning from the attack patterns that you have uncovered.

Earlier alerts: Given that cybersecurity breaches are active on enterprise networks for an average of 200 days before they're discovered, high-fidelity alerts help you protect legitimate assets because you can secure them while the intruder is in your false network.

Pervasive deception: Spotting intrusions early allows you to escalate your responses. You can deploy decoys, breadcrumbs, baits, and lures to engage and eliminate threats at various levels.

Scalable defenses: Deception technology has evolved well beyond honeypots. Rather than relying on a single static ploy, you can implement a whole system that mirrors your actual environment, making it more likely that you will fool intruders. Deception 2.0 technology also can be used in the cloud.

CONS

False reliance: If you're waiting for an intruder to wander into your fake network, you may be too late. They could be in your real network instead. Your false sense of security could cause you to miss a threat.

Expansive resources: Deception technology can be expensive. In addition to the initial investment in building an extensive false network, you have ongoing maintenance costs and occasional upgrade costs to keep your false network believable. You may also have to remediate damages to other systems if an intruder moves beyond the false network.

Needs support: You can't depend solely on deception technology because it only guards against intrusions. You must incorporate other defenses because breaches are increasingly difficult to prevent. You also must implement cybersecurity measures that can help you if a breach occurs.

Alarm fatigue: If you are overworked and understaffed, one more piece of technology may not make any difference. Though you still should investigate what is going on and take action, if you're overworked, you may suffer from alarm fatigue and skip another seemingly mundane task, leaving your network vulnerable to attack.

FINAL THOUGHTS

At the end of the day, deception technology can be useful for detecting an intruder before a breach happens, but it is not a set-it-and-forget-it purchase. You must invest in the resources you need to adequately recognize (and respond) to threats. You have to be able to invest in the staff and technology necessary to build and maintain the network and catch hackers in the trap. If you don't, you will likely frustrate your team by spreading them too thin.

Similarly, deception technology should not be used as a band-aid for a more serious systemic problem. If you do not have proper security controls in place that have undergone a SOC 2 audit by an independent third party, your system could be more vulnerable than you think. Your fundamentals should be rock-solid. No amount of additional threat detection can replace this. Although deception technology is proving to be a useful tool for proactively detecting threats, it should only be used by those that have the time and personnel to properly use it.

About the Author

Tim Roncevich is a partner at CyberGuard Compliance. Tim worked previously at a large global accounting firm, where he specialized in SOC audits. With over 15 years of professional experience, Tim has an excellent diversity of skills to effectively serve his clients. Tim's industry expertise includes Service as a Software (SaaS), manufacturing, technology, banking, retail, consumer products, mortgage, and professional services. Tim can be reached via LinkedIn and at our company website https://www.cgcompliance.com/

DDOS ATTACK EVOLUTION: THE POWER OF UDP AMPLIFICATION

By Corey Nachreiner, CISSP, CTO at WatchGuard Technologies

Over the past three years, distributed denial of service (DDoS) attacks have grown significantly both in quantity and scale, breaking bandwidth records repeatedly. The most recent DDoS evolutions started in 2016, when an Internet of Things (IoT) botnet called Mirai launched a 620 Gbps DDoS attack against Krebsonsecurity.com and a 1 Tbps attack against a European hosting company (OVH). DDoS attacks of this magnitude often take out collateral victims apart from their intended target, and they're only getting stronger.

But before IoT botnets, attackers launched record-breaking DDoS attacks using a technique called Domain Name Service (DNS) amplification or reflection. This technique uses three properties of the DNS service to force public servers to send huge amounts of traffic to unsuspecting victims. However, these three properties aren't unique to DNS alone; they exist in many UDP-based network services, including previously lesser-known ones like Memcached. Recently, UDP amplification attacks took back the DDoS lead with the "Memcrashed" attack, during which criminals generated up to 1.7 Tbps of DDoS traffic using memcached.

In this article, we'll discuss the properties that make UDP-based amplification attacks possible and so effective… but first a quick technical refresher.

A QUICK NETWORKING AND DDOS PRIMER

To understand UDP amplification attacks you first have to remember the differences between TCP and UDP traffic. At a high level, TCP traffic requires a full two-way negotiation between both devices before any real communications can begin. This negotiation is called the three-way handshake. As for DDoS attacks, this means that you can't really spoof TCP-based DDoS attacks (with the exception of TCP *negotiation* attacks like SYN floods). In other words, a TCP attack usually has to come from a computer the attacker controls.

UDP, on the other hand, is a connectionless protocol. It doesn't require a pre-negotiation, nor necessarily a response from the receiving device. There are other connectionless protocols as well, such as ICMP, which have a couple of advantages for DDoS attacks that we'll talk about later.

It also helps to understand how the security industry classifies DDoS attacks. Generally, they place attacks in three categories.

- **Volume Attacks** – These DDoS attacks are designed to overwhelm targets purely based on a huge deluge of network traffic. They don't necessarily care if the target handles the traffic in any way; they simply send enough of it to disrupt all network services. UDP amplification attacks fall under this category, as do some other flooding attacks, like ICMP floods. In general, most volumetric attacks use connectionless protocols.

- **Protocol Attacks** – These attacks eat up the resources of critical network servers or devices (routers, firewalls, etc.) by taking advantage of different protocol-level dynamics. For example, in order to route TCP traffic, routers and firewalls have to maintain a state-table. SYN floods are a type of attack meant to fill up that state table with partially completed or "half open" connections, so the device can't take new connections. Other examples include The Ping of Death or Smurf attacks. Some call these "state exhaustion" attacks.

- **Application Layer Attacks** – These attacks concentrate on layer 7 of the OSI stack. To put it plainly, this means they focus on issues with specific applications such as web services (HTML), email (SMTP), or database services (SQL). Application layer DDoS attacks are often the hardest to recognize because they look so much like normal and legitimate traffic for that application. In some cases, application layer attacks leverage technical vulnerabilities or flaws in a specific application to slow things down or crash the server. In other cases, attackers simply send a whole lot of perfectly legitimate, but process intensive requests, such as GET and POST floods.

Unfortunately, sophisticated DDoS attackers today actually combine many of these DDoS attacks together in a single campaign. Now that we've covered the basics, let's talk UDP amplification.

DISSECTING REFLECTIVE UDP AMPLIFICATION DDOS ATTACKS

Attackers exploit many types of UDP amplification attacks that can leverage several different network services; ranging from DNS, NTP, SNMP, Memcached, and more. Though these attacks differ slightly on a technical level, they all share three common properties. They benefit from being UDP-based, they exploit network services that are commonly exposed to the public, and they offer an asymmetric scaling factor—sometimes exponentially. Let's discuss why these three properties matter, and how they interact together.

- **Leveraging UDP-based network services** – Since UDP traffic is connectionless, it's extremely easy to spoof. A hacker can simply send a UDP packet using your computer's IP address, and since the protocol doesn't requires pre-negotiation, the recipient just accepts that packet as yours rather than the attacker's. This spoofing offers two advantages to attackers. The first is anonymity. For example, attackers can send UDP packets directly to a victim, but lie about where those packets are coming from using random source address IPs.

  The second advantage—and the more important one to UDP amplification—is to "reflect" a packet using UDP spoofing. In this case, rather than sending a packet directly to a victim, the attacker sends a packet to some third-party server, but uses the victim's IP address as the source of the packet. Since UDP is connectionless, the third-party server blindly sends its reply to the unknowing victim. This is why some experts call these attacks reflective, or UDP/DNS reflection.

- **Bouncing off of public Internet services** – To succeed at scale, UDP amplification attacks need public network services to take advantage of. You just learned how UDP traffic allows for spoofing, which in turn allows for reflective attacks. However, attackers need publicly accessible, third-party servers to reflect their attacks off of. Ideally, they need ***a lot*** of publicly accessible servers, because more servers can allow attackers to generate more traffic. In general, UDP amplification attacks work best with network services that are commonly found on the public Internet, which is why DNS—the most common public UDP service—was the first one to be targeted with UDP amplification attacks.

  However, DNS is not the only common public network service using UDP. After early DNS amplification attacks paved the way, DDoS attackers quickly found they could also leverage public NTP, SSDP, SNMP, TFTP, and many more UDP-based services in the same way. That said, one aspect of whether or not these UDP amplification attacks succeed is just how common a particular public UDP service is. Simply put, there are a lot of public DNS servers attackers could potentially reflect traffic off of, so they provide ample opportunity to scale a UDP attack. Meanwhile, you probably won't find that many public Quake Network servers today, so even though that UDP service is technically vulnerable to this sort of attack, it wouldn't generate the largest DDoS attacks.

- **Offering an asymmetric scale factor** – The final property in the UDP amplification equation is the asymmetric scaling factor. Simply put, this means that something in the specific protocol allows for a short request that results in a much longer reply—sometimes exponentially longer. For instance, the most common DNS amplification request involves the resource record type "ANY."

In a nutshell, sending a small DNS request of type ANY to an authoritative DNS server's zone name returns a large reply containing all the records at the apex of the zone. If the server uses DNSSEC, the reply gets even bigger with keys and signatures, and other content. So, attackers can spoof and reflect a single packet that is only tens of bytes, to generate a response to the victim that is thousands of bytes. The spoofing allows reflection, and the asymmetric aspect of some protocols' replies allow the true scale for these attacks.

As with all other aspects of this attack, there are many UDP network services that have some sort of request/reply scaling factor. Another key factor for how bad an UDP amplification attack could be is the size of this scaling factor. Luckily, US-CERT recently released a great alert that quickly shows you the scaling factor of various UDP-based services vulnerable to these sorts of DDoS attacks. Here are a few examples:

UDP-Based Protocol	**Scaling multiple**
DNS	28-54x
NTP	556x
SNMP	6.3x
CharGEN	358x
Memcached	10,000 – 51,000x

Seeing those scaling multiples, you can probably guess why Memcached UDP amplification attacks now hold the DDoS record of 1.7 Tbps of bandwidth. If you can send a small spoofed request and get a public server to generate a reply 50 thousand times the size to anyone else on the Internet, it becomes trivial to eat up that victim's bandwidth and resource.

To summarize, UDP amplification attacks succeed because UDP is spoof-able, that spoof-ability allows attackers to reflect requests off common public servers to unknowing victims, and some UDP services allow for tiny requests that generate exponentially large replies. While each of these UDP services have slightly different request characteristics, all UDP amplification attacks essentially prey on these three issues combined together.

DEFENSE AGAINST UDP AMPLIFICATION ATTACKS

Protection is a little more difficult to describe because some protections require broader industry participation. From a DDoS victim's perspective, there is little one can do to avoid reflective UDP amplification attacks. As a starting point, you should adopt some sort of DDoS protection service that scrubs your traffic upstream.

For organizations that might expose public UDP services to the world, you should definitely be aware of these attacks, and which services are vulnerable to them. US-CERT's alert is a good resource for understanding the services you should know about. However, hardening your public servers against these attacks differs depending on protocol. A general tip here is to avoid exposing any protocol features that are unnecessary or at least limit them to a specific access list.

Finally, there is something all network owners (most importantly, ISPs) can do to really nip amplification attacks in the bud: block spoofing at a network layer. Ultimately, UDP amplification attacks hinge on the ability to spoof traffic from others. If attackers can't spoof traffic, they can't reflect attacks to a victim. It's trivial for network perimeter devices to detect spoofing. You know what IP address space you own. If your gateway device sees traffic coming from your network, claiming to be any IP you don't own, you should block it. In fact, IETF has a published best practice (BCP 38) that specifically outlines how ISPs and network owners can and should block all spoofing at their perimeter. If the industry as a whole adopted this, UDP amplification would fade into history.

This won't be the end of huge DDoS attacks. Between botnets – IoT or otherwise – and organizations that don't follow best practices, these attacks will continue to evolve. Rather than being part of the problem, you can help drive us all toward the solution by making sure to implement anti-spoofing features on your gateway devices, and asking your ISP if they're doing the same.

About the Author

Corey Nachriener

Recognized as a thought leader in IT security, Nachreiner spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Nachreiner has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends.

As an authority on network security and internationally quoted commentator, Nachreiner's expertise and ability to dissect complex security topics make him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, eWeek, Help Net Security, Information Week and Infosecurity, and delivers WatchGuard's "Daily Security Byte" video on Facebook.

WAKE-UP CALL FOR ERP USERS

Cybercrime has become a top concern for the contemporary world. To protect themselves, many organizations have stockpiled solutions against outside attacks—while ignoring the more ominous threats right under their noses.

According to IBM's 2016 Cyber Security Index, 60 percent of cybersecurity breaches come not from an unknown outsider, but from the inside—at the hands of employees. Other sources cite higher numbers upwards of 75 percent. In Cyber Insider's 2018 Insider Threat Report, 90 percent of security professionals reported feeling vulnerable to insider threats.

Some attacks are malicious, with disgruntled workers taking revenge by disabling systems, committing fraud to embezzle money, or profiting by selling company or client data on the dark web. Many other breaches happen inadvertently, the result of worker error or inappropriate permission rights to information.

As a growing number of organizations use enterprise resource planning (ERP) solutions to manage their core business processes, they also have to safeguard against vulnerabilities that can come with ERP use. ERP systems, which provide a unified platform for accounting, human resources, purchasing, sales, and other departments, help businesses run more efficiently. The danger lies in the complexity of the systems, too much internal access to sensitive data and weak controls.

Since attention to internal cybersecurity has lagged behind the emphasis on external threats, companies have only begun to take internal risks more seriously. Increasing education and developing prevention programs are key components in correcting the inequity between the two.

A WAKE-UP CALL

Shockingly, there are companies that never analyze the permissions assigned to their ERP users. One reason for this is a tendency for companies to be reactive rather than proactive when it comes to internal risks, waiting until a costly or critical breach occurs instead of preventing incidents to begin with.

Conversely, all businesses understand the urgency in having a security system to prevent physical intrusion into facilities and to thwart external hacks into systems. They don't wait until a break in or breach takes place to protect valuable assets.

And yet, "privilege creep," in which an employee may gain increasing access as their roles and permissions change—even beyond what they need or should have—happens all of the time if not monitored. Another common problem is granting privileges that mirror existing user access when onboarding new users. Over time, a company can create their own worst permission-bloat nightmare.

Without regularly evaluating their ERP access and security, enterprises leave themselves incredibly exposed to inside cyber hazards.

PREVENTION IS MORE THAN JUST AN OPTION

There are steps an organization can take to guard against insider attacks, even of sensitive ERP systems. The first step is to acknowledge the problem, and take internal threats seriously. Even small enterprises where "everybody knows your name," can be vulnerable—particularly so, if the intimate atmosphere creates a sense of complacency.

Secondly, prevention has to move to the forefront of internal cybersecurity. Once a company has acknowledged the real possibility of employee-based access violations, take steps to:

- **Safeguard against mishaps and insider fraud with tight and agile controls**. Double check who has access to what to avoid "privilege creep," making sure that each employee has only the access they need to perform their job. This important precaution is often overlooked—but it's the authorized access, not the unauthorized, that so often gets organizations in trouble. It's a daunting task to do manually, but it must be done if an automated solution is not in place.
- **Understand the most common segregation of duties (SoD) conflicts.** Is it possible for a single person to access all the processes involved in doing business in your organization? This end-to-end access is the linchpin of a security crisis. Analyze your SoD policies and procedures and redefine them where needed, then audit them continuously to ensure that they are being followed and are working.
- **Educate users on security protocols.** How security-aware are your employees? Your executives? Everyone in the organization, regardless of role, needs thorough training and regular refreshers on secure password protocols and proper use of ERP systems.
- **Review your sensitive access monitoring controls *at least* once a year.** Even the strictest controls can have "cracks." Checking for them, and for suspicious behaviors, is key to prevention and early detection of insider breaches. Have a system in place to continually monitor privileged users' activities—and to alert you to attacks. Track changes to critical data, as well, and set up audit trails on important transactions.

In the increasingly fast-paced world of business with global employees and many points of access in extremely large organizations, monitoring your ERP for internal security breaches isn't a nice-to-have option. It's a must-have.

When it comes to ERP security, the devil is in the details—often, in the ones you can't see due to lack of attention on them or tools to simplify spotting them. The biggest risk to any enterprise's security comes not from employee actions, but organizational inaction: the failure to act until after a breach occurs.

About the Author

Jody Paterson is the CEO of ERP Maestro.

He is a security evangelist, thought leader, speaker and KPMG veteran who is committed to creating smarter ways to keep companies secure on the inside and ease the burden of managing, monitoring and auditing access to critical business systems.

Jody can be reached online at jody.paterson@erpmaestro.com and at our company website http://www.erpmaestro.com

FACEBOOK EXTENDS A PRIVACY OLIVE BRANCH TO USERS

By Dan Goldstein and Jill Messinger

Data privacy is a big issue today. Just a few weeks ago, cable news pundits were breathlessly describing the wide ranging impact of the Cambridge Analytica scandal. More recently, SEO and online marketing publications have been highlighting the EU's General Data Protection Regulation (GDPR). When you combine this with high profile data breaches from large corporations, it is no wonder that the public is becoming more skeptical of the way large companies and online platforms safeguard their users' privacy.

Many users have lost faith in Facebook's ability and desire to protect user privacy with some deleting or threatening to delete their profiles altogether. In fact, a recent Reuters poll shows that a majority of Americans don't trust Facebook to obey laws that protect their personal data.

FACEBOOK RESPONDS

Facebook has responded to this new reality and seems to be getting the message that privacy and transparency are important to its users. It started with Mark Zuckerberg's public testimony before a congressional committee, but Facebook has not stopped there.

Last week, Zuckerberg announced a new Facebook privacy control feature, called Clear History. The announcement came both through his personal Facebook account and at the F8 annual developer conference in San Jose, California.

Clear History will provide Facebook users the ability to clear cookies and history within the social media platform, including the websites they've visited and content they've clicked on. And while this new privacy feature was surely developed to improve Facebook's reputation in the current climate, it will definitely affect the way the social platform is utilized - both for users and marketers.

THE CAMBRIDGE ANALYTICA DEBACLE

Before we get into the Clear History update, let's review what happened with Cambridge Analytica and how that differs from typical Facebook advertisers.

Cambridge Analytica had access to private user data that was harvested by a professor at Cambridge University (Dr. Aleksandr Kogan). According to Recode.net, Dr. Kogan created an app called "thisisyourdigitallife" that utilized Facebook's login feature.

Approximately 270,000 people used the Facebook login feature to create accounts on "thisisyourdigitallife.com". From those 270,000 logins, Kogan was able to access personal data from approximately 50 million Facebook users (Facebook friends of the initial 270,000 users). Of those 50 million users, Cambridge Analytica was able to harvest detailed personal data on approximately 30 million people to build psychographic profiles. Cambridge Analytica then sold its services to the Trump campaign.

After that personal data was gathered by Kogan and sold to Cambridge Analytica (allegedly against Facebook's Terms of Service), Facebook closed the loophole to prevent other app developers from gathering users' private data through the Facebook login vehicle.

PRIVATE DATA AND THE FACEBOOK EXPERIENCE

Today, Facebook advertisers don't have access to the private information that was used and manipulated by Cambridge Analytica. In fact, Facebook users are typically served advertisements via information they voluntarily provide, such as marital status, date of birth, where they graduated college, where they live, as well as companies, interests, and brands they "Like".

Of course, a significant amount of targeting data also stems from external websites, search queries, and data collection companies. However, this data is not shared with advertisers. Rather it is used by Facebook to ensure that an advertiser's ads target the right users. This benefits the advertiser and makes the Facebook experience more enjoyable since each person is served ads that are specifically relevant to that user.

The high degree of personalization on Facebook is what makes each individual user's experience feel unique. It's essentially what makes Facebook, Facebook. Content, friend suggestions, apps, advertisements, etc. are all targeted to specific individuals based on their interests, which is accumulated over time as you use Facebook and the Web.

COULD CLEAR HISTORY HURT FACEBOOK USER EXPERIENCE?

When Zuckerberg made his Clear History announcement, he acknowledged that "when you clear your cookies in your browser, it can make parts of your experience worse. You may have to sign back in to every website, and you may have to reconfigure things. The same will be true [with Facebook's Clear History]. Your Facebook experience won't be as good while it relearns your preferences."

For Facebook users, restricting what Facebook knows about you through your online history will probably result in a much more generic experience, at least initially. It will be interesting to hear user feedback after the Clear History option is released.

Privacy advocates have been lobbying for stronger privacy settings and increased transparency so users can see what is happening with their private data. Facebook's Clear History is a good step in that direction. It remains to be seen, however, how many Facebook users will actually take advantage of this option. And, for those who try it, how many will regularly go back and use it again, particularly if the user experience is more generic.

SOCIAL MEDIA MARKETING IN THE AGE OF DATA PRIVACY

From a marketing standpoint, Facebook's in-depth understanding of its users, both demographically and geographically, makes Facebook an ideal advertising platform. It allows advertisers to ensure that their ads are reaching the right target audience at the right time.

Here at Page 1 Solutions, we work with clients in the plastic surgery, cosmetic dentistry, ophthalmology, and personal injury law verticals. Our marketing specialists rely on Facebook to build our clients' brands and market their services directly to people who those clients can help. For example, if a law firm wants to generate new cases involving nursing home abuse and neglect, it can use Facebook to advertise to a highly targeted audience. In addition to restricting the ad campaign to users in the appropriate geographic and demographic groups, we can narrowly target the ads to people who have searched for or expressed interest in things like nursing homes, caretakers, elderly care, negligence, lawyers, legal advice, and so on.

If Clear History is widely adopted by Facebook users, a similar ad campaign would have to cast a much wider net and would not be able to target the right people at the right time. This could mean that many users with no interest in our clients' services would be served nursing home neglect ads, whether or not those ads are relevant to them. We expect that such a campaign would irritate users and waste our clients' marketing dollars. In the long run, advertising without precise targeting options and user data could delegitimize Facebook as a viable advertising platform altogether.

CONCLUSION

Facebook is taking appropriate steps to appease privacy advocates and reassure users that their privacy is a priority. It will be interesting to see if Facebook's newfound belief in user privacy is enough to win back the trust of its users. And, if Clear History is widely used, there is an open question as to whether it will kill Facebook's golden goose.

Dan Goldstein is the president of Page 1 Solutions, LLC, and Jill Messinger is a Social Media Specialist at Page 1 Solutions, LLC. Page 1 Solutions is a website marketing company providing SEO, website design, social media marketing, reputation management, and more for attorneys, plastic surgeons, dentists, and ophthalmologists. Dan can be reached at DanG@Page1Solutions.com and Jill can be reached at JillM@Page1Solutions.com.

FIVE RED FLAGS YOU HAVE A CYBER SECURITY INSIGHTS PROBLEM

By Nik Whitfield, CEO, Panaseer

RED FLAG ONE: YOUR BOARD, ITS REGULATORS, AND EVEN AUDITORS WANT CONTINUAL REPORTING

Cyber security has hit the board-room and above with a splash. In years past it was the CISO and/ or CTRO's role to come up with a plan, present it to the board, negotiate the budget and come back next year. But in today's data-driven customercentric world where the risks have significantly increased ongoing monitoring or updates to the status of the organisational cyber security health has become a board topic. It's no wonder as the backlash of a breach today comes with a significant price tag both financially and to the brand.

Symptoms: A lack of confidence in the data being presented and a gut-wrenching feeling that the data is not really meaningful or useful.

RED FLAG TWO: ROI IS NOT A 'NICE TO HAVE' BUT RATHER MEASURED AND EXPECTED

In tough financial and economic environments globally, budgets are shrinking. If money is to be spent on security, there needs to be a demonstrable return that the business is recouping in return a level of risk reduction. Every security team is now required (and if you aren't you will be soon) to show that what they are doing is having an effect and additionally that every product or solution is being squeezed for any ounce of value.

Symptoms: You haven't got a view of the coverage of your existing solutions across a trusted device inventory list.

RED FLAG THREE: TEAMS SPENDING TOO MUCH TIME WITH THEIR HEADS IN DATA

If your teams are experiencing any of the following it should be a red flag to you that things are not working to plan:

- You're spending more time on fighting over data integrity than actually solving the problem
- Teams are challenged with the same time sucking manual problems month on month.
- Results are out of date the moment they are finalised, or you're pretty sure they are incomplete
- You've had to go back the next month and apologise for getting your figures wrong

Symptoms: These are usually pretty obvious, the loudest most often being Security teams complaining about the amount of reporting they have to do

RED FLAG THREE: YOU'RE NOT QUITE SURE IF THE BASICS ARE GETTING DONE

Just know you aren't alone. Getting the basics done can often be the most challenging part of the security process. When you have tens to hundreds of thousands of devices and often complex environments it can be difficult to keep track.

Organisations of all sizes struggle to keep on top of the almost daily requirement for something to be addressed. But the reality is that most breaches and especially the large ones always come back to the basics such as a missing vulnerability patch or an unsecured server that fell off the radar.

Symptoms: The performance of vulnerability and patching of devices is more guesswork than fact, or the installation, configuration and operational effectiveness of your anti-malware solutions is more folklore than reality.

RED FLAG FOUR: PAM IS A DIRTY WORD

You will always need to allow people access to systems and sensitive data, but let's face it, they also represent a vulnerability that attackers can take advantage of. Balancing ease of access with security is a difficult challenge to maintain a safe yet still productive environment. If you aren't auditing and monitoring these effectively, you could be leaving the keys to the castle on the table. With the complexity in most organisations, it's hard to identify and reduce the risks, even harder when you have privilege users circumventing specific PAM controls.

Symptoms: Are you sure all ex-employees have had their rights revoked? If the answer is 'I'm not sure,' you've got yourself a red flag.

If any of these ring true, and especially if more than one is playing havoc with your sanity, it's time to take a step back as you most likely have an insight problem. You are missing a vital ingredient in your organisational arsenal as true insight can help you face the challenges of security differently. This isn't about finding yet another new security solution that relies on addressing the FUD approach of firefighting. Instead, how liberating would it be to approach the problem by fireproofing your organisation? Actually staying ahead of the game. By leveraging insight, you can know where your weaknesses are, understand your areas of opportunity to reduce the risk within your organisation, and have the power to make informed decisions based on fact, not fiction.

That requires a commitment to being truly data-driven and leveraging the data that already exists within your organisation, within your existing products and solutions. Combining your security, business, and IT data into a single trusted source, giving it life and a voice by using the right best-practice security metrics and analytics. Automation of this process is not a choice anymore; it's a must. And finally, it's about building trust. Working against a single source of trusted data security, risk and IT can work in a single unified direction.

About the Author

Nik Whitfield, *CEO, Panaseer*

A globally recognised figure in the field of cyber and financial technology, Nik brings direction and leadership to the team, where he applies his phrase #deservetowin daily.

NEW REGULATIONS GOVERNING DATA PROTECTION – INCLUDING THE USE OF ENCRYPTION – NOW IN EFFECT IN THE EU AND NEW YORK STATE

By: Ruben Lugo, Strategic Product Marketing Manager at Kingston Technology

Even in a divided, conflicted world, there is one thing everyone can pretty much agree: security breaches and cybersecurity issues leading to the use of stolen or compromising of personal data is a major, major issue. Not just in a few isolated places around the world, but in every corner of this round planet we call Earth.

Recently, several new regulations went into effect that take giant steps in requiring businesses to do something about protecting people's identity. Or, if not, face some unpleasant penalties.

These new stronger regulations are the European Union's General Data Protection Regulation (EU-GDPR) and the New York State Department of Financial Services' 23 NYCRR 500. The former, which has an enforcement date beginning May 25, 2018, pertains to any organization – EU or non-EU – that works with information relating to EU citizens. The latter, which went into full effect on February 15 of this year, relates to New York insurance companies, banks, and other regulated financial services institutions as well as anyone who provides a service or is on contract as a vendor to these industry firms, including agencies and branches of non-US banks licensed in the state of New York.

Both of these, quite simply, require all businesses or organizations that fall into the categories above and who process or hold personally identifiable information (aka PII) to implement adequate security measures – including the use of encryption – to protect said data, regardless if it is "at-rest" or "in-transit," or be ready to face sanctions and law suits.

In the EU regulation, personally identifiable information refers to data held about EU citizens that, if disclosed, could result in damages to those whose information has been compromised. It can include medical records, biometric data, passport numbers, and personally identifiable financial information (PIFI), such as social security and credit card details. Information that might not be considered PII, such as first name and surname, can become PII if linked to other data.

New York's says personally identifiable information, or sensitive personal information (SPI), is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. The National Institute of Standards and Technology's (NIST) Special Publication 800-122, which the state referred to in its regulation, defines PII as "any information about an individual maintained by an agency, including,

(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and,

(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

In either case, an organization's data assets should be identified as part of a risk assessment, including how data is stored and accessed, what level of risk it's exposed to and whether it contains PII. Data assets might be stored in application databases, server file systems, and on end user devices.

Both regulations require notification of a data breach within 72 hours of learning of an occurrence.

So, what kinds of penalties are we talking about? As you might imagine, drastic times take drastic measures.

Under the GDPR regulation, non-complying organizations can be fined up to 4 percent of annual global turnover or €20 million (in the neighborhood of $24 million USD) or whichever is greater. Companies can also be fined 2 percent for not having their records in order, not notifying the supervising authority and data-subject about a breach, or not conducting an impact assessment.

The New York regulation does not specifically detail any potential penalties or the impact of noncompliance. Instead, it passes enforcement to the superintendent of the New York State Department of Financial Services, who will be guided by the New York Banking Law.

Under that scenario, penalties would range from license revocation and/or fines up to (a) $2,500 per day during which a violation continues, (b) $15,000 per day in the event of any reckless or unsound practice or pattern of misconduct, or (c) $75,000 per day in the event of a knowing and willful violation.

So far, we have provided you broad overview of the regulations. Now, let's take a closer look at each.

There are five primary areas to concern yourself with in order to meet compliance:

1. Encryption of sensitive data, both in-transit and at-rest
2. Appointment of Data Protection Officers (for companies of 250 or more people)
3. Establishment of a cyber security program
4. Documented accountability
5. Understanding consent

This is hardly a complete listing, but here are five things you should do to ensure compliance:

1. ***Self-evaluate*** – have your Data Protection Officer conduct an internal review of the handling of personally identifiable information of your employees and customers.
2. ***Map internal and external products / devices that store data*** – log and require company equipment used, to be covered under your data security policy and ensure data encryption is utilized with items such as servers, hard drives, USB flash drives, computers, and mobile devices.
3. ***Take Inventory Analysis*** – evaluate the total amount of personal data in your system.
4. ***Purge*** – eliminate archives of unnecessary PII.
5. ***Controllers of Information*** – review privacy risk and impact assessments.

Two more things to know about the EU-GDPR. The first is *consent*. The conditions for consent have been strengthened, and companies will no longer be able to use long unintelligible terms and conditions full of legalese. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

The second is the right to be forgotten, also known as *Data Erasure*. The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing the data. The conditions for erasure include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent.

23 NYCRR 500

Similar to those listed in the EU-GDPR section, here are five primary areas to be concerned with in order to be compliant with New York State's 23 NYCRR 500:

1. Encryption of sensitive data, both in-transit and at-rest
2. Appointment of a Chief Information Security Officer (CISO)
3. Establishment of a Cyber Security Program
4. Adoption of a Cyber Security Policy
5. Manage third-party service providers, by including
   - Annual penetration tests
   - Bi-annual vulnerability assessments

New York's sweeping regulation holds state-chartered banks, foreign banks licensed and operating in New York state, insurance companies, private bankers, mortgage companies, and other financial service providers strictly accountable for shielding both in-transit and at-rest data. It also mandates that companies define criteria, have an incident response policy, and update vendor management with minimum standards to do business with the financial institutions. Organizations are also required to include these enhanced data-encryption standards in their contracts with third party service providers.

ENCRYPTION IS KEY

The best way for an organization to be sure that it is complying with either regulation is to implement appropriate safeguards, technical standards, and policies, including data encryption of personal data. Both regulations require organizations who process or hold personally identifiable information to implement adequate security to protect personal data loss.

Likewise, to somewhat differing degrees, both require organizations to encrypt sensitive data, both in transit and at rest to ensure a level of security appropriate to the risk. This can be achieved through the use of secure, encrypted USB flash drives, such as Kingston's lines of Kingston and IronKey Encrypted USB drives; security solutions for outside the firewall.

Of these, a USB drive with hardware-based encryption is an excellent, simple security solution to protecting data from breaches, while also meeting evolving governmental regulations. Such devices that meet tough industry security standards offer the ultimate security in data protection to confidently manage threats and reduce risks.

A hardware-centric/software-free encryption approach to data security is the best defense against data loss, as it eliminates the most commonly used attack routes. This same software-free method also provides complete cross-platform compatibility with any OS or embedded equipment possessing a USB port and file storage system.

About the Author:

Ruben Lugo is the Strategic Product Marketing Manager for Kingston's encrypted USB line, including the globally respected IronKey line of ultimate security encrypted USB drives as well as Kingston's Server Premier DRAM and Enterprise SSD / NVMe solutions for today's high-performance servers. As a solutions, technology and security enthusiast with over 18 years' experience, he leverages his unique expertise in the development, delivery and sales / marketing management from the CE, AV and IT Networking industries. He's contributed to the initiation of new trends in technology from launching the first reliable wireless high definition audio video distribution system to high-bandwidth fiber optic networking solutions.

KNOW YOUR DATA

IMPROVING BUSINESS CYBER DEFENSE

by Charles E. Caldwell, CEO, GEM Analytics

What do you need to know about your data? More than you think. All of the data and information in your business can give you insight on levels and sources of risk, plus highlight opportunities. Executives know their business, but can also learn more by managing analytics as assets. C-suite teams can gain a distinct advantage by learning how to apply data and advanced analytics to improve use of capital and resources. CIOs cannot do all heavy lifting alone when they are maxed out managing systems and applications.

Running a successful business depends on how you create value. You must know how activity creates value to heighten level of understanding. The lack of critical types of data is why companies fail to measure true value creation. Decades of research and public relations disasters reveal why businesses still need to learn how to manage vast amounts of data as an asset. When thinking about this problem, consider how your business has evolved. It has taken years of hard work to grow your business. Capabilities and practices are constantly being cobbled together to support operations. Complexity blooms as system and application functionality grows. At the same time, data and information multiplies rapidly. Keeping up with this level of expansion is impossible unless you change your thinking about how to use your assets more wisely to drive growth.

Cyber defenses rely on how you manage data and information. Businesses need to modernize data architectures to enhance use of data assets. Start the process by focusing on four concepts: who you are, what you do, what you need, and what you want. This might seem like Business 1.0, yet it is not. You will need focused insight and tools to manage your data and guide your transformation.

BASELINE OF MEASUREMENT

Your first step is to set a baseline of measurement to evaluate effectiveness. This entails converting historical data and information into a framework to measure your value creation. This baseline model creates the foundation you need to align assets and resources to maximize value creation. Then it is possible to apply Artificial Intelligence (AI) and Machine Learning to enrich your information to give you more business insights. Advancing your business is easier once you benchmark state of effectiveness.

BUSINESS POTENTIAL

Better management of data assets creates opportunity to reduce risks. Your best defense against being hacked is to improve your data architecture to reduce sources and levels of risk. Your business functions based on the products and services you deliver. Structure, process, capabilities and decision-making of every business are different. There are no “one-size-fits-all” solutions. Once you establish a baseline of measurement, you create opportunity to “know” your business potential. Your mission is to optimize your business and to implement strategies to grow profits. This is possible when you improve knowledge worker productivity, lower costs and maximize use of capital and resources. Opportunity to realize your business potential depends on how you use insight to develop and implement step-change strategies, solution roadmaps and action plans to modernize operations.

ACTIVITY TO VALUE INSIGHT

Activity-based insight will help you to align capabilities, practices and resources to optimize value creation. The objective is to optimize use of resources and efforts to increase returns for your business. Insight about how day-to-day work activities impact value creation can be game changing. Gaining new perspective about your effectiveness will help you focus on making the best improvements.

Business transformation is an ongoing process. Decision-making slows down and is often paralyzed by overwhelming amounts of information. This issue impacts innovation. Activity to value insight will help you improve business agility and expand returns on investments. Avoiding pitfalls that hinder work and degrade value creation is critical. This is why need to create activity-based insight is significant. See what you need to see to know how to run your business more effectively.

RISK AVERSION

By the time many businesses react to changing situations, it is too late. Reactionary management is expensive. In some cases, lack of an appropriate response can put you out of business. Why would you not want to avoid adverse situations in the first place? Today, you can use new technologies to reduce risk. Of course, this depends on how you anticipate change. Getting in front of change creates opportunity to preempt situations that can have an adverse effect on your business. Predictive data can give you a sizeable advantage by helping you improve your position to gain an edge.

To understand your problems, take a deeper look at your current situation. Look at what you are doing today versus what you could be doing to improve your positioning. Predictive data can help you model hypothetical situations to evaluate future areas of

risk and opportunity. Taking steps today to avoid future risks can be substantial. Know what is possible so you can reduce risks and seize better opportunities.

STEP CHANGE STRATEGY

Step Change is the process and actions you take to leap into the future. Step change involves getting people engaged to realize the best opportunities. Pulse Surveys are tools you can use to drive engagement. People do not like to change. There has to be a definitive reason to drive change. What's-in-it-for-me concerns must be served to satisfy needs. The objective is to take a giant leap forward to be where you want to be to take the best advantage of your current situation.

Ability to implement strategy is complex. How will you get your people involved? What do people need to know to change perspective about their work? The answers depend on what people know and do not know. People are so busy working that they seldom think about how they work. Being busy and creating value is not the same thing. Predictive insight can be eye opening. Sometimes all it takes is one "aha" moment to change a perspective. Strategy execution involves getting people to engage. Work must be meaningful and needs must be respected. Turning a negative situation into an opportunity is possible if you can change your thinking. Predictive insight makes change possible when people do the right things.

DATA ARCHITECTURE

One of the greatest challenges businesses face is data. Advancing technologies, globalization and growth of the Internet represent a few drivers that have changed how people work. Businesses that do not recognize and adapt to this change are at risk. Cause and effect are realities of situations and actions. Business structures must adapt to support the way people "need" to work. Removing structures and silos of business to make work flow more efficiently is vital. As information has grown, knowledge worker productivity has declined. People are working more hours and getting less done. This is because current data structures have become extremely inefficient.

MODERN DATA ARCHITECTURE

Information growth has created a great amount of instability for business. When we analyze data structures, we discover that data and information is everywhere. Levels of redundancy, bottlenecks and inefficiencies create risk. Need to connect "data dots" between disparate systems and applications has built an unsustainable structure of data that is impossible to maintain and extremely expensive. The result – more and more businesses are getting hacked. There is only one solution, businesses need to simplify how they manage and use information.

Your opportunity is to focus on improving the quality and use of your data and information. Activity to value insight will help you quantify risks and costs as you model inefficiencies that affect your business. You need to develop a data architecture that meets the needs of your business. This is extremely complex and difficult, but possible when you know what to do. Currently, businesses do not have the tools and insight to do this work efficiently. This is why this work is not getting done. Focus on learning more about what people do each day to learn more about your strengths and weaknesses. The answers you need become more obvious when you know your data.

About the Author

Charles E. Caldwell is CEO of GEM Analytics. He is a performance management specialist with strong operations and development experience who provides thought leadership and subject matter expertise to executives, solution providers, project managers and consultants who need strategic insight, advanced data analytics, AI diagnostic tools and know-how to help businesses grow profits. Charlie can be reached online at (chas@glbvst.com, @chas628_gem) and at http://www.gemanalytics.com/

THERE IS NO SILVER BULLET FOR CYBER SECURITY BUT UNIFIED DEFENSE IS BEST APPROACH

By: Mohammad Jamal Tabbara, Senior Systems Engineer – UAE & Channel at Infoblox

Enterprises of all sizes are falling victim to very determined malicious actors whose motivations range from financial gain to government sponsored campaigns. The threats are not limited to commercial enterprises but have significant impact on civilian and non-civilian government agencies.

The nature of what organization must address has changed dramatically over the past decade. The threat surface has expanded significantly, the nature of the threats is evolving at an unprecedented rate and the complexity of what makes up an organization has grown. Organizations have migrated from having a tightly controlled network with endpoints and devices provided by the company, to one where the very definition of an endpoint and device is changing, driven by the proliferation of the Internet of Things (IoT), organizational policies to allow employees bring their own devices on the network (BYOD) and the adoption of private and public cloud deployments. The definition of a network has changed too, it is no longer a walled garden but an amorphous structure where users can access organizational resources from anywhere, anytime, and from almost any device.

To counter these factors, organizations have started implementing solutions to address security. However, this might be a disappointment to several of you, but reflects reality. **There is no silver bullet!** - no single solution that can address all security issues. A “defence in depth” approach did not come about by accident but is based on the determination that while you might need a thousand solutions in your network, you need solutions that address different aspects of security.

You are not alone. Your networks have changed significantly and you have multiple solutions. That establishes a baseline. The question is what can organizations do differently to be better prepared. Here are some suggested best practices.

INTROSPECTION

This means understanding your capabilities and risks. Just understanding the impact of being breached in terms of cost, downtime and reputation of the brand will help you prioritize what actions to take.

GET VISIBILITY

Develop a clear picture of the key assets you have, where they are located, who has access to them, identify the most critical assets. In the digital age, data is king so knowing which devices have access to your data is key. Note that data is not just the domain of the large enterprise, but a reality for every size and type of organization. This assessment will lead to you the determination of what makes up your organization.

EXAMINE YOUR ARCHITECTURE

With the proliferation of IoT, adoption of BYOD, growth in use of virtualized environments, and adoption of public and private cloud infrastructures – all require that you step back and examine how you architected your core network. Focus on the outcomes you desire while you examine the architecture – is your network architected to maximize availability and ensure continuity even if it is under attack, have you secured your data paths to make sure you are protecting every known avenue that can be used to steal that data, does your protection extend to the physical and virtual elements in your network.

DO A PROCESS INVENTORY

Technology is a key element to addressing security challenges, but technology is part of the solution. People and processes play an equally important role in maintaining a robust security posture. Developing an understanding of how sensitive information is handled, who has access to sensitive information, your internal policies on how you treat sensitive data, policy enforcement mechanisms and ongoing training of personnel handling sensitive data must be part of the overall solution.

START BY ADDRESSING THE BASICS

Often organizations invest in the latest and greatest technology and buzz word driven solutions. Sometimes there is a perceived correlation between “high end solution” and impact. But there is a difference between perception and reality. Organizations must start with the basics.

INSTITUTE BEST PRACTICES

Like I said above, people and process are a critical component of addressing your security posture. Make sure you have instituted best practices around passwords, patching your systems with the latest updates and keeping up to date with your hardware and software.

ADDRESS THE CORE OF YOUR NETWORK

Organizations that have adopted a defense in depth approach have done so for several critical applications like e-mail, web traffic and endpoints. Often, they ignore the core of their network –the basic systems that allow access to applications and services on their network. In other words, core elements like DNS, DHCP and IP address management, often referred to as DDI.

GET HELP

Too often organizations rely on internal expertise, but budget constraints and the availability of trained security experts constrain their ability to have the extensive coverage they need. Help comes in many forms, technology and external expertise. Augmenting the team's skill sets with the latest development in technology that allows automation and leverages machine learning to drive better insight into threats is key. Relying on security expertise from organizations that specialize in security is often underutilized.

UNIFY YOUR APPROACH

Make sure that all the elements of your defense in depth approach work in unison. This means that when one system sees a vulnerability that information should be shared with the other parts of the infrastructure. Whether that information is an indicator of compromise or threat intelligence – the information should be shared. For example, if your DDI infrastructure identifies a new device on the network, that information should be shared with a Vulnerability Scanner so it can scan the device to ensure its integrity. While the information in isolation is useful (a new device on the network) it is becomes actionable and more impactful when it is shared with other parts of your infrastructure. Of course, this requires that the vendors you select have an open approach and have built their products with the ability to share information with other parts of your infrastructure.

IN TODAY'S THREAT LANDSCAPE, CHOOSE AN OUNCE OF PREVENTION RATHER THAN A POUND OF DETECTION

By Joe Saunders, RunSafe Security CEO

Cybercrime is on the rise and becoming one of the biggest threats to business operations and continuity. While many cyber security companies continue to focus on detection, increasingly sophisticated criminals are finding new ways to sidestep these solutions. As such, it is now more important than ever to move beyond simple detection-based security to a more proactive strategy that stops attacks before they happen. In these perilous times, an ounce of prevention can carry far more weight than a pound of detection.

TRADITIONAL SECURITY MAINLY DETECTS SYMPTOMS

Last year, Cybersecurity Ventures predicted that cybercrime will cost the world up to $6 trillion per year by 2021, roughly double the global costs of 2015. The firm said cybercrime will soon grow to become the greatest transfer for wealth in history, and eventually become more profitable than the entire illegal drug trade. But not only are attacks becoming more frequent, they're also becoming more sophisticated. Hackers are hitting organizations of all sizes with ransomware, DDoS attacks, phishing and Zero Day exploits on a regular basis. Even the FBI is having trouble keeping pace.

Despite the growing threats, traditional security measures continue to focus on detecting symptoms of attacks. They use *external* network and perimeter technologies such as gateways, firewalls, intrusion prevention and antivirus agents.. In addition, *internal* approaches such as static and dynamic analysis are used to try to detect vulnerabilities in code.

The problem with such traditional security is that it focuses more on *detecting* symptoms rather than on addressing the underlying cause(s). While established tools have worked for decades on known attack types, their effectiveness is diminishing as hackers with time and financial resources become increasingly skilled in designing attacks to avoid detection.

For example, buffer overflows are one of the most common memory corruption vulnerabilities in software. In these hacks, attackers insert data with code designed to trigger specific actions that could damage files, change data or expose confidential information. These attacks sidestep traditional external detection and are frequently

missed by code analysis that has to cover the end-to-end software binaries, from the apps, to the OS, hypervisor, operating system, and firmware.

PUTTING A FOCUS ON PREVENTION

Detection will always be a critical component of cybersecurity, as identifying and remediating threats before they spread can alleviate some risk and damages incurred by a cyberattack.

But detection alone will no longer suffice in this increasingly perilous environment. Detection tools offer no protection in cases where the supply chain itself is compromised, in the case of fileless attacks like memory corruption such as buffer overflow, stack and heap attacks, Return Oriented Programming (ROP) chain attacks or zero-day attacks.

Host-based detection agents may also create performance issues that can require retooling and retesting to implement. Further, detection monitoring and alerting also requires time, investment and expertise. Finally, re-engineering code adds a requirement for a level of resources, as well as compliance challenges and risk that most companies are unable or unwilling to meet - especially in instances when the software stack might be hundreds of thousands or millions of lines.

Finding vulnerabilities and closing the gap can reduce risk and stop attacks in a far better fashion than simply identifying symptoms. One such strategy is Runtime Application Self Protection (RASP) which offers built-in security in the app and app environment itself to prevent real-time attacks from succeeding and from scaling across identical target systems.

There are several RASP techniques, including randomization (also known as binary stirring) which protects an app binary by rendering each version functionally identical but logically unique. Another technique is Control Flow Integrity (CFI) that puts curbs around jumps and returns to preserve the order of execution and functionality.

STOPPING ATTACKS FROM BEING EXECUTED

It's worth nothing that 80 percent of cybersecurity leaders who participated in the ISACA's 2017 State of Cyber Security Study believed they're likely to experience a cyber attack during the year. In today's environment, companies must operate with the assumption that they will be attacked at some point, and as such, do more to stop attacks rather than just identifying them.

While the majority of security solutions focus on preventing breaches with firewalls, antivirus software and intrusion prevention, those in charge of security must continue to assume that an attacker will eventually get in, and prepare accordingly. The key isn't to detect malware, it's to harden devices and systems to prevent attacks from being executed in the first place.

Joe Saunders is the CEO of RunSafe Security, a pioneer of cyberhardening technology for embedded systems and devices.

COVERING SECURITY FROM EVERY ANGLE

by Craig Riddell, senior solutions architect, SSH Communications Security

The Agile framework is most often thought of with respect to application development. However, there is now the concept of Agile security, in which security is factored into the design of a network environment from the beginning. The other approach is retro-fitted security, in which systems must be patched, updated and modified along with other solutions to piece together a secure environment.

Retro-fitting seems like a reasonable and affordable plan, at least initially, but dealing with several different appliances that must be managed as one-off point solutions makes the environment overly complex and adds costly overhead. This raises the total cost of ownership and leaves a business dependent on the vendor or vendors that sold the solution. Integration with these appliances that weren't part of the design from the start will almost certainly leave gaps that bad actors can exploit.

SKIRTING THE SECURITY ISSUE

It's not that organizations haven't considered security to be important. It is just that the possibility of a security breach and the penalties that would follow have been less of a concern than the possibility of slowing down the business with a strict security protocol.

IT security teams must juggle safety and productivity. They have to make sure every part of the architecture is as safe as possible (reducing risk to an acceptable level) without slowing down the speed and growth necessary for modern businesses. This has been true for the entire digital age with the invention of the internet and how quickly it was adopted as a platform for outreach, sales and marketing. Security was a secondary concern, and the only thing that mattered was getting the business online.

In this cloud era, businesses are hosting their data on someone else's servers and relying heavily on them for security, sometimes to a fault. For example, in the Department of Defense (DoD) AWS breach, security was only as good as the people implementing it. The DoD had all of the proper systems in place, along with their AWS hosts, but a contractor left the S3 storage publicly accessible, and top-secret data could be downloaded, along with the system image that was used for Linux-based virtual machines.

The standard network defense has involved protecting the perimeter from outside forces, but cloud computing, if not designed properly, is flat – allowing for unchecked lateral movement. The threat landscape is ever-changing, and the focus has shifted from keeping the attacker out (which, of course, is still important) to "What do we do and how will we know if they are already in?"

SECURITY FRONT AND CENTER

A security discussion that involves both business professionals and security professionals, from the earliest point possible, will allow them to design a plan where the business can grow but also be secure. In this way, they can make sure that all of the proper counter-measures are in place so that as the company's footprint grows on-premises or in the cloud, the attack surface remains as small as possible.

Interactive access should be monitored and controlled, privileges need to be minimized, and all network traffic should be treated as untrustworthy. Organizations need to adopt a "zero-trust model" and proactively inspect all network traffic to validate the authenticity of user activity.

The model consists of these basic steps:

- Watch cloud, app and database behavior to catch anomalies that can indicate threats and compromise.
- Commit to patching and configuration control to reduce the attack surface.
- Segment networks and reduce single points of failure.
- Reduce access scope and rights.
- Build resilience so teams and products can recover quickly from incidents.
- Consider using Endpoint Detection and Response (EDR), an emerging technology. It is a category of tools and solutions that focus on detecting, investigating and mitigating suspicious activities and issues on hosts and endpoints.
- Consider using Network Behavior Anomaly Detection (NBAD) – the real-time monitoring of a network for any unusual activity, trends or events.
-

SECURITY TRAINING

If an employee keeps leaving the back door open, all the network defenses in the world are useless. Start training employees on Day One so that they start thinking about cybersecurity best practices. Security should matter to everyone from the admin to the CEO. This will build resilience into products and teams.

Best practices include:

- Choose strong passwords and password management practices and solutions.
- Keep sensitive data secure and off your laptops and mobile devices.
- Look out for suspicious emails and calls from outsiders trying to obtain your information (phishing).
- Make sure your software is up to date.
- Make sure your antivirus software is up to date.
- Use caution when clicking links online and in emails.
- Don't leave your devices unattended.
- Always back up your data in case of a ransomware attack.

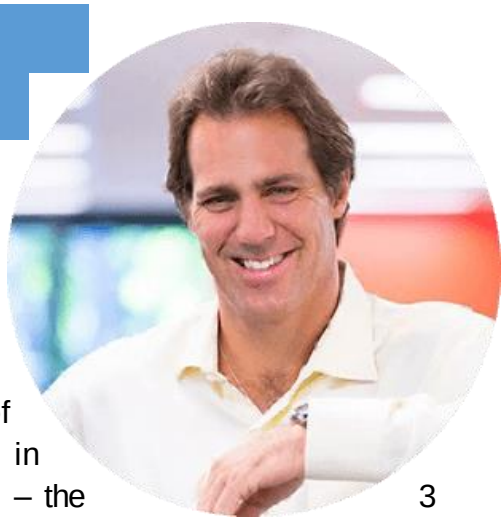
A SOLID SECURITY FOUNDATION

When leadership teams meet to form the business strategy, cybersecurity is on the checklist. Everyone understands the high level of importance attached to safeguarding the network. But for organizations that formed before cybersecurity became a critical necessity, security measures have been added on piecemeal, for the most part. This can lead to gaps in safety, which malicious actors are looking to exploit. However, whether newly formed companies have applied the Agile framework to their cybersecurity or an older company is knitting together its defenses, the best practices above will help protect the network environment and its business-critical data.

About the Author

Craig Riddell is an IT Security Systems Architect with over 10 years experience across all major business platforms, primarily in evaluating, designing, implementing, and supporting enterprise solutions.

UNDERSTANDING THE FUTURE OF CYBERSECURITY



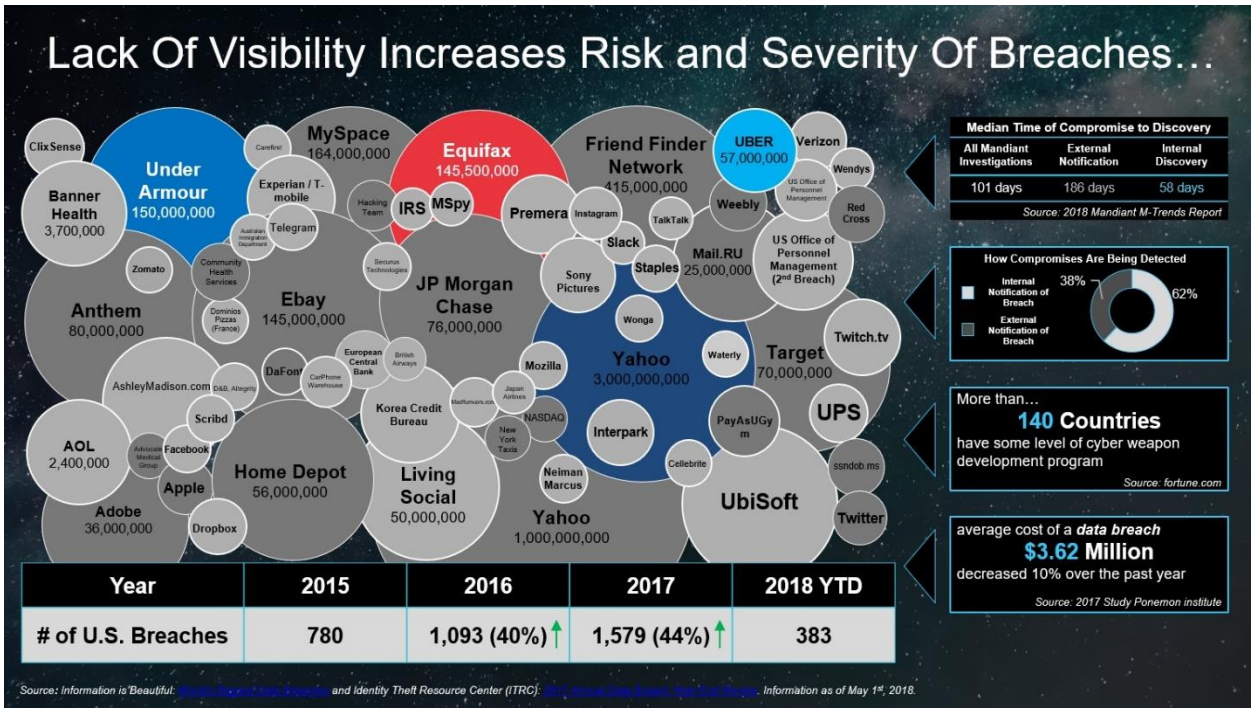
When you finish reading this article, and I recommend you read it two or three times, you will have a keen understanding of where the future of Cyber Defense is going from one of the most brilliant and successful minds in the industry.

I had the opportunity and honor to catch up with one of the most talented and innovative movers and shakers in our industry, yet someone who lives what he preaches – the 3 H's – Honesty, Humility and Hard-work – none other than David G. DeWalt, the founder of NightDragon Security who is also a partner at Allegis Cyber and Momentum Cyber among about 14 or 15 other ventures and activities, to name a few – he's also Vice Chairman of Delta Air Lines as the Safety/Security board member so he is boots on the ground in critical infrastructure as well. He's also serving on the National Security Telecommunications Advisory Council for the US Government. It was refreshing to hear David speak at the Cyber Investing Summit in New York City and then to follow it up with a one-hour deep dive into his strategies and platforms.

I assure you, this article, learning who David DeWalt is, where he is investing and what he's predicting could be the most important piece of Cyber Defense Intel for 2018 and beyond.

Building out the first Cybersecurity Platform from Inception to Exit

So, Dr. David G. DeWalt has more than 30 years of experience in the industry – over 20 years in high tech and 17 years as a CEO, as he says "68 quarters of executive leadership has given me a front row seat – it's my love, my passion – it's not just a job – I feel lucky and blessed." With these blessings and successes, Dr. David G. DeWalt has taken a bird's eye view of what happened in the past, what's happening today and predicting where we need to be in the very near future. His main driving concern is that the lack of visibility continues to dramatically increase the risk and severity of the breaches. This also opens up a new world of investment opportunities in cyber defense innovations.

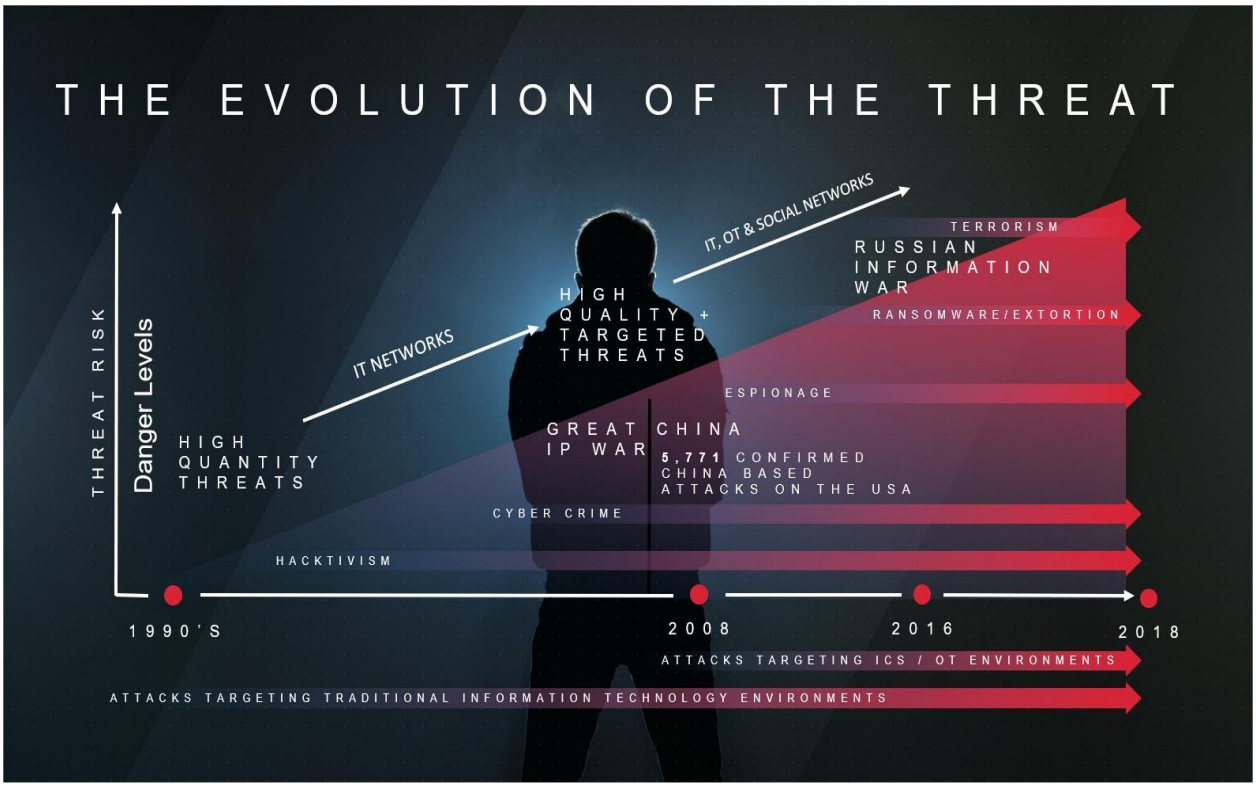


Pictured Above, Dr. David G. DeWalt's Thoughts On Greater Risk and Severity of Breaches

He's building out NightDragon Security (see http://www.nightdragon.com) as a very innovative platform for cyber – a massive keiretsu of companies to make cyberspace a better, more secure and safe place for us all. Incubators – Team8 (see: https://www.team8.vc/) and DataTribe (https://datatribe.com/), new companies, a Venture Capital platform with one of my personal favorites, Bob Ackerman at Allegis Cyber (see http://www.allegiscyber.com/) and an amazing group of investment bankers and experts at M&A at MomentumCyber (see http://www.momentumcyber.com).

WE'VE ENTERED THE PERFECT STORM IN CYBER DEFENSE

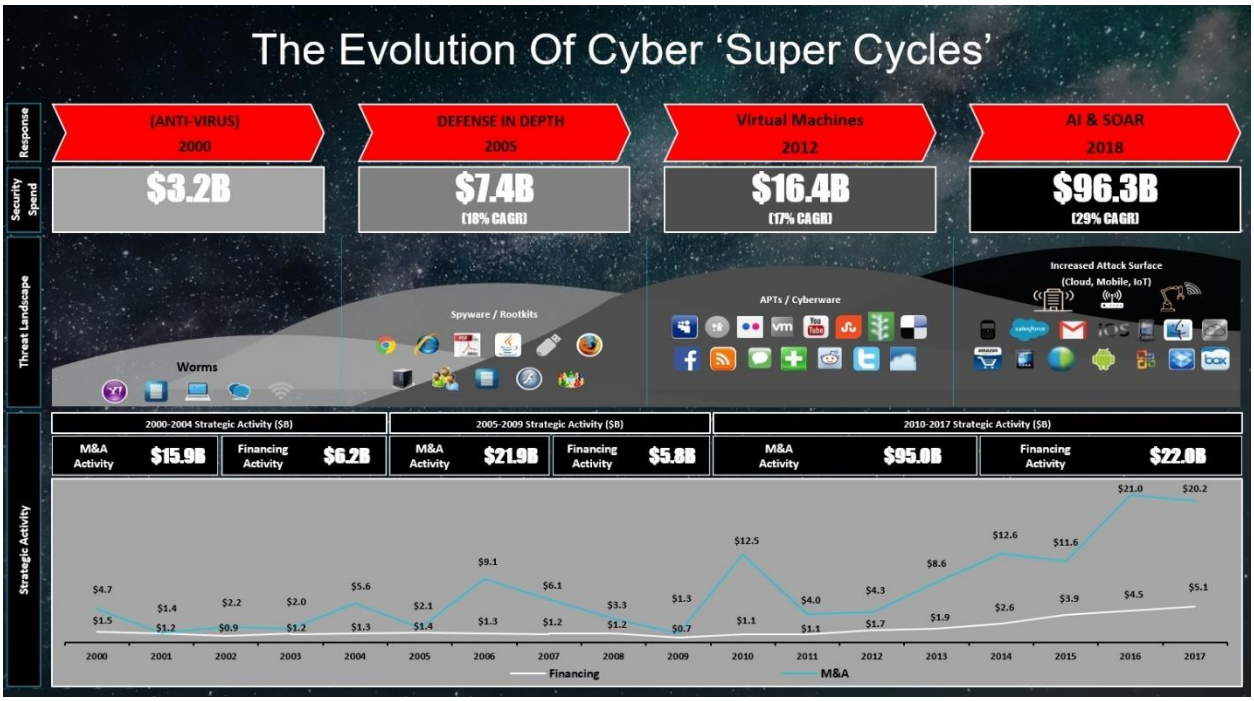
According to Dr. David G. DeWalt, with the biggest gaps comes the biggest investment opportunities, - if you see a threat, you will quickly see customer spend expand, then Venture Capitalists (VCs) pouring more money into those companies and of course it's cyclic, by the time the vendors solve it, the actors are onto new threats….



Pictured Above, Dr. David G. DeWalt's Threat Evolution from the '90's up to 2018

Dr. David G. DeWalt calls these "super cyber cycles" whereby these threat cycles drive vendor spending and investments, when he talks about biggest gaps, it's the offense or the threat vs commercial defense.

Wherever you see the biggest gap, it opens up to the biggest opportunities; Case in point: Fireeye. Along came the super threat cyber cycle in which advanced persistent threats (APTs) – multi-stage, attack vector, we'd never seen before and the antivirus (AV) vendors did not know how to stop 'all the objects.' "We took the risk at Fireeye and solved this challenge – we could tear apart APTs and understand their multi-object layering and multi-stages of behavior. I knew this would be a short, 3 year window – a big gap and a big opportunity – I see similar threat cycles coming our way and I call these Cyber 'Super Cycles'," said Dr. David G. DeWalt.



Pictured Above, Dr. David G. DeWalt's Idea of Cyber 'Super Cycles'

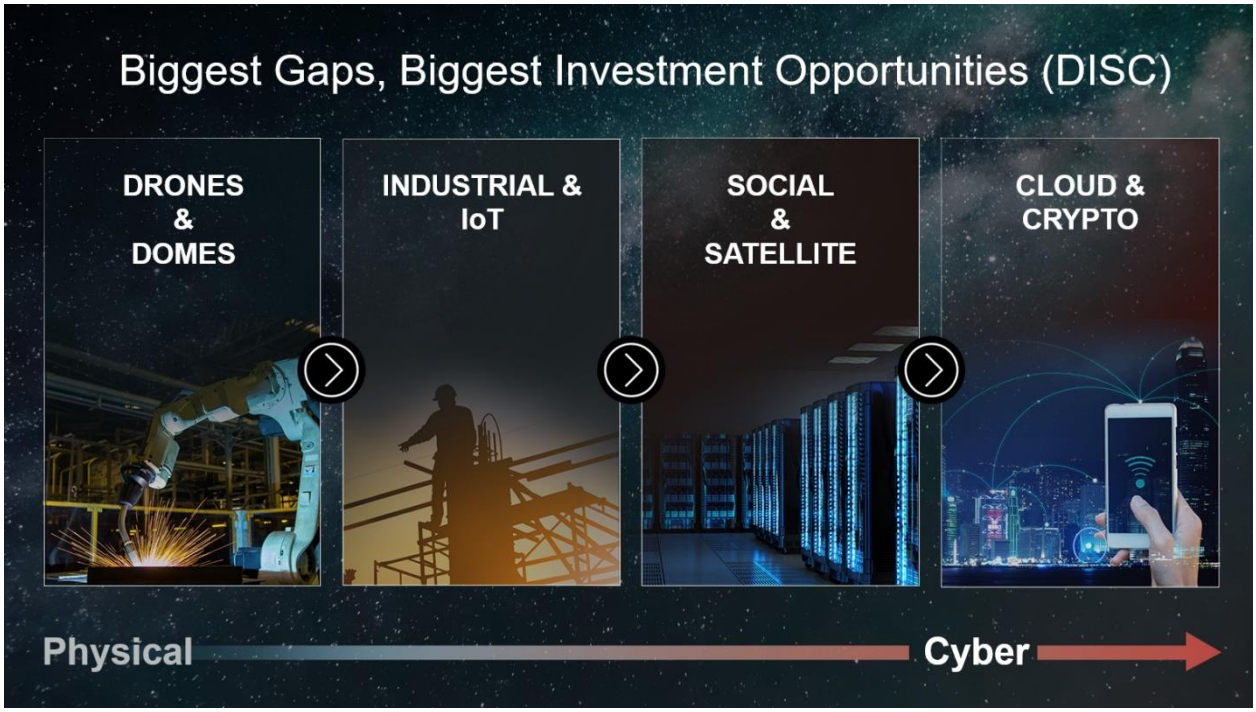
WHAT'S DRIVING THE PERFECT CYBER STORM?

According to Dr. DeWalt, the speed of innovation is driving vulnerabilities everywhere, but in particular, eight key areas – Mobile, Social, Cloud, Satellite, IoT, Industrial, Physical, & Consumer. Add to this the levels of danger expanding from hacktivism to crime to espionage to terrorism to warfare. In addition, we have a tremendous increase in geo-political tensions, a complete lack of governance and law enforcement models compounded by internet anonymity. Moreover, we have legacy security providers unable to detect or prevent the next threat – hence, we've entered a perfect Cyber storm.

A PERFECT STORM BRINGS A PERFECT OPPORTUNITY FOR INVESTING…

Given these critical issues, Dr. David G. DeWalt has decided to form NightDragon Security as a unique Cybersecurity Platform – to drive leadership into a new world of investment opportunities in cyber defense innovations. From inception to incubation to market deployment, acceptance and potential cyber defense global dominance – his mission is to create and/or find the market leaders to help us get one step ahead of the next breach. He's even predicting, very intelligently where those breaches will be happening – and you'd be very surprised. Today, it may be relatively easy to get to a CEO through a spear phishing attack but tomorrow, stealing his identity may happen through his home automation and internet of things (IoT) devices. Cybercriminals have already started planning on moving from drive by malware found on websites to actually

driving by (whether remotely through the internet or actually pulling a proximity attack) of an executive's property, eavesdropping on his or her insecure routers and weak home cybersecurity environment and making that the next big attack vector for cyber crime and espionage. Will the executive's Alexa or Nest system hold up to the scrutiny of cyber criminals or their 3-year-old wireless router that came with their cable modem? Highly doubtful. This is just one tiny example of what Dr. DeWalt has discovered. Let's read on and learn more from his key slide on the eight areas of high exploitation and high investment opportunity coming in the very near-term:



Pictured Above, Dr. David G. DeWalt's Cyber 'Super Cycles' Biggest Gaps Investment Vision

There's so much more to this 15 page article – this is just a teaser – read the entire story online on our website, here: http://www.cyberdefensemagazine.com/exclusive-interview-the-future-of-cybersecurity-with-dr-david-g-dewalt/

About the Author

Gary Miliefsky, Publisher, Cyber Defense Magazine

Gary is our Publisher and a globally recognized cybersecurity expert, speaker and keynote, investor, advisor and consultant. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), the National Information Security Group (http://www.NAISG.org) and the OVAL advisory board of MITRE responsible for the CVE Program (http://CVE.mitre.org). Learn more about him at http://www.cyberdefensemagazine.com/about-our-founder/

INFOSECURITY EUROPE 2018: TRIP REPORT

By Sarah Brandow, VP of Marketing, Cyber Defense Media Group

We really enjoyed this event. Because this edition is so packed full of great information, I've been tasked with making this short and sweet and to the point. This awesome event took place at the Olympia convention center between June 5-7, 2018 in London, United Kingdom.

There were over three hundred of the best and most innovative information security vendors from all over the Globe at this event – they literally packed the convention center to the rafters with two floors of great expo halls. There was great content, excellent educational sessions and keynotes and best of all for us at CDM, we had a chance to continue our Cyber Defense TV platform build-out with many more CEOs and C-level founders in our "HotSeat". These videos will be online in the near future and are packed with information in short, digestible snippets.

Infosecurity Europe is the region's number one information security event featuring Europe's largest and most comprehensive conference program and over 400 exhibitors showcasing the most relevant information security solutions and products to 19,500+ information security professionals. Our team enjoyed meeting old and making new friends. There were 240+ free to attend conference sessions led by industry influencers. We had the chance to meet both established vendors and new players all under one roof in three days of face-to-face business and network with our peers To learn more, visit InfoSecurity Europe 2018 online at http://www.infosecurityeurope.com/ Sarah Brandow can be reached at sarahb@cyberdefensemediagroup.com

EVENTS

ABU DHABI

GLOBAL ROAD & TRAFFIC SAFETY

Under the patronage of:

دائـرة التـخطيط العـمراني والبلـديات
DEPARTMENT OF URBAN PLANNING AND MUNICIPALITIES
بلـديـة مـديـنـة أبـوظـبـي
ABU DHABI CITY MUNICIPALITY

24 - 25 SEPTEMBER 2018 | Abu Dhabi, UAE

CREATING AWARENESS AND DELIVERING INNOVATION IN ROAD AND TRAFFIC SAFETY

AN EXCELLENT AGENDA PUT TOGETHER WITH A STELLAR LINE-UP OF SPEAKERS

Eng. Saleh Aljabri, Head of Traffic Services Section, **Abu Dhabi City Municipality**

Eng. Mohammed Faisal Al Hashmi, Senior Engineer - Traffic Safety, **Abu Dhabi City Municipality**

Stephen Lambert, Road Engineer, **Abu Dhabi Municipality**

Susanna Zammataro, Executive Director, **International Road Federation – Geneva**

Thomas Edelmann, Founder & Managing Director, **Road Safety UAE**

Eng. David Dunn, Lighting Expert, **Abu Dhabi Municipality**

Dr. Britta Lang, Technical Director – Education and Evaluation, **4E Road Safety and Transport Consultants**

David George, Road Safety Specialist, **Al Ain City Municipality**

SUPPORTING ORGANISATION	RoadSafetyUAE.com
NETWORKING PARTNERS	CLS Camera Lowering Systems; SSAB; HARDOX® WEAR PLATE
MEDIA PARTNERS	Railway Gazette International; الرؤية; Arab Wheels; VL Voices of Leaders; UAEBusiness.com

Cyber Security Summit

July 18-20, 2018

Gurney's Newport Resort & Marina
Newport, RI

Join us for Opal Group's Cyber Security Summit – set in Newport, RI, this premier event will gather C-Level & Senior Executives responsible for defending their companies' critical infrastructures together with technology providers & distinguished information security experts. Learn from acclaimed security professionals on how to protect your business from cyber attacks during interactive Panels & Keynote presentations.

Convene with fellow influential business leaders, C-Suite executives, investors & entrepreneurs over 3 days of sailing, sessions, and networking opportunities.

Sponsorship and Exhibiting Opportunities are Available
If you are interested in attending, sponsoring, speaking or exhibiting at this event, please call 212-532-9898 or email info@opalgroup.net or marketing@opalgroup.net for questions on registering.

Register
To register, visit us online at www.opalgroup.net or email us at marketing@opalgroup.net

Ref Code: CSSC1802

Opal Group

NEURAL NETWORKS 2018

+44-2088190774
neuralnetworks@enggconferences.com
artificialintelligencemeet@gmail.com

"Harnessing the power of Artificial Intelligence"

Major Sessions:

- ARTIFICIAL INTELLIGENCE
- BIG DATA
- BIOINFORMATICS
- AUTONOMOUS ROBOTS
- SUPPORT VECTOR MACHINES
- COGNITIVE COMPUTING
- DEEP LEARNING
- ARTIFICIAL NEURAL NETWORKS
- CLOUD COMPUTING
- NATURAL LANGUAGE PROCESSING

6th Global Summit on Artificial Intelligence and Neural Networks

Venue: Helsinki, Finland

October 15-16, 2018

https://www.linkedin.com/in/sheo-shankar-singh/

@networks_neural

https://neuralnetworks.conferenceseries.com

8TH EDITION

2018

Trainings: 25 - 27 June
Talks: 28 - 29 June

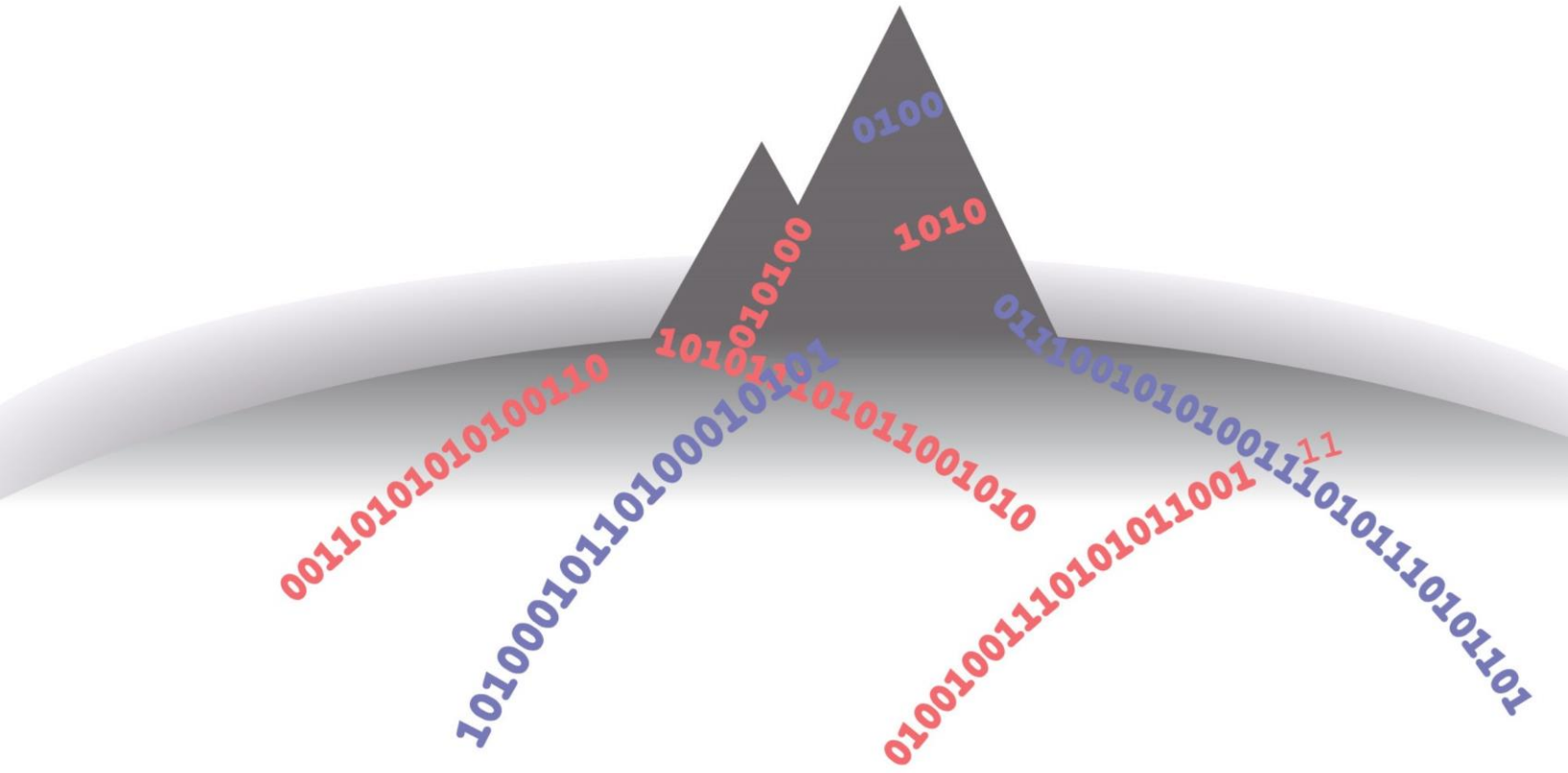
MAISON DE LA CHIMIE

www.hackinparis.com

organized by

SYSDREAM IT SECURITY SERVICES

www.sysdream.com



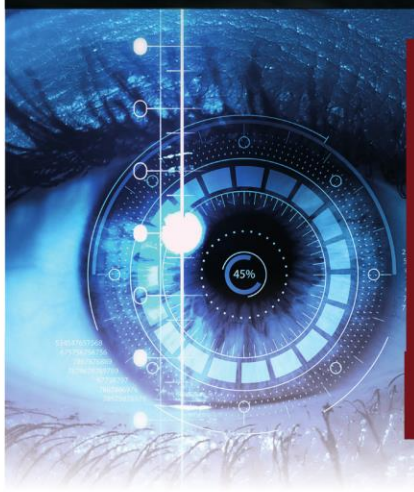
The Midwest's most impactful week for IT Security Information Collaboration is coming to Cleveland, Ohio October 22-26th

Now accepting Call for Papers through July 15th

www.informationsecuritysummit.org/summit-2018/

INFORMATION SECURITY SUMMIT℠
Building Community Through Education

FUTURE FORCES FORUM International Platform for Trends & Technologies in Defence & Security www.future-forces-forum.org



SMART CYBER DEFENCE WORKSHOPS

17 - 19 October 2018, PRAGUE, Czech Republic

Conference Main Partner: Deloitte.

Cyber Pavilion Partner: Fidelis Cybersecurity

Under the auspices of

NÚKIB

In cooperation with

AFCEA, ict unie, NCBI

Topics

- Current cyber threats and trends
- Cloud Security
- The Future of Cyber Defence
- Forensic analysis
- Data theft and protection
- New generation IDS / IPS
- Advanced cyber threats
- Ransomware
- Access control and authorization

www.future-forces-forum.org

FUTURE FORCES FORUM International Platform for Trends & Technologies in Defence & Security www.future-forces-forum.org

BIOMETRIeCS 2018

Modern Trends & Challenges

LET'S MAKE LIFE EASIER AND SAFER

17-19 October 2018, PVA EXPO PRAGUE, Czech Republic

Organized within the European Month of Cyber Security

Conference General Partner: SIT Simplified IT

Under the auspices of

NÚKIB, Ministry of the Interior of the Czech Republic, Úřad pro ochranu osobních údajů, Brno University of Technology

In cooperation with

AFCEA, CTU, ict unie

Topics

- Current trends in biometrics
- Electronic identity
- Forensic analysis
- Cryptography
- Modern biometric technologies
- Data theft and protection
- Advanced security threats
- Access control and authorization

www.future-forces-forum.org

Defence iQ presents the first

BIG DATA ANALYTICS FOR DEFENCE

In partnership with the

Defence and Security Accelerator

Conference Workshop Day: 26th June 2018 | Main Conference Days: 27th-28th June 2018 | Millennium Copthorne Tara Kensington, London

SECURE. ANALYSE. ACTION.

A senior speaker panel, including:

Dr. Peter Lenk , Branch Chief Service Strategy and Innovation, **NATO Communications and Information Agency**

Brigadier General **Juergen Broetz,** Chief, Military Intelligence, **Bundeswehr**

Brigadier Rob Sergeant, Head of Future Force Development, **British Army**

Engineer General of Armament Caroline Laurent, Director of Strategy, Directorate General of Armaments **French Ministry of Armed Forces**

Colonel Steven Desjardins, Director, Canadian Intelligence Corps, **Canadian Armed Forces**

Benefits of attending:

- **Achieve technical superiority** by incorporating cutting edge technologies in data analytics and Artificial Intelligence, with proven success in the commercial sector
- **Maximise the window of opportunity to exploit intelligence** by enhancing the speed and accuracy of data analysis using new AI and machine learning capabilities
- **Eliminate the threat of data hacking** by understanding how to develop secure and bespoke solutions for your needs alongside big data storage experts
- **Optimise your data analysis processes** by using the data analytics tools recommended by experts deploying high-end technical capability in the civilian sector
- Align your systems to the military requirement by **engaging directly with the senior decision makers** and capability directors from the Armed Forces, responsible for building big data capabilities into their own defence organisations

2018 Partners:

SCJ SecurityCleared Jobs.com

DATAFLOQ Driving Innovation

HOWES MEDIA

CDM CYBER DEFENSE MAGAZINE

+44 (0) 207 036 1300 | ENQUIRE@DEFENCEIQ.COM | BIGDATADEFENCE.IQPC.COM

International Conference on

Mechatronics & Robotics

Helsinki, Finland

Major Session on

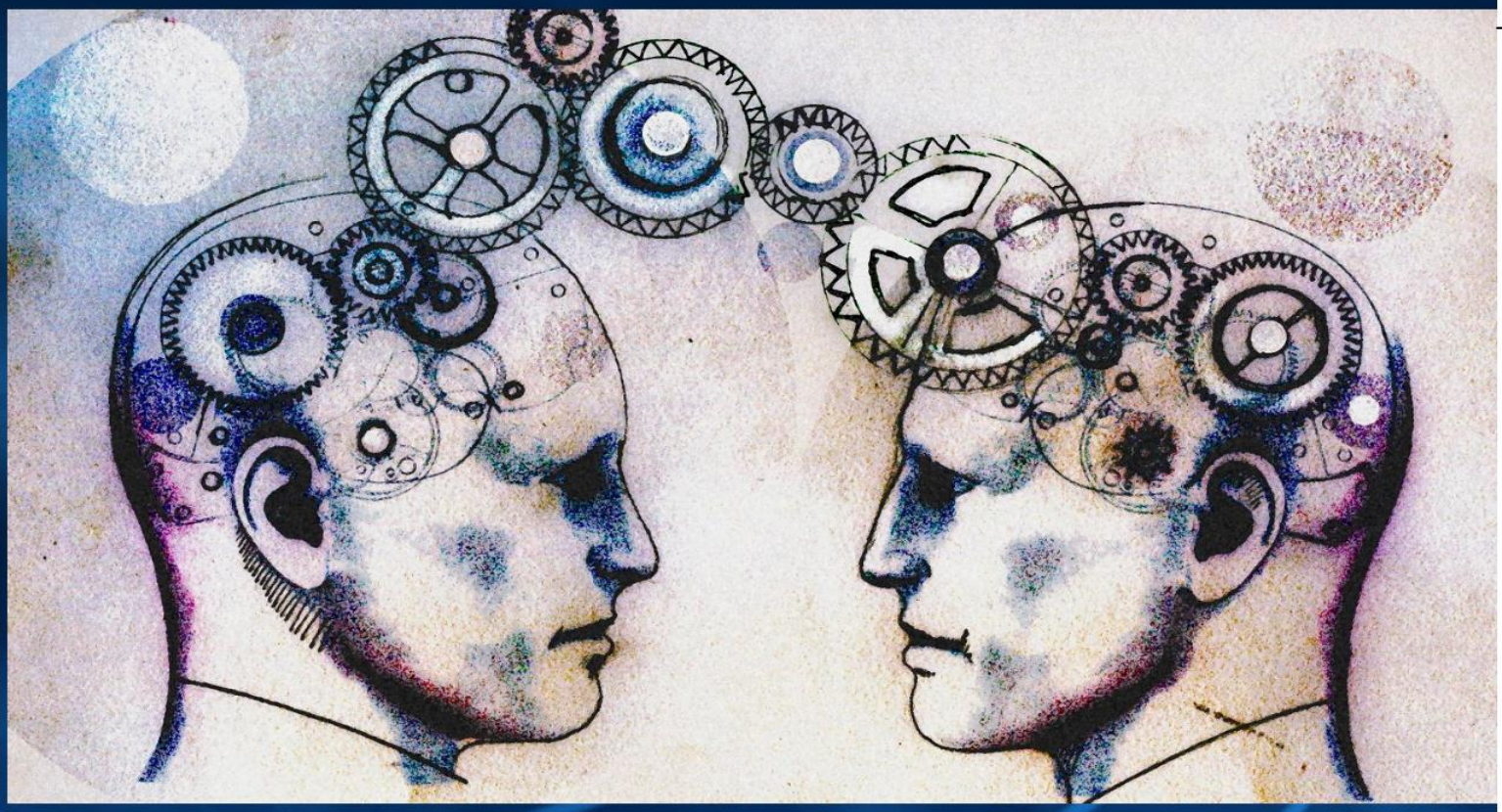
Artificial Intelligence future of Cyber Security

Register and Save 20%-MR18CDM20

October 15-16 2018

Contact: Kevin Mathew | Program Manager
Mechatronics & Robotics 2018
Mail: roboticsmeet@enggconferences.com

robotics-mechatronics.enggconferences.com



World Congress on Computer Science, Machine Learning, and Big Data Analytics

August 30-31, 2018

Dubai, UAE

https://computer-science.enggconferences.com/

Don't miss the world's leading event in Intelligent Transport Systems & Services

25TH ITS WORLD CONGRESS
COPENHAGEN
17 – 21 SEPTEMBER 2018
Quality of life

Early Bird Registration now open!

17 – 21 September 2018
Copenhagen, Denmark
www.itsworldcongress.com

A unique opportunity to:

- Exchange information and network with 10 000+ stakeholders and decision makers
- See the latest mobility solutions
- Share experiences and lessons learned
- Monitor progress and measure results of implementation and deployment
- Exhibit and experience cutting-edge technologies and innovative products and services
- Enter business and partnership opportunities

Organised by: ERTICO ITS EUROPE

Co-organised by: ITS AMERICA

ASIA-PACIFIC ITS

Hosted by: CITY OF COPENHAGEN

Supported by: GREATER CoPENHAGEN, its DENMARK, INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE The Danish Industry Foundation

TRANSPORT SECURITY & SAFETY EXPO

DETER / PROTECT / RESPOND

co-located with SAFE RAIL

Gold Sponsor

WATERFALL
Stronger Than Firewalls

Silver Sponsor

nccgroup

June 11-12, 2018
Hilton, Washington D.C.

SECURITY AND SAFETY FOR MASS TRANSPORT IN THE DIGITAL AGE

11%+

CAGR of the global transport security technology market from 2017 to 2022*

*Source: QYReports

"Understanding how to better safeguard operations and protect critical networks and infrastructure from damage is paramount. Opportunities like TSSX that bring the industry together for training and solutions are welcomed by SANS."

Doug Wylie, Director, Industrials & Infrastructure Portfolio, **SANS Institute**

Contact Tim Edwards, Event Director to see how you can get involved:
tim@transportsecurityworld.com
+44 (0) 207 045 0945

Please visit **www.transportsecurityworld.com** for more information.

produced by

TRANSPORT SECURITY WORLD
DETER / PROTECT / RESPOND

International Conference on
Mechatronics & Robotics

October 15-16, 2018 | Helsinki, Finland

Theme:“Unfolding Knowledge with a Delineate Technical World"

Mechatronics and Robotics 2018 warmly welcome all the researchers, developers, experts, students from the field of mechatronics & robotics to attend International Conference on Mechatronics & Robotics during October 15-16, 2018, Helsinki, Finland. The Conference will be composed around the theme “Unfolding Knowledge with a Delineate Technical World".

Sessions related to Mechatronics & Robotics 2018

1. Mechatronics and Robotics
2. Design and product development
3. Materials Science
4. Materials and Manufacturing
5. New Approaches in Automation and Robotics
6. Computational Vision and Robotics
7. 3D Scanning
8. wearable robots
9. Medical Robotics and Computer-assisted Surgery
10. Industrial Automation
11. Autonomous Technology
12. Sensor Networks
13. Intelligent Machines
14. Automotive and Vehicle Technology Systems
15. The Coming Future of Artificial intelligence
16. Power storage

This will be the best common platform to learning and offer new thoughts, create a network amongst the Technologist, Professionals, Industrialists, Researchers, Innovators and students from the area of Technical as well as Non-Technical background.
For more details: https://robotics-mechatronics.enggconferences.com/

For Queries
Contact: Kevin Mathew
Program Manager | Mechatronics & Robotics 2018
Mail: mechatronicscongress@enggconferences.com
Office Ph: +1-702-508-5200 Ext 8122
Toll No: +1-800-216-6499 (USA & Canada)

https://robotics-mechatronics.enggconferences.com/

"Asia's Premier Counter-Terrorism and Internal Security Exhibition and Conference!"

CTAX

COUNTER TERROR ASIA EXPO 2018

4 - 5 DECEMBER 2018

Marina Bay Sands, Singapore

Co-Located With:

www.counterterrorasia.com

An International Conference on Counter-Terrorism and Internal Security

For more info, contact us:
Phone: (+65) 6100 9101 | Email: sg@asiafireworks.com

Organized by:

FIREWORKS® TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

13 SEPTEMBER 2018, LONDON

The UK's largest summit for technology leadership

TECH LEADERS SUMMIT

ia
information-age.com

Registrations are now OPEN for the Tech Leaders Summit 2018

Tech Leaders Summit is the UK's largest conference for technology leadership, bringing together four streams - Data Leadership, Security Leadership, Digital Leadership and Cloud Leadership - to discuss the challenges and opportunities surrounding the most disruptive innovations facing the enterprise.

Tech Leaders Summit provides a 360° high-level view of the technologies and trends most impacting organisations, and se to drive innovation in 2018 and beyond. Its 40+ renowned speakers are the cream of the crop of the IT world when it comes to demonstrating real business value from deploying technology in large organisations.

This is an unparalleled opportunity to learn from the best in the business: the leaders who have experience the highs and lows, benefits and challenges, of implementing IT strategies and transformations, and kept such projects aligned to business goals.

Registrations are now open and close on 7th May.
Ticket information and prices can be found on our website.

a **vitesse**media event

TECHLEADERSSUMMIT.COM

Don't Forget To Register For

FutureTech EXPO Presents
The Bitcoin, Ethereum & Blockchain Superconference II

September 14-16, 2018

Held at the Kay Bailey Hutchison Dallas Convention Center.

TOP CONFERENCE SPEAKERS

Randi Zuckerberg
Founder & CEO - Zuckerberg Media
Created Facebook Live

Tim Draper
Billionaire Venture Capitalist DFJ Ventures; Draper University

Mark Yusko
Founder, Morgan Creek Capital Mgmt ($4.5 Billion under mgmt)

David Hirsch
Enforcement Attorney at U.S. Securities and Exchange Commission

Nick Spanos
Founder and CEO of Blockchain Technologies Corp.

Arman Rousta
Founder & CEO of KidCoin

Dustin Byington
President of Wanchain

Gary Leland
Speaker, Blogger, Podcaster, Videographer, Social Media Marketer , Publisher at CryptoCousins

Get 10% OFF - Use Code: CDM10

Get a Companion Ticket For $97 With Every Ticket Purchase

1,000+ Attendees Expected

www.thefuturetechexpo.com/register

CYBER DEFENSE MEDIA GROUP®
Where InfoSec Knowledge is Power

Meet Our Publisher Here!

Gary S. Miliefsky, CISSP, fmDHS

https://www.blackhat.com/us-18/

Meet Our Publisher: Gary S. Miliefsky, CISSP, fmDHS

"Amazing Keynote"

"Best Speaker on the Hacking Stage"

"Most Entertaining and Engaging"

Upcoming Engagements: CloudSec September 2018, IPEXPO Europe October 2018 and many more…If you are looking for a cybersecurity expert who can make the difference from a nice event to a stellar conference, look no further email marketing@cyberdefensemagazine.com

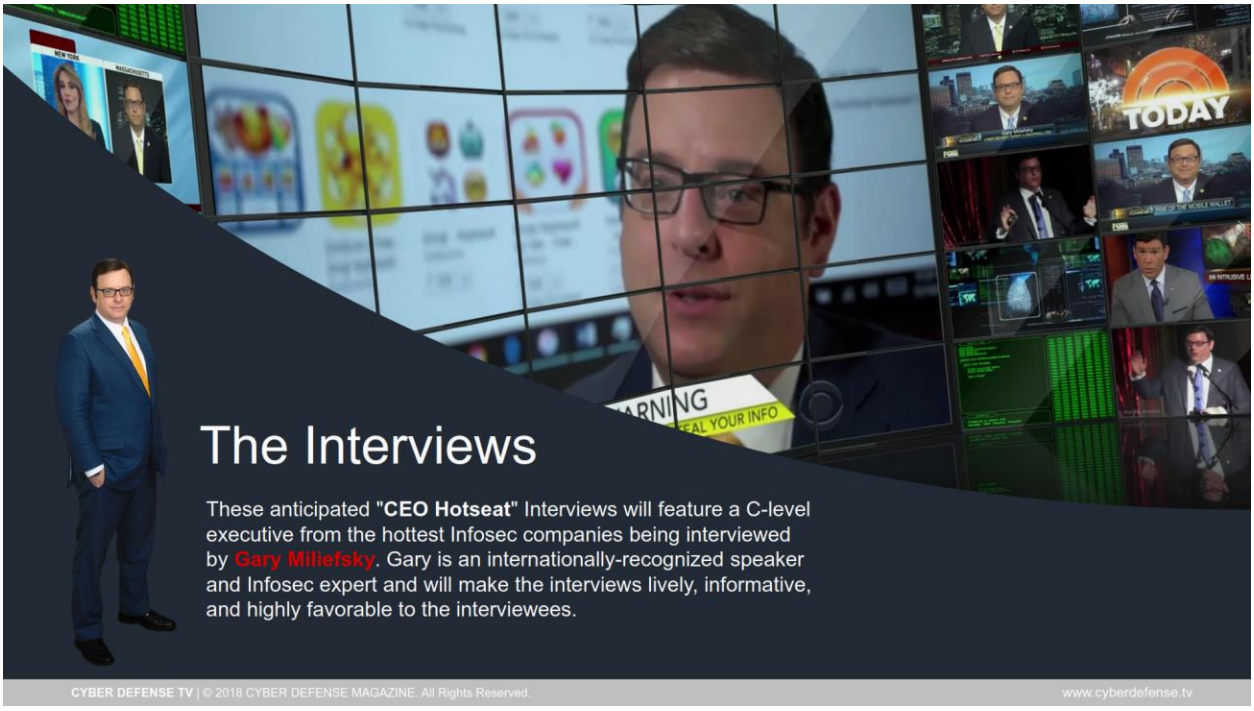
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

You asked, so we're doing it! Coming in 2018, we're launching CyberDefense.TV

Market leaders, innovators, CEO hot seat interviews and much more.

A new division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



FREE MONTHLY CYBER DEFENSE EMAGAZINE VIA EMAIL

ENJOY OUR MONTHLY ELECTRONIC EDITIONS OF OUR MAGAZINES FOR FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Defense e-Magazines will also keep you up to speed on what's happening in the cyber-crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy. You get all of this for FREE, always, for our electronic editions. Click here to sign up today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

MARKETING AND PARTNERSHIP OPPORTUNITIES

BANNERS, E-MAILS, INFOSEC AWARDS, DOWNLOADS, PRINT EDITIONS AND MUCH MORE…

JOB OPPORTUNITIES

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

PO Box 8224, Nashua, NH 03060-8224.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

Our New Office Addresses coming soon: **NEW YORK** (US HQ), **LONDON**, **HONG KONG**
Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 06/12/2018

ANNOUNCING CYBER DEFENSE GLOBAL AWARDS 2018

Cyber Defense Magazine (CDM), the global leader at information sharing and knowledge exchange of all things cyber defense that it's 6th annual Cyber Defense Global Awards for 2018 is now open.

Nominees please visit the following web page to apply: http://www.cyberdefensemagazine.com/cyber-defense-global-awards-2018/

CDM is looking for applicants who are helping their customers get one step ahead of the next breach with innovative products, services and technologies in the following categories: http://www.cyberdefensemagazine.com/global-awards-2018-categories-selections/

Finalists will be notified in September and Winners will be announced at IPEXPO Europe 2018 in London, England, United Kingdom on October 3, 2018 at the Excel London convention center and in the year end print edition of Cyber Defense Magazine that CDM staff will be handing out by the thousands at this event. Online versions of this special edition as well as six years of Cyber Defense e-Magazines are always freely available by signing up at http://www.cyberdefensemagazine.com

About Cyber Defense Global Awards 2018
This is Cyber Defense Magazine's sixth year of honoring cyber defense and information security innovators. Our submission requirements are for any startup, early stage, later stage or public companies in the INFORMATION SECURITY (INFOSEC) industry who believe they have a unique and compelling value proposition for their people, products and services. Download our Cyber Defense Global Awards 2018 Fact Sheet here: http://www.cyberdefensemagazine.com/wp-content/uploads/2018/06/CDM-Global-Awards-Facts-Sheet-2018.pdf

Your search for a secure file transfer solution, simplified.

If you've identified a need for a secure file transfer solution in your organization, you know that the decision to buy software is the easy part.

The difficulty hits when figuring out which solution you should purchase. There are many options available on the market. Which solution will fit your budget, meet your compliance requirements, and integrate with your current operations?

Tackle the software evaluation process with our ultimate buyer's guide to secure managed file transfer.
In this guide, you'll discover:

- The benefits and features of MFT
- Which questions to ask vendors
- What to consider in different industries
- How to determine your budget
- And much more.

We've compiled the knowledge you need to simplify the buying process.

Visit **https://info.goanywhere.com/mft-buyers-guide** to get a free copy of the guide.

GO ANYWHERE®
Managed File Transfer