CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

INSIDE THIS EDITION

Cyber Resilience: The Real Battle…

Deception Technology for Active Defense

Five Reasons CISO's Fail

Managing Digital Authentication Credentials

Top 10 Tricks to Avoid Malware

The Internet of Things Predictions

Why is Cybercrime a Big Threat in IoT Era?

Why VPNs Are More Than Just Security Apps

and much more…

DECEMBER 2018

MORE INSIDE!

CONTENTS

What's Your Secret – Best Practices for Managing Digital Authentication Credentials 18

4 Reasons Why Vpns are More Than Just Security Apps 21

Big Data and Cyber Attacks: The Cyber Dragon Awakening 25

What is PII and Why Criminals Want Yours 32

New Data Affirms Cyber Threat for Industrial Control Systems..... 36

How Organizations are Tackling Cyber Challenges: Takeaways from the Cybersecurity Imperative 39

Ransomware and Cyber Attacks Dive in 2018..... 41

5 Reasons CISO's Fail..... 44

The Internet of Things Predictions for 2019..... 48

Cyber Resilience: The Real Battle is Behind the Frontline 51

Why is It a Bad Idea to Download Apps from Third Parties? 54

Two Decades Later, SIEM Technology Finally Delivers on Its Original Promise 58

Do I Need to Be GDPR Compliant 61

Top 10 Tricks to Avoid Malware 65

Why is Cybercrime a Big Threat In IoT Era?..... 74

Is Building a Shark-Cage Right for Global Business? 79

Your Security Auditing is Failing You, and Here's Why..... 82

Being Compliant Isn't Secure Enough for Critical Infrastructure..... 84

Leading The Way in Discussions for National Privacy Laws 88

How Businesses Can Avoid S3 Bucket Leaks to Protect Company and Client Data..... 91

Passwords and Honeywords 95

Another Cyber Security Month is Over: So What's New? 99

2/3 Of Fortune 50 Companies are at Risk of Being Taken off the Internet – Is Your Company Too?.....102

7 Network Security Tools to Protect Your Digital Assets from Malicious Activity 104

Faxploit: Critical Flaws in The Fax Protocol? Not So Fast… 108

Brands Beware! Strengthen Data Privacy or Pay a Hefty Price 111

Deception Technology for Active Defense: Changing the Game on Attackers 114

Six Essential Questions About "ePrivacy" 119

A New Approach to Secure Mobile Banking Apps 122

Streamlining RMF Accreditation to Speed Deployment of New Defense Technologies 125

Why Zero Trust is The Answer to Securing Healthcare Data 129

The Modern Business Has No Perimeter 132

A CISOs 'playbook': Practice How You Fight 135

AI and Machine Learning Must Be Used Strategically in Cybersecurity 138

Data Security Tops 2019's Intelligent Workplace Priorities 141

Watchguard Technologies 2019 Security Predictions 144

If I Use The Word Recidivists, Will They Come? 150

Regent University's Institute for Cybersecurity 154

Cryptographic Key Management Considerations for Secure Cloud Computing 157

The Only Counter Strategy Against Data Loss: Reliable Backup Methodology 160

Revisiting Conficker 10 Years Later 163

@MILIEFSKY

From the

Publisher…

CyberDefense.TV welcomes you as a founding member, free, no strings, please join now.

Dear Friends,

Have you ever been hit with a big surprise? I have. It's how we react that counts the most. I have so many examples of this, personally and in business. On the business side, we're so thrilled and honored to be reaching the RSA Conference 2019 in our 7th and most exciting year, adding yet another platform (service) offering we think you'll love – like we did with CyberDefense.TV which continues to grow.

So, here's the surprise – RSA Conference 2019 is coming about 45 days earlier than last year.

That gives my team very little time to prepare – we have four judges working on our prestigious InfoSec Awards, we've hired new staff to help with this and scaling our content management system, we have to organize our nearly 100-page print edition for the show – yet it has to be ready for print in January! Sometimes when you are hit with a challenge, you either continue to feel the pain and stress or you turn it into a great opportunity. So our team brainstormed and we decided the only way to get there is to make an incredible offer to our friends at public relations firms and all InfoSec players who feel they have a story to tell and content to share through this link at www.cyberdefensedeals.com. We've never offered so much for so low a cost, but we know it will help us get everything done on time. It's a great lesson on how to turn a really early deadline from sour lemons into sweet lemonade. Just add sugar and move on! *With much appreciation to our all our sponsors – it's you who allow us to deliver great content for free every month to our readers…for you, our comarketing partners, we are forever grateful! Have an awesome holiday season and wonderful New Year!*

Warmest regards,

Gary S. Miliefsky

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

P.S. I've been honored to keynote and speak at conferences throughout the year and will continue to do so. Please come meet me in Washington, D.C. January 8th, 2019 – details to follow in social media.

InfoSec Knowledge is Power. We will always strive to provide the latest, most up to date FREE infosec information.

From the

Editor…

We're about to turn a corner into 2019 and I'll be working on my Cybersecurity Predictions for 2019 with our Publisher, Gary, which we'll share with you at RSA Conference March 4-7, 2019, in San Francisco, California in our upcoming 7th annual Print Edition.

Meanwhile, we're watching innovations unveiled to help speed our ability to defend against new forms of malware and cyber-crime and at the same time we see new attack vectors and methods never before used by nation states, cyber threat actors and cyber criminals.

Happy Holidays!

To our faithful readers,

Pierluigi Paganini

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group 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
Marketing Team
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:

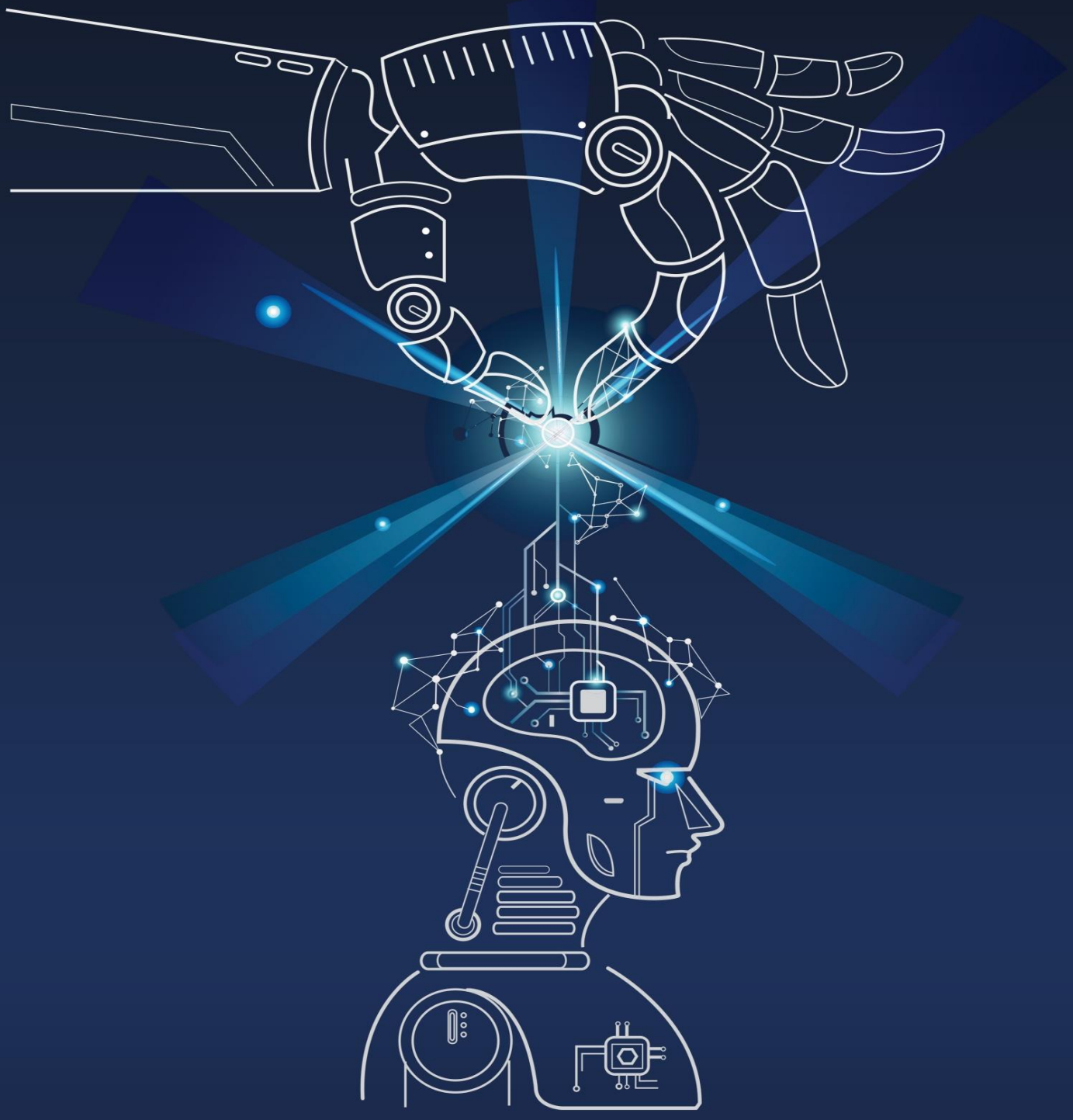
CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE **TV** **AWARDS**

SEE US IN MARCH 2019 AT…

SPONSORS

InfoSec Knowledge is Power
Free Cybersecurity Resources



www.cyberdefense.tv
www.cyberdefensemagazine.com

DON'T LET COMMUNICATION BE YOUR POINT OF FAILURE.

The **Vaporstream® Secure Communication Platform** lets organizations securely collaborate with confidence during times of crisis.

Vaporstream eliminates the vulnerabilities of the traditional communication and information sharing channels such as email and standard SMS. Our enterprise-grade, secure and compliant communication platform empowers business continuity and command of any crisis outside of your network, without worrying about information leaks to bad actors, the media or the competition that could impact your reputation or bottom line. Take control of communication during any crisis. **Learn how Vaporstream helps you keep communications secure, compliant and leak free.**

Vaporstream

Visit us at www.Vaporstream.com/security.

Connectivity with Salesforce, Google Drive, SharePoint, and More...Simplified

Wouldn't it be nice if your file transfer solution allowed for plug-n-play connectivity with the web and cloud applications you use every day?

THIS IS 100% POSSIBLE WITH

GO ANYWHERE®
Managed File Transfer

GoAnywhere is a managed file transfer solution that simplifies how you encrypt and automate your data transmissions. Together with GoAnywhere Cloud Connectors - powerful web and cloud integrations - you can streamline connections with these applications and more:

Dropbox

Google Drive

VOTIRO SECURED.

salesforce

SharePoint

Jenkins

Microsoft Dynamics 365

zendesk

Simplify Your Processes and More with Secure Cloud Integrations

Request a Demo: www.goanywhere.com/demo

Visuality Systems

Protect Your Product From Malicious SMB File Sharing Activities, Upgrade To An

Encrypted SMB VERSION 3

Secured Access To Remote Files

sanernow

Array of tools for Endpoint Security and Systems Management

- ✓ Vulnerability Management
- ✓ Patch Management
- ✓ IT Asset Management
- ✓ Compliance Management
- ✓ Endpoint Threat detection
- ✓ Endpoint Management

secpod

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**?

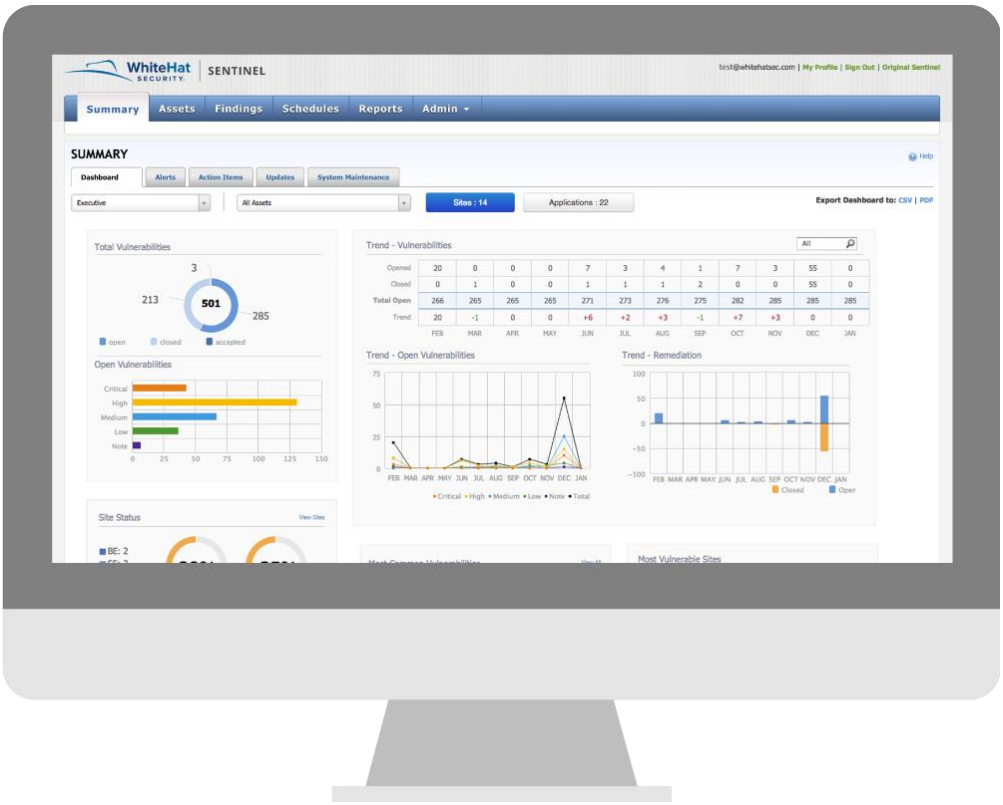
Look no further...

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



Your website could be vulnerable to outside attacks. Wouldn't you like to know where those vulnerabilities lie? Sign up today for your free trial of WhiteHat Sentinel Dynamic and gain a deep understanding of your web application vulnerabilities, how to prioritize them, and what to do about them. With this trial you will get:

An evaluation of the security of one of your organization's websites

Application security guidance from security engineers in WhiteHat's Threat Research Center

Full access to Sentinel's web-based interface, offering the ability to review and generate reports as well as share findings with internal developers and security management

A customized review and complimentary final executive and technical report

Click here to sign up at this URL: https://www.whitehatsec.com/info/security-check/

PLEASE NOTE: Trial participation is subject to qualification.

Your peers use managed file transfer to solve key business initiatives - but how?

IT professionals discover innovative uses for their secure file transfer solution every day. From tracking weather patterns in Alaska to eliminating third-shift staffing, MFT makes solving their organizational needs easy.

In The GoAnywhere Book of Secure File Transfer Project Examples, you'll discover 20+ ways your peers use managed file transfer to meet ambitious goals and requirements in their company, including:

- A distribution company that uses MFT to send barcode scans to a file repository.
- A healthcare organization that uses MFT to move faxes into an API for processing.
- A manufacturing business that uses MFT to check a server for firmware updates.

Find the inspiration and know-how for your next file transfer project.

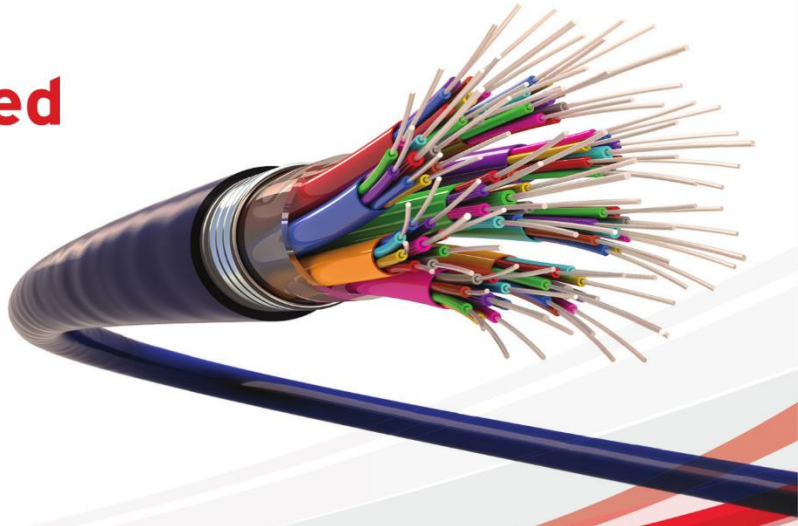
GO ANYWHERE®
Managed File Transfer

Visit ***info.goanywhere.com/use-cases-for-mft*** to get the free guide sent right to your inbox.

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 >

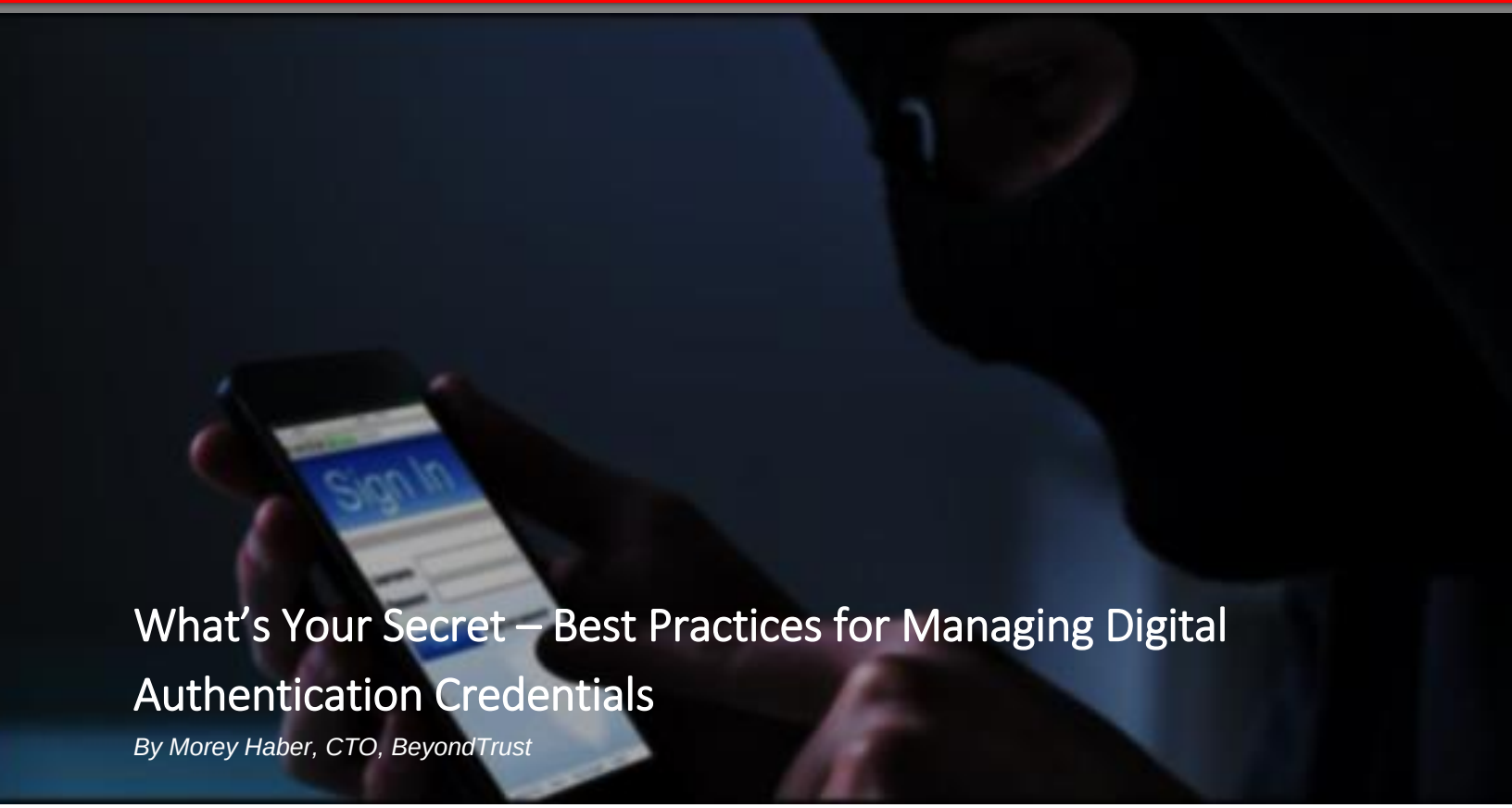
WIRELESS SECURITY
view >

MALWARE ANALYSIS

MOBILE SECURITY TESTING

BLOCKCHAIN SECURITY

ARTICLES



What's Your Secret – Best Practices for Managing Digital Authentication Credentials

By Morey Haber, CTO, BeyondTrust

Secrets management refers to the tools and methods for managing digital authentication credentials (secrets), including passwords, keys, APIs, and tokens for use in applications, services, privileged accounts and other sensitive parts of the IT ecosystem. While secrets management is applicable across an entire enterprise, the terms "secrets" and "secrets management" are referred to more commonly in IT with regard to DevOps environments, tools, and processes.

Challenges to Secrets Management

Passwords and keys are some of the most broadly used and important tools your organization has for authenticating applications and users and providing them with access to sensitive systems, services, and information. Because secrets have to be transmitted securely, secrets management must account for and mitigate the risks to these secrets, both in transit and at rest. But as the IT ecosystem increases in complexity and the number and diversity of secrets explodes, it becomes increasingly difficult to securely store, transmit, and audit secrets. Common risks to secrets and some considerations include:

- ***Incomplete visibility and awareness*** of all privileged accounts, applications, tools, containers, or microservices deployed across the environment, and the associated passwords, keys, and other secrets. SSH keys alone may number in the millions at some organizations, which should provide an inkling of a scale of the secrets management challenge. This becomes a particular shortcoming of decentralized approaches where admins, developers, and other team members all manage their secrets separately, if they're managed at all. Without oversight that stretches across all IT layers, there are sure to be security gaps, as well as auditing challenges.

- ***Hardcoded / embedded credentials:*** privileged passwords and other secrets are needed to facilitate authentication for app-to-app (A2A) and application-to-database (A2D) communications and access. Often, applications and IoT devices are shipped and deployed with hardcoded, default credentials, which are easy to crack by hackers using scanning tools and applying simple guessing or dictionary-style attacks. DevOps tools frequently have secrets hardcoded in scripts or files, which jeopardizes security for the entire automation process.
- ***Privileged credentials and the Cloud:*** Cloud and virtualization administrator consoles (as with AWS, Office 365, etc.) provide broad superuser privileges that enable users to rapidly spin up and spin down virtual machines and applications at massive scale. Each of these VM instances comes with its own set of privileges and secrets that need to be managed.
- ***DevOps tools****:* While secrets need to be managed across the entire IT ecosystem, DevOps environments are where the challenges of managing secrets seem to be particularly amplified at the moment. DevOps teams typically leverage dozens of orchestration, configuration management, and other tools and technologies (Chef, Puppet, Ansible, Salt, Docker containers, etc.) relying on automation and other scripts that require secrets to work.
- ***Third-party vendor accounts / remote access solutions:*** How do you ensure that the authorization provided via remote access or to a third-party is appropriately used? How do you ensure that the third-party organization is adequately managing secrets?
- ***Manual secrets management processes:*** Leaving password security in the hands of humans is a recipe for mismanagement. Poor secrets hygiene, such as lack of password rotation, default passwords, embedded secrets, password sharing, and using easy-to-remember passwords, mean secrets are not likely to remain secret, opening up the opportunity for breaches. Generally, more manual secrets management processes equate to a higher likelihood for security gaps and malpractices.

Best Practices & Solutions for Secrets Management

While holistic and broad secrets management coverage is best, regardless of your solution(s) for managing secrets, here are 7 best practices you should focus on addressing:

- ***Discover / identify all types of passwords, keys and other secrets*** across your entire IT environment and bring them under centralized management. Continuously discover and onboard new secrets as they are created.
- ***Eliminate hardcoded / embedded secrets*** in DevOps tool configurations, build scripts, code files, test builds, production builds, applications, and more. Bring hardcoded credentials under management, such as by using API calls, and enforce password security best practices. Eliminating hardcoded and default passwords effectively removes dangerous backdoors to your environment.
- ***Enforce password security best practices***, including password length, complexity, uniqueness expiration, rotation, and more across all types of passwords. Secrets, if possible, should never be shared. If a secret is shared, it should be immediately changed. Secrets to more sensitive tools and systems should have more rigorous security parameters, such as one-time passwords, and rotation after each use.

- ***Apply privileged session monitoring*** to log, audit, and monitor all privileged sessions (for accounts, users, scripts, automation tools, etc.) to improve oversight and accountability. This can also entail capturing keystrokes and screens (allowing for live view and playback). Some enterprise privilege session management solutions also enable IT teams to pinpoint suspicious session activity in-progress, and pause, lock, or terminate the session until the activity can be adequately evaluated.
- ***Extend secrets management to third-parties*** and ensure partners and vendors conform to best practices in using and managing secrets.
- ***Leverage threat analytics*** to continuously analyze secrets usage to detect anomalies and potential threats. The more integrated and centralized your secrets management, the better you will be able to report on accounts, keys applications, containers, and systems exposed to risk.
- ***Embrace DevSecOps*** – With the speed and scale of DevOps, it's crucial to build security into both the culture and the DevOps lifecycle (from inception, design, build, test, release, support, maintenance). Embracing a DevSecOps culture means that everyone shares responsibility for security, helping ensure accountability and alignment across teams. In practice, this should entail ensuring secrets management best practices are in place and that code does not contain embedded passwords in it.

The right secrets management policies, buttressed by effective processes and tools, can make it much easier to manage, transmit, and secure secrets and other privileged information. By applying the 7 best practices in secrets management, you can not only support DevOps security, but tighter security across the enterprise.

About the Author

With more than 20 years of IT industry experience and author of Privileged Attack Vectors, Mr. Haber joined BeyondTrust in 2012 as a part of the eEye Digital Security acquisition. He currently oversees BeyondTrust technology for both vulnerability and privileged access management solutions. In 2004, Mr. Haber joined eEye as the Director of Security Engineering and was responsible for strategic business discussions and vulnerability management architectures in Fortune 500 clients. Prior to eEye, he was a Development Manager for Computer Associates, Inc. (CA), responsible for new product beta cycles and named customer accounts. Mr. Haber began his career as a Reliability and Maintainability Engineer for a government contractor building flight and training simulators. He earned a Bachelors of Science in Electrical Engineering from the State University of New York at Stony Brook.

4 Reasons Why Vpns are More Than Just Security Apps

See how VPNs can help you in other ways aside from security.

by John Mason, Chief Researcher, TheBestVPN

Unless you've been living under a rock for the past few years, odds are you've already heard about VPNs. This wonderful software has secured people's online activities for well over 2 decades now. And the way things are going, it seems the VPN is not going away any time soon.

But, how exactly do VPNs provide security? Well, it's all about the data packets.

Let me explain:

When you search for something on the internet, your browser sends a request to a DNS server. This request contains data packets which in turn contain readable plain text. These data packets then make their way to the proper DNS server that records their contents along with your IP address.

Normally, these data packets are readable to anyone who's able to gain a hold of them -- which means their normally unsecured. However, with a VPN, these packets get encrypted, thereby, making them unreadable. Furthermore, anyone trying to read your data packets won't be able to trace them back to you since a VPN also masks your true IP address.

Long story short: VPNs secure your online activities.

But, what most people may not know is that VPNs lets them do much more besides simply securing their connection.

4 reasons why VPNs are more than just security apps

1. Privacy

One of the first, and most obvious, extras you get with a VPN is privacy.

You see:

When a VPN encrypts your data packets and hides your true IP, it's not only protecting you from the hackers that want to infect your device with malware, it protects you from **anyone** just snooping around your connection.

This includes entities like:

- Your school: They often monitor your device's connection to block certain sites (more on this later).
- Your ISP: Your Internet Service Provider can actually track your online habits. This is because the requests your browser makes always travels through your ISP before they are sent to the proper DNS server. This fact lets ISPs monitor and record your online searches.
- Your Government: You may have heard stories about Governments spying on their citizens. Well, there is evidence that some of these stories are true.

With Black Friday, Cyber Monday, and the holidays coming up, are you thinking about using your hotel or airport Wi-Fi to do your online shopping? Use a VPN to shop on secure HTTPS online shops. This ensures your privacy from anyone snooping around that public Wi-Fi's connection who might want to find and steal your personal information.

With all that said:

VPNs were primarily made for security, not privacy. It just so happened that this primary function also allowed some benefits to privacy. But, you shouldn't expect 100% anonymity from a VPN alone. You can install additional privacy apps (like TOR and DuckDuckGo) that work with your VPN to get you the privacy you need.

2. Save Money for Airline Tickets, Car Rentals, and Many More

Did you know that your VPN can save you money on online booking?

Don't worry, this isn't anything illegal. You're simply taking advantage of how retail websites work. It all has to do with your IP address.

Look:

If you've been traveling for some time, you may have noticed in the past that prices for airline or car rentals often fluctuate. This is because prices differ by location due to foreign currency leverages and advantages of the points of sale.

Simply by switching VPN servers, you can, therefore, use your VPN to have your IP address appear like you're from another location -- preferably one with cheaper online booking.

In theory, this method can also work for other sites that require you to pay for a service. These include Hotels, Streaming, and Subscription software.

3. Get around Site Blocks

If you're a resident of the EU that frequented American websites, you may have noticed that some sites have blocked you from accessing their content. Apparently, the GDPR taking effect led to some sites simply blocking European IP addresses rather than spending money for compliance.

Perhaps your an individual who likes downloading torrents but you can no longer do so because you're in a place that has blocked these torrent sites for whatever reason.

These blocks are done by blocking your IP address. But since your VPN masks your true IP address and can make it appear to originate from another location, you're therefore free to access these sites.

4. Netflix and KODI

I don't think I need to explain what Netflix is, right? It's currently one of the biggest names in the entertainment and streaming industry and has become a household name.

KODI, on the other hand, is relatively new. It's an open-source home theater software that lets you watch what you want via its plug-ins.

The problem you may have encountered with these two entertainment media is that their content is geo-blocked. These blocks were set up for various reasons like possible copyright infringement and for financial reasons. Is a VPN the solution to this problem? Yes, but there's good and bad news.

The good news is that a VPN **can** unblock these geo-restrictions.

The bad news is that **not all** VPNs are able to do so.

On Netflix's part, this is because the company itself has taken steps to block VPN servers. This means that they're effectively blocking paying users who now live outside the unrestricted locations.

If you want to access Netflix wherever you are, you can look for the best Netflix VPN currently available. These VPNs are some of the only ones to unblock Netflix.

VPNs are Good for More than Just Security

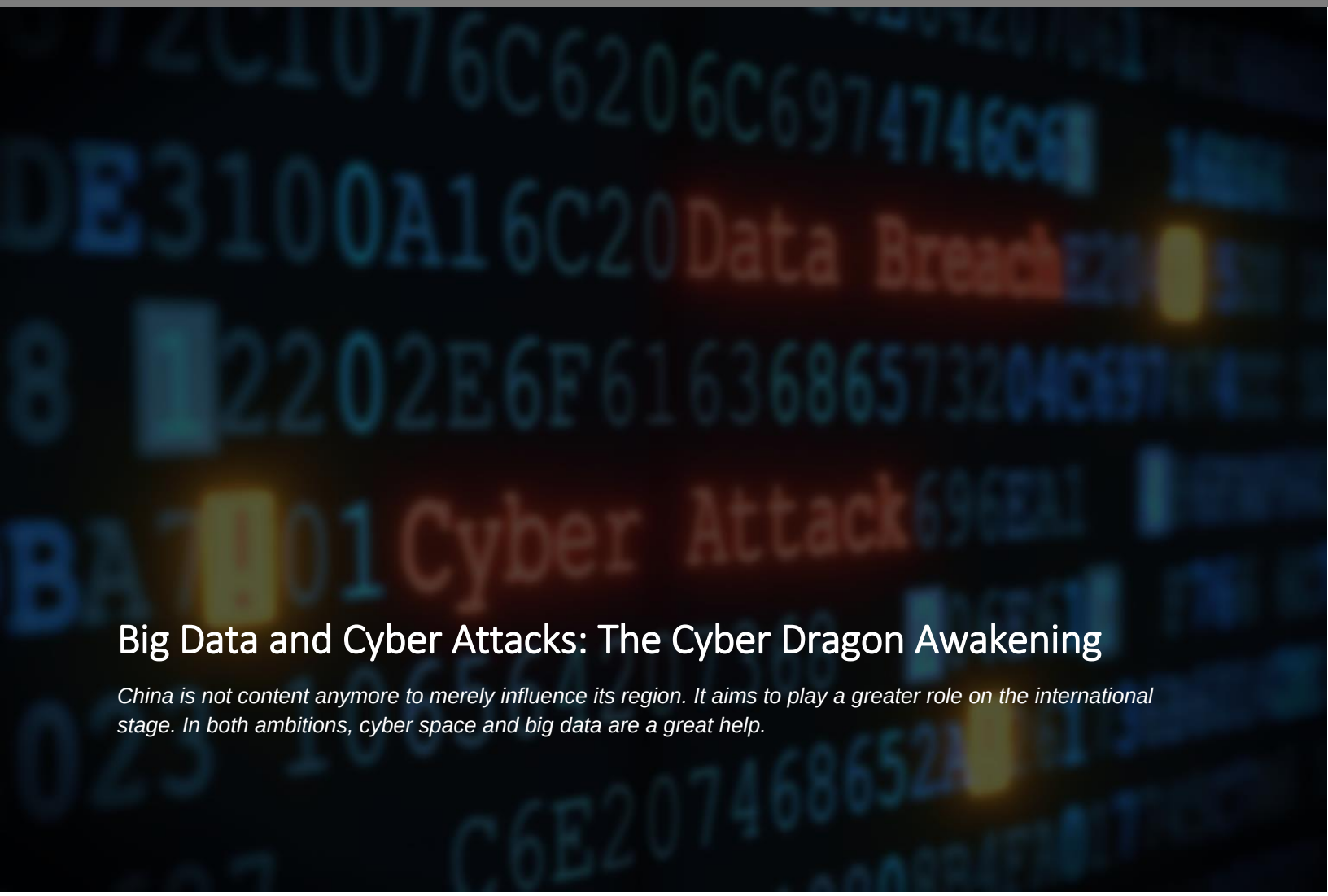
If you're using a VPN, you've got yourself a handy tool that not only protects you from hackers but also from spies.

Make use of its IP masking and separate server locations to save money on airline tickets, car rentals, and many more.

Use it to get around those annoying site blocks and even gain access to the best entertainment content on Netflix and KODI.

About the Author

John Mason the Chief Researcher at TheBestVPN. He is an avid privacy advocate and the founder of TheBestVPN. John can be reached online at john@thebestvpn.org and at our company website https://thebestvpn.com/



Big Data and Cyber Attacks: The Cyber Dragon Awakening

China is not content anymore to merely influence its region. It aims to play a greater role on the international stage. In both ambitions, cyber space and big data are a great help.

The Great Contender with Resentment

China has the world's second-largest military budget with USD 228 billion spent in 2017.[1] It represents 13.4% of the world's economy and, by 2026, it will overtake the US as the largest GDP.[2,3] Its solid growth is combined with new policies to ensure a supply of raw materials, thus switching from a "made in China" policy to a "created in China" one, with innovation as a core principle and the defense of its economic and political interests abroad a key goal.

China's aspirations of expansion and liberty of movement do not only come from its wish for a global policy, but also from a past century of humiliation: 100 years etched in its collective mind as a terrible

[1] SIPRI, "Military expenditure by region in constant US dollars, 1988-2017", *SIPRI*, 2018
https://www.sipri.org/sites/default/files/4_Data%20for%20world%20regions%20from%201988–2017.pdf

[2] SCOTT Malcom & SAM Cedric Nigel. "China and the United States: Tales of Two Giant Economies", *Bloomberg*, May 12, 2016

https://www.bloomberg.com/graphics/2016-us-vs-china-economy/

[3] China Power Team. "What does China really spend on its military? ", *China Power CSIS*, Oct 9, 2018

https://chinapower.csis.org/military-spending/

part of China's history. Indeed, from 1840 to 1949, China knew defeats, occupations, and internal disorder: the two Opium Wars; unequal treaties favoring European powers; territorial losses (Korea, Mongolia, and Tibet); the Boxer rebellion; wars against France, Japan, and Russia; Japanese invasion; and a civilian war that ended up with the victory of the communist party and the escape of the nationalists (the Kuomintang party) to Taiwan.[4]

In the aftermath of this civilian war, Mao Zedong declared that it was the end of the century of humiliation. By picking up this resentment, Xi Jinping declared, in 2012, that he wanted to achieve the two centennial goals: build a prosperous society for the 100th anniversary of the Chinese Communist Party in 2021 and, more importantly, have a "fully developed, rich, and powerful"[5] nation for the 100th anniversary of the People's Republic in 2049. Xi Jinping is on his way to become the second most important leader of the country after the greatest strategist Mao Zedong and to surpass the US in terms of global influence.

The Rise of the Renewed Pax Sinica

On top of its regional aspirations, China wishes to play a greater global leadership role, as seen in the latest Davos Forum (which Xi Jinping attended for the first time) and the latest Belt and Road Forum (which 30 world leaders attended).

During the 2017 G20 meeting in Hamburg, Xi Jinping introduced the concept of "the China Solution"[6], which he described as the support of "the common development of all countries, not just China's own sphere of influence. It is meant to build not China's own backyard garden, but a garden shared by all countries"[7]. This "China Solution" is represented by the Belt and Road Initiative (BRI), or the revival of the Silk Road, composed of mainly two corridors going from China to Europe: one by land through Central Asia, South Asia, and the Middle East, and the other by sea through the South China Sea, Bay of Bengal, and Red Sea.

In total, it will cover 65 countries, 60% of the world's population, and will improve trade, finance, and infrastructures[8]. It is in accordance with the shift to a model based on high-value industries, services, and domestic consumption for a country that wants to ensure its imports and exports[9]. China is slowly trying to establish military bases along the waterways from China to Europe; in Djibouti to protect the Bab-al-

---

[4] CHALIAND Gérard & RAGEAU Jean-Pierre. "Asie hindouisée – Asie sinisée", in *Géopolitique des empires*. Flammarion, Champs essais, 2015, p. 74

[5] GRAHAM Alison. "What Xi Jinping Wants", The Atlantic, May 31, 2017
https://www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/

[6] EDWARDS Will. "The 'China Solution': Beijing Aims for Global Leadership", *The Cipher Brief*, May 2, 2017
https://www.thecipherbrief.com/article/asia/china-solution-beijing-aims-global-leadership-1095

[7] EDWARDS Will. "The 'China Solution': Beijing Aims for Global Leadership", *The Cipher Brief*, May 2, 2017

https://www.thecipherbrief.com/article/asia/china-solution-beijing-aims-global-leadership-1095

[8] HILLMAN Jonathan. "Belt and Road Summit: Beijing's Push on Trade", *The Cipher Brief*, May 2, 2017

https://www.thecipherbrief.com/article/asia/belt-and-road-summit-beijings-push-trade-1095

[9] Stratfor. "China Paves the Way for a New Silk Road", *The Cipher Brief*, May 15, 2017

https://worldview.stratfor.com/article/china-paves-way-new-silk-road

Mandab Strait, in Pakistan for an easy reach to the Ormuz Strait, or in Myanmar's Coco Islands for quicker access to the Strait of Malacca, the soon-to-be busiest waterway in the world[10]. Thus, it comes with no surprise that Beijing is developing a power projection capability with blue-water navy maritime force to protect the flow of raw materials and merchandises.

The New Regional Hegemon

The current US uncertainty towards Northeast and Southeast Asia is a great opportunity for China, which has been more hawkish in the last few years. Beijing invested massively to create a modern and flexible army; the military budget doubled in 10 years, the first aircraft carrier is now deployed (with a second one under construction), and next-generation aircrafts are almost ready. All these efforts are possible thanks to cyber attacks and retro engineering prowess and enables power projection to support an Anti-Access/Area Denial tactic [A2/AD] to protect its activities in the South China Sea (aka the Nine-Dash Line).

The People's Republic of China (PRC) uses a mix of traditional (money) and cyber means (threat) to pressurize neighbors and protect its "strategic belt" (i.e. its coast, where most economic activities occur). In South East China, after a decade of cordial relations with some states through generous economic, commercial, infrastructural and cultural programs, the PRC shifted its approach and started to "flex its muscles". In Malaysia, the President is concerned about debt issue and cancelled a $22 billion worth project, such as the East Coast Rail Link (ECRL), which is part of China's BRI.[11] In the Philippines, the hard talk round seems to be over and both countries are trying to resolve their maritime disputes; a meeting is schedule before the end of the year between both leaders. [12] Furthermore, long-established allies of China, like Myanmar and Vietnam, are becoming more suspicious; a Chinese-backed dam project in Myanmar is at risk and in 2017, Vietnamese banks and airports were hacked allegedly by Chinese state-sponsored groups.[13]

Nevertheless, the lack of unity and capacity in the ASEAN will not stop China. ASEAN states can only sustain a low to medium intensity "gunboat diplomacy" even if the US deployed, to guarantee freedom of navigation, the USS Ronald Reagan aircraft carrier, in addition to the permanent carrier that belongs to the Navy's 7th Fleet based in Japan (USS Carl Vinson).

---

[10] HUANG Kristin. "Chinese defence adviser says Djibouti naval facility is a much-needed military base", *South China Morning Post*, May 13, 2017
http://www.scmp.com/news/china/diplomacy-defence/article/2094194/chinese-defence-adviser-says-djibouti-naval-facility

[11] MA Alexander. "Malaysia stood up to China's demands to hand over its persecuted Muslim prisoners, and Beijing is furious", *Business Insider*, Oct 12, 2018

[12] HEYDARIAN Richard, "Major Hurdles – and rewards – as China and Philippines try to forge deal to share South China Sea resources", *South China Morning Post*, Sept 22, 2018
https://www.scmp.com/news/china/diplomacy/article/2165237/major-hurdles-and-rewards-china-and-philippines-try-forge-deal

[13] LIVES Mike. "A Chinese-Backed Dam Project Leaves Myanmar in a Bind", *The New York Times*, Mar 31, 2017

https://www.nytimes.com/2017/03/31/world/asia/myanmar-china-myitsone-dam-project.html

Energy at Stake in Europe

Energy is fundamental for economic growth; it "is a massive generator of wealth"[14]. Energy is power and it ensures survival. As we see, the BRI poses a security dilemma for states surrounding the South China Sea over strategic waterways but not only. Indeed, in Europe, another issue is at stake. Although the BRI will "connect" Europe to China and ease trade and business with the Middle Kingdom, state-owned electric utility company *State Grid Corporation of China* is investing, mostly in mergers and acquisitions in Europe, just like Russian energy companies did in the 2000's and let to a divided European voice against Putin's vision of the Russian reemergence.

At that time, generous oil and gas prices gave Moscow the ability to defend and expand its interests outside its borders. Through economical investment (like joint ventures, the purchase of shares, acquisitions of pipeline companies and refineries, etc.) in oil and gas companies, Russia increased its leverage. It created a grip and a decision capability in the heart of the European Union territory.

Similarly, in recent years, Europe has received record levels of Chinese inward investment, with minimal barriers to Chinese-led mergers and acquisitions. But now, Western nations are pushing through stronger measures to block foreign direct investment (FDI) and foreign takeovers of strategic economic assets, citing security concerns.[15] Recently, Germany, the UK, France and Italy, took steps to introduce legislation, while the European Union looks to adopt an investment screening mechanism by the end of the year.[16]

The Chinese grand strategy will not be easy to implement, but it paves the way for a long-term vision for China to protect its own interests like former and current superpowers such as Spain, Great Britain, or the US. This century will be China's and a renewed *pax sinica* is slowly taking shape.

The Dragon's Cyber Claws

China's traditional hacking against the US, along with cyber spying, mostly targeted defense and aerospace companies for reverse engineering purposes, as seen in two major Advanced Persistent Threat (APT) campaigns dubbed "Titan Rain" and "Byzantine Hades" that enabled massive exfiltration of classified information. But one of the biggest data breaches allegedly attributed to China, against the Office of Personal Management (OPM) in 2015, was probably

[14] YERGIN Daniel, "The Prize: The Epic Quest for Oil, Money, & Power", New York: Free Press, 1991, p.13
[15] THIRUCHELVAM Sharon, "Strategic foreign takeovers worry the West", *Raconteur*, Oct 2, 2018
https://www.raconteur.net/finance/strategic-foreign-takeovers
[16] Ibid.

done to compile a database of 22.1 million US government employees for further use.[17] For the last three years, China has been especially aggressive on espionage and the 2017 killing or imprisoning of dozen of US sources in China might be related to the OPM breach.[18] Other explanations also incriminate a mole within the CIA or the crack of the encrypted method of communication between the CIA and its field assets.[19]

Nevertheless, since the 2015 US-China deal on electronic espionage, Chinese hacks dropped and their attacks are now particularly focused on critical infrastructure across Asia in India, Indonesia, the Philippines, Vietnam, Hong Kong, Japan, and Singapore.[20] All these countries are part of the BRI project or are related to political interests in Hong Kong and Japan. Beijing is probably trying to get entry points within governments and critical infrastructure to have better leverage in the medium and long term. The fear of cyber economic espionage, notably in Germany, the UK and Australia, pushed similar "non cyber attacks" deals.[21]

George Orwell 2020

Regarding its domestic policy, the communist party is obsessed with control. It tries to control citizens' lives in every possible way to avoid liberty, protest, alternative thinking, initiative, or unpredictability. The PRC combines legislation and technological actions to censure and regulate the Internet domestically. For example, the new Cyber Security Law that came into effect in 2017 gives the Chinese government a greater oversight over the cyber space architecture.[22] For example, in some parts of the law, the language is vague and imprecise, which could be invoked by the authorities for inspections, even into proprietary technologies or intellectual property, compromising business secrets and sensitive information.

On top of the "Great Firewall" that limits access to websites on the global Internet (like *Facebook* or *Google*) and the "Green Dam", a software package installed on personal computers to monitor online activity, the government devised a new way to enforce obedience among the citizenry: *Sesame Credit*. The social credit system app collects data to measure how much the user follows the party line. For

---

[17] NAKASHIMA Ellen. "Hacks of OPM databases compromised 22.1 million people, federal authorities say", *The Washington Post*, Jul 9, 2015
https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[18] MAZZETTI Mark. "Killing C.I.A. Informants, China Crippled U.S. Spying Operations", *The New York Times*, May 20, 2017
https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html

[19] MAZZETTI Mark. "Killing C.I.A. Informants, China Crippled U.S. Spying Operations", *The New York Times*, May 20, 2017
https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html

[20] VASAGAR Jeevan. "Chinese hackers shift focus to Asia after US accord", *Financial Times*, Apr 26, 2017
https://www.ft.com/content/c8e634fa-2a31-11e7-9ec8-168383da43b7

[21] SMYTH Jamie. "Australia and China in pact against cyber theft", *Financial Times*, Apr 24, 2017
https://www.ft.com/content/9df81164-28b5-11e7-9ec8-168383da43b7

[22] MUNCASTER Phil. "Foreign Firms Should Fear New Chinese Cyber-Law: Report", *Infosecurity Magazine*, Sep 1, 2017
https://www.infosecurity-magazine.com/news/foreign-firms-fear-new-chinese/

example, it collects big data about the user's behavior on social media, travels, what is shared or posted, and a multitude of other data like shopping patterns.[23]

All behavior is related to points and an overall score is displayed. For example, if you purchase a foreign item, like a Japanese manga, your score goes down. If you repost news from state media agency, it goes up. The higher the score, the better citizen you are. A good score rewards you with benefits: find a new accommodation in a good neighborhood, make it easier to get a loan, be able to enroll your child in a highly rated school, have online discounts or avoid queues for administrative documents.

It goes even further. Because it is based on social media, the app scans your network and, if you have friends with low scores, it will downgrade yours. That is the strongest point of this app: the government does not really need to intervene because social pressure will do the job. There are no consequences yet for a low score, but rumors say that they could come by 2020 when the app should be highly recommended to download. These consequences may be slower Internet speed or restriction from certain job applications.

Days of Future Past

Currently, China is already the biggest cyber market in the world with more than 730 million Internet users, mostly on mobile phones.[24] Its tech companies, such as *Baidu, Alibaba, and Tencent* (aka BAT), even if relatively unknown on the global market, are economic giants.[25] These companies are growing, investing abroad (transport, automobiles, e-commerce, on-line services), and supporting the international government's policy.

Assisted by big data, the rise of BAT and the imposition of domestically built technologies in its strategic sectors like banking or energy, the Middle Kingdom is able to sustain its mixed model of an authoritarian system coupled with economic growth. With this patriotic sense of belonging, the government tries to avoid the affirmation of the newly established middle class that could also wish for more liberty and democracy. Moreover, the rest of the world has less and less room for manoeuver regarding Beijing schemes, as seen with the disappearing of Interpol's ex-president Meng Hongwei or the situation with the Muslim minority in Xinjiang. Xi Jinping is the Chinese leader who has centralized most power since Den Xiaoping and he will continue this way after having been reelected during the 19th National Congress in October of last year.

---

[23] HATTON Celia. "China social credit: Beijing sets up huge system", *BBC*, Oct 26, 2015

http://www.bbc.com/news/world-asia-china-34592186

[24] International Monetary Fund, "China's Economic Outlook in Six Charts", *IMF News*, Jul 26, 2018
https://www.imf.org/en/News/Articles/2018/07/25/na072618-chinas-economic-outlook-in-six-charts

[25] The Economist. "China's Internet giants go global", *the Economist*, Apr 20, 2017

http://www.economist.com/news/business/21721203-tencent-leading-acquisition-spree-alibaba-close-second-chinas-internet-giants-go

About the Author

Julien Chesaux is a Cyber Security Consultant at Kudelski Security, a Swiss and American cyber security company. Julien mainly works on cyber security, information security and geopolitics analysis in order to help clients to find solutions regarding their threats. He is also a mediator and writer for the Swiss Think Tank Foraus and the co-founder of the www.stralysis.com. He has worked in diplomacy and cyber security for seven years in Switzerland, Australia and France. His main research interests are Global Security, Cyber Geopolitics, and International Affairs.LinkedIn profile: www.linkedin.com/in/julien-chesaux-65279456

What is PII and Why Criminals Want Yours

As any cybersecurity expert will tell you: the ultimate goal of securing your online presence is protecting your PII data. PII, also known as Personally Identifiable Information, is simply any information that can be used to identify, locate or contact you or an individual. Examples of PII data include information as basic as a name, more personal info like your social security number and, unfortunately, even extremely private data like health and financial information and records.

And to criminals involved in PII data discovery, your email happens to be an absolute goldmine. It's why email hacks are becoming more commonplace. For instance, you might have heard about the effective Gmail phishing campaign from 2017 that affected thousands of users, or when Yahoo admitted last year that they suffered a massive hack that compromised three billion user accounts.

Fortunately, it isn't a hassle to protect your PII data anymore, as there are quick and simple methods to secure it.

What is Your PII Data?

Your PII is basically any information used for identification, such as:

- Name
- Birth date
- Social security number
- Addresses
- Telephone numbers
- Passwords
- Payment methods
- Education information
- ID numbers
- Insurance information
- Medical records

Look familiar? It's likely that you've emailed many of these items in one form or another.

It's important to point out that even seemingly unrelated PII data can be pieced together like a puzzle; an enterprising cyber-criminal can use that information to complete an online profile of you to impersonate you or others online. Little details like street addresses, name of spouse, and other bits of information commonly used for security questions are common targets for hackers with the time and patience to sift through your information.

And, considering the types of accounts protected by these security questions: social media accounts, online banking, ecommerce sites, it's not hard to see how PII data discovery could be a gateway to other, more serious breaches.

What's My PII Worth?

Believe it or not, consumer data and businesses alike have a very high monetary value. Not just because a hacker can potentially access your bank account and credit card numbers (although that's always a risk), but because your information can fetch a pretty penny on the dark web and online black market.

On average, a consumer's passwords sell for around $80, while even small details like purchase history can sell for $20. Credit card numbers can sell for as little $5, while passports might fetch up to $2,000.

Where My PII Is Sold

Your PII is a hot item in the dark web, the underground markets where hackers can illegally sell your information. Depending on the information they extract from your emails, your PII can be sold for identity fraud, fraudulent loans, counterfeit credit cards, money transfers, or even more complicated schemes like blackmail and extortion.

A cybercriminal can use PII data for activities such as paying bills, performing fraudulent online transactions, creating counterfeit credit cards for their own use, and transferring money out of a victims' bank account.

What Can I Do to Protect My PII?

Your emails function as a type of online ID, which is why it's so essential that you take great care to secure PII data when communicating online. If you're sending important documents like marriage certificates or tax forms, make sure to encrypt the attachments—encryption will protect your information and keep it from anyone other than the intended recipient. You should also encrypt emails if you feel like there's any relevant PII in the content. Even a name, address or phone number. Tracking and postmarking electronic communication are also great ways to secure your emails to make sure they are going where they should—and to whom they should.

According to a recent survey by Generali Global Assistance, 75% of online users are worried about online identity theft. Yet surprisingly, another survey by TransUnion showed that only 15% of consumers believe they have the proper tools to protect their personal data. Thankfully, the tools are definitely out there. If you're ready to protect yourself from online threats, look for a trustworthy secure email service with the ability to track and encrypt all your emails. Your PII—and your online identity—will thank you.

About the Author

Idan Udi Edry is the CEO of Trustifi, a software-as-a-service company offering a patented postmarked email system that encrypts and tracks emails. Before his work with email encryption, Idan served as an Israeli Air Force officer for more than eight years, reaching the rank of captain and leading hundreds of professionally trained military personnel in building and operating advanced information systems. A trusted authority in information technology and data security, Idan has 13 formal certifications from the most renowned IT and telecommunications organizations, and his insight has been featured in major publications like Fox News, Bloomberg BNA, and MD Edge.

New Data Affirms Cyber Threat for Industrial Control Systems

Recent CyberX report finds that plain-text passwords, direct internet connections and weak anti-virus protections place industrial control systems at risk for cyberattacks

by *Phil Neray, VP of Industrial Cybersecurity, CyberX*

"Press Here to Kill Everybody," the provocative title of Bruce Schneier's new book, gets right to the heart of the risks involved in industrial cybersecurity. Destructive malware such as WannaCry and NotPetya, as well as targeted attacks such as TRITON and Industroyer, have shown the potential impact of cyberattacks on our industrial control systems (ICS). The costly production outages and clean-up costs alone put companies at great risk, but even those are overshadowed by the potential impact of catastrophic safety and environmental incidents.

Though positive steps have lately been taken to secure our ICSs, new data from CyberX, the IIoT and ICS security company, finds that these systems are still soft targets for adversaries. The data behind our 2019 "Global ICS & IIoT Risk Report," released on October 23, shows that major security gaps remain in key areas such as plain-text passwords, direct connections to the internet and weak anti-virus protection.

We also found the prevalence of Windows XP and other legacy Windows systems has decreased year-over-year — driven top-down by management in the aftermath of NotPetya's financial damage — but we're still finding unpatchable Windows systems in 53 percent of all industrial sites.

Unlike questionnaire-based surveys, our report analyzes real-world traffic from production ICS networks, making it a more accurate representation of the current state of ICS security. The report is based on data collected over the past 12 months from more than 850 production ICS networks, across six continents and all industrial sectors including energy and utilities, manufacturing, pharmaceuticals, chemicals, and oil and gas.

Among the key findings of our report, we found that 69 percent of industrial sites have plain text passwords traversing the network. Lack of encryption in legacy protocols like SNMP and FTP exposes sensitive credentials, making cyber-reconnaissance and subsequent compromise relatively easy.

Whether for convenience or inattention, 40 percent of industrial sites have at least one direct connection to the public internet. With digitization as a key business driver, operational technology (OT) networks are now also increasingly connected to corporate IT networks, providing additional digital pathways for attackers.

According to our findings, at least 57 percent of industrial sites are still not running any anti-virus protections that update signatures automatically, leaving the programs largely ineffective, and 16 percent have at least one Wireless Access Points (WAP). Misconfigured WAPs can be accessed by unauthorized laptops and mobile devices, and sophisticated malware such as VPNFilter target access points such as routers and VPN gateways, enabling attackers to capture MODBUS traffic, perform network mapping, destroy router firmware and launch attacks on OT endpoints.

As we continue to both assess past attack methods and the current state of our networks and vulnerabilities, a path towards remediation and protection becomes clearer. Not everything can be protected at once, but ruthless prioritization is required. In the report, we lay out a series of eight steps towards protecting an organization's most essential assets and processes. These include: continuous ICS network monitoring to immediately spot attempts to exploit unpatched systems before attackers can do any damage; threat modeling to prioritize mitigation of the highest consequence attack vectors; and more granular network segmentation.

Analyzing the data for the second time in two years also gave us an opportunity to compare data and look for trends, and perhaps the most important conclusion we reached after looking at the delta between last year's report and this year's report is that the delta itself is small, and the industry may not have changed much over the course of the past year. Other than the drop of industrial sites using legacy Windows systems from 76 percent last year to 53 this year, the rest of our data changed in relatively small increments.

In comparison to last year, where the median overall risk-readiness score across all industrial verticals was 61 percent, our latest research puts the score at 70 percent. These results, however, fall short of CyberX's minimal recommended readiness score of 80 percent. With this year's report, the risk-readiness score by industry is 67 percent for manufacturing, 68 percent pharmaceuticals and chemicals, 79 percent for energy and utilities, and 81 percent for oil and gas.

As these numbers suggest, awareness about the need for stronger ICS defenses is growing, but there's still a lot of work to be done. When looking at the scope of the current ICS security situation and its many complexities, it bears remembering that we are attempting to close a 25-year gap between OT and IT security practices.

About the Author

Phil Neray, vice president of Industrial Cybersecurity, CyberX. Prior to CyberX, Phil held executive roles at enterprise security leaders including IBM Security/Q1 Labs, Symantec, Veracode and Guardium. Phil began his career as a Schlumberger engineer on oil rigs in South America and as an engineer with Hydro-Quebec. He has a BSEE from McGill University, is certified in cloud security (CCSK), and has a 1st Degree Black Belt in American Jiu Jitsu.

Phil can be reached on Twitter @ rdecker99.

How Organizations are Tackling Cyber Challenges: Takeaways from the Cybersecurity Imperative

Joe Gittens, Director of Standards, Security Industry Association

The physical security industry has joined other business sectors in fully embracing the age of digital transformation. As innovative ways of accessing, creating and processing information radically change the expectations of customers, enterprises are spending vast resources on their digital transformation strategies. While this fast-paced technological revolution is proving to add value to the top and bottom lines of businesses, attention to cybersecurity needs to be baked into the process – and cybersecurity is often overlooked by those companies that are beginning this journey. The Security Industry Association has joined business and technology leaders such as HP, Baker Mackenzie and *The Wall Street Journal* in supporting a first-of-its-kind research study, The Cybersecurity Imperative. The study, conducted by independent research company ESI ThoughtLab, collected data from a wide sample of over 1,300 global companies to provide cybersecurity benchmarking on how organizations are tackling cyber challenges via focuses on people and technology while in the throes of the new industrial revolution.

You cannot go to an industry trade show or trade press without being inundated with messages about the rise of new technologies such as artificial intelligence, blockchain, open application platforms and the Internet of Things. While the business potential of these technologies is obvious, The Cybersecurity Imperative found a strong correlation between the digital maturity of a business (identified by maturity on the National Institute of Standards and Technology framework) and its cyber risk exposure. Particularly frightening, the study showed that over half of the companies that were digital leaders on the business end were not cybersecurity leaders. This combination of rapid digital expansion and lagging cybersecurity posture could be a powder keg, and the problem is expected to grow: new technologies mean new vendor partners. While only one in five businesses are currently concerned about the likelihood of being attacked

through partners and vendors, that number rises to 70 percent when organizations are asked if they see the same as a risk they will have to deal with in the next two years.

It's not all doom and gloom; the research also goes into detail about what companies are doing correctly to keep cybersecurity on pace with digital maturity.

- Education is key; 87 percent of companies reported that general staff represented the greatest cyber risk within their organizations. More cyber- mature organizations invest in continuous training that bakes security into the culture of the organization, not only a quick onboarding.
- Investment is crucial; however, even more important is a well-rounded and evolving investment strategy. Too much investment in technology without investment in skilled cybersecurity talent is a recipe for disaster; however, the reverse is true too – not even the most skilled cybersecurity talent can function effectively without the right tools of the trade.
- Engagement is necessary. This engagement should be at the C-suite and board levels. Companies should consider recruiting leaders with information technology and cybersecurity expertise. An organization must ensure that the leadership team is given a clear picture of cyber preparedness, improvements in risk identification and knowledge of the cyber talent/technology portfolio of the organization.

The impact of cybersecurity incidents is disruptive – to operations, finances and reputation. The stakes are too high for organizations to not have well-rounded cybersecurity plans in place connected to their overall digital maturity. Business leaders must embrace network security just as readily as they embrace new avenues of digital customer interaction, and The Cybersecurity Imperative shows that they are not alone in this journey.

About the Author

Joe Gittens is the director of standards for the Security Industry Association. In this capacity, he is the staff liaison in direct support of the various technical efforts underway in the SIA Standards subcommittees and working groups. Joe provides leadership in assessing and educating SIA members on emerging technologies that require the industry's attention – advancing the continued convergence of physical and information security. He was recognized as a 2016 American National Standards Institute Next Generation Standards award winner for his work with SIA and liaising with other standards development organizations. Joe holds degrees in mechanical engineering and economics from the University of Virginia and spent his early career performing technical research in various fields ranging from information technology to financial services.

Ransomware and Cyber Attacks Dive in 2018

Sean Sullivan, Security Advisor, F-Secure

Cyber-crime isn't tied to a calendar. But when the calendar hit 2018, the threat landscape seemed to transform suddenly.

In 2017, the two largest ransomware outbreaks ever – WannaCry and NotPetya – rocked businesses around the world. F-Securer's global network of honeypot servers detected 546 million ransomware attacks in the last half of 2017 yet, in 2018, attacks were slowing with a total of just 246 million.

From Russia, With…Love?

So what accounted for much of the overall reductions in attacks? The answer - one country.

F-Secure began reporting data from decoy servers set up expressly to attract the interest of attackers in 2016. Since then, Russia has been the source of the greatest number of attacks. But in the first six months of this year, the UK knocked Russia out of its usual first place.

The United States remained the top destination country for attacks at 97.7 million attacks. Russia endured a little less than third of that volume with 32.7 million attacks and Germany was hit by 29.6 million in third place.

Perhaps unsurprisingly, the most common attack was still Russia to the United States. However, the volume of attacks is much lower than before – only eight million in first half of 2018, compared with about 140 million for all of 2017.

A quick note: the presence of a country on the list does not necessarily indicate the people behind an attack are inside that country. There are several methods where attackers can leverage proxies to cloak their activities, including VPNs or TOR, and compromised machines or infrastructure.

The slowdown of attacks from Russia could turn out to be temporary, but one shift in the threat landscape looks to be more enduring.

The End of the Ransomware Gold Rush

Ransomware attacks grew in volume by over 400 percent in 2017 compared with the previous year, thanks largely to WannaCry. But they became less common as the year progressed. In 2018, ransomware remained a potent threat but the slowdown in attacks continued.

A number of factors played into what appears to be the end of the ransomware "gold rush." These include the wild unpredictability of Bitcoin pricing which made it impossible for people to pay ransoms, improvements in antivirus that led to increased effectiveness in blocking the threat and the decline of exploit kits as a means of infecting users.

There's no one answer but the shift of focus by cyber criminals was clear; the number of unique ransomware families or variants per month peaked at 45 in May of 2017 and was down to 15 by December.

Cryptojacking – unauthorized borrowing of a device's computing resources for cryptocurrency mining – overtook ransomware in terms of numbers in 2018. Spam also experienced a mighty resurgence, coming in at #1 as an attack vector of the first half of 2018.

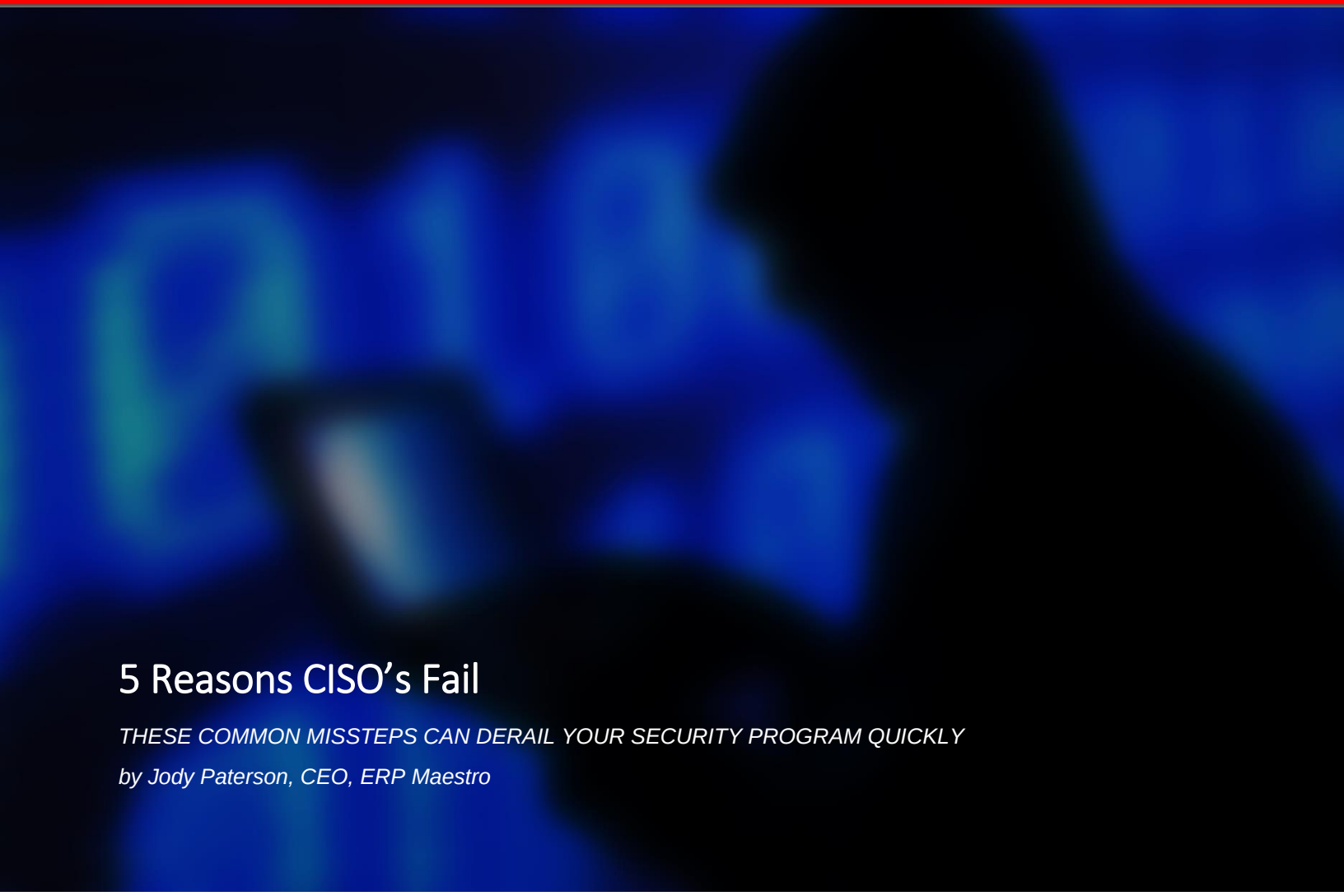
This also suggests cyber criminals are running out of other attack vectors due to improved system security against software vulnerabilities and exploits. Left without these tricks, attackers are attempting to exploit users through social engineering instead.

About a third, 31%, of spam email featured links to malicious websites, while 23% contained malicious attachments. In addition, 85% of malware attachments were found to be one of five file types: 7Z, DOC, PDF, XLS, or ZIP, and most were infostealers, RATs and banking Trojans. The other 46% of spam was mostly dating scams, which also appear to be making a comeback.

Cyber criminals have proven they have no loyalty to anything but making money. If one type of attack stops proving financially viable, they try another and another until they've tried anything that connects to the internet. All cyber defenders can do is keep improving defenses, plugging vulnerabilities and preparing for an inevitable successful attack. If you do all three, you may get a little luck. That seems to be what has happened in 2018. At least, so far.

About the Author

Sean Sullivan, Security Consultant Chief Security Scientist, F-Secure Sean aims to bring security issues to a global audience by actively communicating with the media to make technology more approachable. He has been with F-Secure since 2006, previously as a research analyst. Joseph can be reached on f-secure@eclat.co.uk, @ 5ean5ullivan and at our company website https://www.f-secure.com/en_GB/welcome



5 Reasons CISO's Fail

THESE COMMON MISSTEPS CAN DERAIL YOUR SECURITY PROGRAM QUICKLY

by Jody Paterson, CEO, ERP Maestro

Increased security breaches, fraud and access risks have resulted in the advent and rise of the Chief Information Security Officer (CISO) as a critical executive. Statistics indicate that these security concerns continue to escalate and also include a surge of internal cyberattacks. The need for the CISO is clear.

According to a Ponemon Institute report, "as cyberattacks and other threats increase in frequency and sophistication, the CISO role will become more critical, especially in managing enterprise risk, deploying security analytics, and ensuring the security of Internet of Things (IoT) devices."

Most CISOs have a sharp vision for the mission of their role: protect the organization, safeguard the business name and reputation, prevent personal and executive liability, and try to do it in the most cost-effective way possible.

However, even the most experienced security executive can make mistakes that put a company at greater risk. The following are common blunders that cause CISOs to fail and put their jobs at risk, with advice on how to avoid making the same errors.

Failure to Communicate Effectively With the Board

CISOs are typically expected to present to the board of directors and give them an overview of security operations and the state of risks, as well as to make the business case for further security investments. Audit committees and chairs are increasingly requiring solid security metrics to prove a company's risk level. They, too, don't want to incur risk or reputational damage related to their own accountability. However, such communication between boards and security leaders can be a stretch if a CISO struggles to effectively share knowledge that makes sense to corporate leadership, especially if intuitive reporting that is easy enough for board members to comprehend quickly is lacking. Additionally, there is often a disconnect between the security leader's priorities and the board's agenda.

A 2017 report from risk management firm Focal Point Data Risk found that a majority of CISOs struggle to adequately convey the value of security to the board. Many CISOs cited board awareness of security (or, specifically, lack thereof) as a major reason why it is difficult to communicate security's value effectively.

It is the CISO's job to understand what the board values, learn to speak their language, and to make the case for security. And that means taking every opportunity to engage with executive leadership and board members to discuss the challenges a CISO faces. It is also critical to explain how security furthers corporate goals and serves as a business enabler. The CISO should demonstrate security's value with concrete examples in a way

the board and can relate to and understand. That means skip the deep analytics and talk to them in plain, understandable language when you have their ear. Use visual reporting when possible to show risks in an easily digestible format.

Failure to Foster a Corporate-Wide Security Culture

According new research from ISACA and CMMI Institute, CISOs are still struggling to make security a priority throughout their organizations. The Cybersecurity Culture Report found that just five percent of employees think their organization's cybersecurity culture is as advanced as it needs to be to protect their business from internal and external threats.

The research, based on more than 4,800 business and technology professionals who shared their insights, also found 42 percent of organizations do not have an outlined cybersecurity culture management plan or policy.

What's at the heart of an effective cybersecurity culture? It is an understanding among all employees that security is everyone's business. Security awareness and behaviors are part of daily operations and it is considered a priority at the highest level. Unfortunately, in many businesses, this is still not the case as the research revealed that just 34 percent of respondents understand their role in their organizations' cyber culture.

Getting everyone's buy-in on security, and creating a top-down security culture, should be a top mandate for any CISO.

Failure to Communicate the Right Balance of FUD and Hyperbole

As mentioned, CISOs need to not only communicate security's importance to the board, but also to employees across the company. A certain amount of fear, uncertainty and doubt (FUD) to stress the importance of security measures, enforce policies and avoid complacency is necessary, but creating an environment of exaggerated risk is not conducive to positive change and adoption of security measures. Conversely, enabling employees to don rose-colored glasses is likewise not effective. Find the balance.

Using real-world examples to educate within reason is great; however, make sure you communicate them in the context of your own organization and have a clear picture of your own risks as they relate to such stories. Offer facts and then explain what security is doing to respond and/or prevent threats in your organization. Even better, can you bring forward examples of what you are doing to mitigate risk and how it helps your business avoid becoming the next statistic?

Failure to Adopt a Holistic Strategy

In an excellent post on Forbes, William H. Saito, Special Advisor of the Cabinet Office and Prime Minister for the Government of Japan, and former Vice Chairman for Palo Alto Networks Japan, makes the case that it is time to stop playing whack-a-mole with threats. Randomly addressing risks as they occur does nothing to prevent risks overall.

CISOs need to look at security from a holistic view–including both external and internal risk –starting with a big-picture concept of strategy that is unique to one's organization, and then implement tools from there. Saito recommends getting away from piecemeal integrations put in place without any overarching policy, which translates into costly but poor integration.

Security strategy should be proactive, with an eye on current and future threats. CISOs always should be striving for self-education on security trends and solutions by networking with peers, reading the latest news, and communicating with others in the industry.

Failure to Use the Best Defense Tools

New technologies bring new risks. It's the CISO's responsibility to understand and vet all new technologies a company considers for use and to comprehend the security risks for each. Additionally, the CISO is accountable for finding and implementing the security platforms to keep those systems protected –from both external and internal risks.

The CISO should be able to present ongoing security assessments for technologies continuously throughout the year as part of an access control strategy and to satisfy audit requirements. Being able to keep a company safe in an efficient and cost-effective way will help a CISO win favor with the CEO, CFO and board members.

Avoid These Pitstops on the Road to Security Success

The same Ponemon report stated that “the IT security function will transform from a cost center to a revenue center; hence the CISO will be more involved in brand and reputation protection.” Having the right security knowledge and tools, clearly communicating risk, building a balanced security-centric culture and holistic strategy to address both internal and external risks can help the CISO avoid missteps and keep both a company and his/her job secure.

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/.

The Internet of Things Predictions for 2019

By Milica D. Djekic

It appears that this 4th industrial revolution would bring us so many new stuffs that could dramatically impact our lives and businesses. One of the best known outcomes of our modern time is the Internet of Things (IoT). The IoT technologies are not anything being so genuine, but rather the transformation of a digital landscape that has existed before. The tendencies through the history would suggest that new and new solutions would seek from us more skills, knowledge and expertise. Even if you are the end user of this cutting-edge technology, you would need to demonstrate the certain level of familiarity with those advancements.

Right here, we would want to make a brief discussion how the IoT landscape would change in the coming year and why it is important to remain up-to-dated with the new trends. In other words, if you understand the changes in any field, you would get capable to take the quite huge advantage over such an area. The IoT is so recent concept that would show the tendency to get better, bigger and more progressive, so for those reasons – we would make our prognoses about how it would look like in the 2019. In this effort, we would use the five indicators that would support us to deeply cope with this area's tendency. The indications are as follows!

The Better Security

It's quite known that the main challenge with the current technologies is their security. The similar situation is with the IoT advancements. Such a field would get bigger, but so many consumers would complain that they would not feel safe enough relying on these solutions. The ongoing trends would suggest that year by year the experts would work so hard in order to investigate and respond to security requirements of their solutions. The better security may mean the stronger encryption, but would that be sufficient in case of the IoT technologies? There is no unified answer to that question and if we talk about the IoT – we should know that it's about bunches of devices being connected to the global network which would offer them an opportunity to communicate with each other using the internet connectivity. In other words, any IoT device would deal with the web connectivity and get the IP address being assigned to so. It's well-known that the good cryptography would mean more reliable communications channel and such an approach may resolve only the part of the entire problem. The rest of the response coping with the better security would need the best practice getting applied to this sort of improvement. So, if you want to tackle the challenge as security is you need to work so hard on your cyber defense procedures and policies as well as education and training.

The Higher Performances

The next thing that could get improved in the coming time is the IoT performance. As we would know, the IoT is nothing else, but the digital transformation of something exiting much before. On the other hand, if we discuss the IoT – we should know that it may combine the digital, embedded and mechatronics systems with the web connectivity. For instance, if we apply the faster internet communications to our IoT solution, it would definitely cope with the higher performances. Also, any of the mentioned technological advancements could get improved and if the embedded system gets the better microprocessor or more memory – it would obviously offer the better performances to the entire IoT system. The tendencies over the globe would suggest that our electrical, electronics, mechanical and computing solutions are getting better and better developed every single day, so for such a reason – we can predict that the entire IoT systems would get with much higher performances in the 2019!

The Bigger Marketplace

It would seem that the IoT marketplace would develop at a quite fast pace. Some indicators would suggest that in the next year or two we would have about 50 billion IoT devices getting connected to the huge network. This fact could open up so many doors to the IT industry actors to make the good profit and also empower their economies. Such a tendency may bring with itself a plenty of social impacts as well. For instance, there would be the large IoT community worldwide that could deal with some kind of new culture hanging on the web and using the smart devices. The social impacts could go that far away to change the ways how people think and live. Anyhow, this would not happen that rapidly, but rather more slightly – so we can expect that the 2019 would bring some changes and not the entire boom in such a sense.

The Need for Standardization

The IoT marketplace is growing so fast, so would that mean we should make some sort of the order within such an area? Definitely yes! Some tendencies would indicate that there is the strong need for the international standardization of the IoT landscape. The experience would suggest that any kind of the standardization could bring us more quality regarding our organizational and management demands. Even the NIST would stress on the need for international cybersecurity standards for the IoT technologies and such an initiative would cope with so many well-researched and developed overviews. The standardization usually means the better productivity and effectiveness because of its keen to deal with well-developed organization of both – people's activities and production processes, so far! As it's known, the standardization of the IoT is the big job, so we believe that the 2019 would make some progress on in such a fashion.

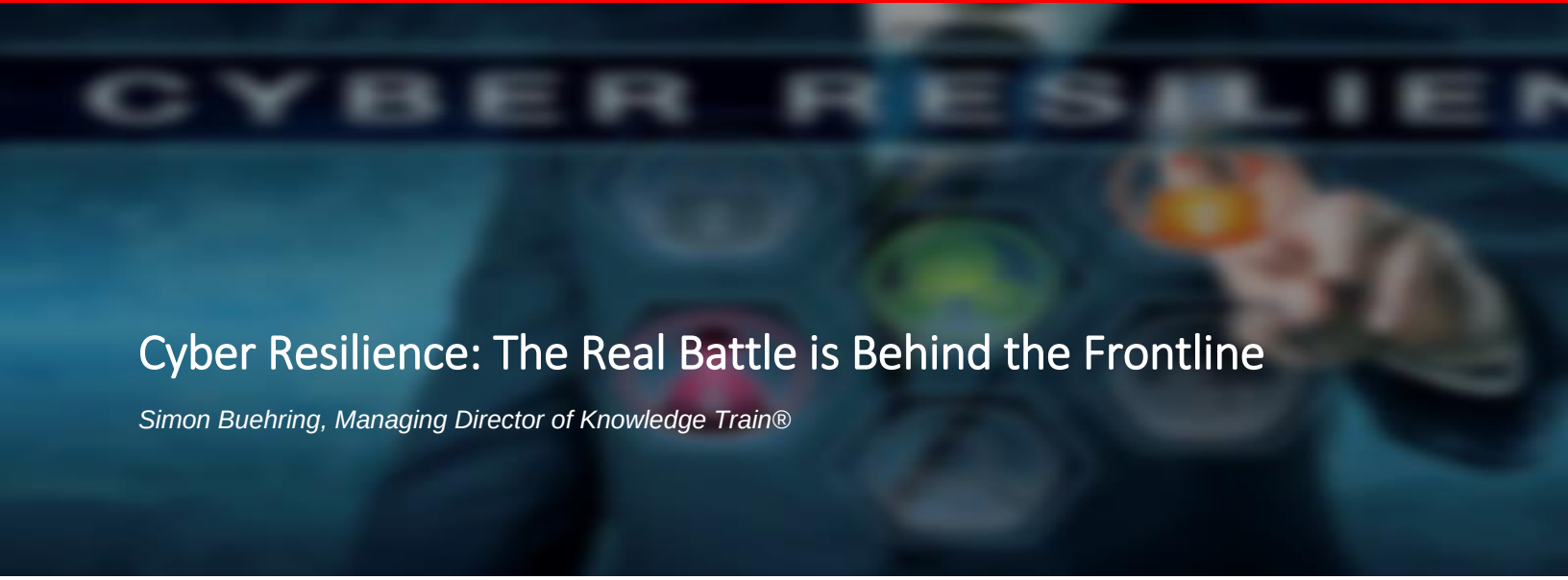
The More Optimal Production Cycle

Indeed, the IoT solutions would pass through some production process and this kind of stuff could get so complicated. In order to simplify such a requirement we should look for more sophisticated approaches. The good production cycle should bring us the excellence as the outcome and from such a point of view; we would need to think smartly how to organize our production. The standardization can help here a lot, but what we need the best is some kind of strategic planning and intelligent scheduling of the entire

process. Any project needs the good preparation and research at its beginning and so many assessments and quality controls at its finalizing stage. In such a way, if we make things being more optimal – we can expect some financial benefits for a reason we could avoid the business discontinuity and minimize any kind of losses. The 2019 is just around the corner, so we would see what it would bring on to us!

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book *"The Internet of Things: Concept, Applications and Security"* being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Her fields of interests are cyber defense, technology and business.



Cyber Resilience: The Real Battle is Behind the Frontline

Simon Buehring, Managing Director of Knowledge Train®

Whilst media reports about cybersecurity focus on high profile cyberattacks, behind the cyber frontline a new battle is being fought.

It was recognized earlier this decade that the US was at risk of calamitous cyberattack from state-directed actors. If a hostile nation wanted to wage war against the US, it would likely be in a form of warfare which the world had not yet seen. Maliciously damaging the country's infrastructure, particularly its power generation, nuclear, water, transportation, health services or critical manufacturing plants would have a crippling effect on the population.

A sign of things to come arrived in 2010, in the form of the Stuxnet attack by Israel on Iran's nuclear centrifuges. It was the first high-profile cyberweapon specifically targeting industrial control systems. Stuxnet shut down over one third of Iran's centrifuges. It showed that cyberweaponry could be a very potent new type of weapon which could be used to seriously degrade an adversary's industrial capability.

In 2017, the WannaCry ransomware attack was reported in over 150 countries. Although WannaCry was not designed to target industrial control systems (ICS), it managed to infiltrate some ICS which led to the downtime of industrial production, such as the one which affected the Dacia car company, a subsidiary of Renault.

On the front line of defense for businesses, governments and individuals have been cybersecurity tools and techniques. These often encompass identifying electronic data, implementing technology and the business practices that will protect it.

Yet there's been a growing realization over the years that hackers will always have the upper hand. As new vulnerabilities emerge, they are quickly exploited, and a game of cat and mouse ensues with security companies patching holes in systems only for new vulnerabilities to emerge. These in turn are targeted by hackers.

In response, the assumptions upon which the cybersecurity industry were based have shifted. Instead of assuming that hackers can be kept out by applying ever-more sophisticated defenses, there's been a growing realization that at some point systems will be penetrated. It would be wise therefore to be able to recover quickly from such an attack with minimal damage.

That's the concept of cyber resilience - broadly speaking your organization's ability to withstand or quickly recover from cyber events that disrupt usual business operations. It has been discussed for several years now, as the risk of cyberattacks has increased.

Back in 2009, Carnegie Mellon University Software Engineering Institute announced its CERT® Resilience Management Model (CERT®-RMM) version 1 as a foundation for a process improvement approach to operational resilience management. The CERT®-RMM is a maturity model which can be used by organizations to help them manage and improve their operational resilience.

When the Department of Homeland Security (DHS) published its Cyber Resilience Review (CRR) in 2016, it was derived from CERT®-RMM. The CRR assesses organizations against a set of criteria from the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Later the same year, the DHS created The Critical Infrastructure Cyber Community (C^3) Voluntary Program to help organizations use the Cybersecurity Framework to improve their cyber resilience. This included guidance on how to use the Framework in key industries: chemicals, critical manufacturing, dams, emergency services, healthcare, nuclear, transportation and water to name just a few.

One of the problems with the US government's approach to cyber resilience is that C^3 is voluntary. That's a concern. According to The State of Industrial Cybersecurity 2017 report by Kaspersky, over half of the sampled organizations experienced one or more incidents on their industrial control systems in the previous year. In fact, targeted attacks were the second biggest actual threat to industrial systems and caused incidents in over a third of companies.

So, as the likelihood of aggressive state actors view ICS as a target, there remains no legally-binding mechanism to force companies to build resilience into their systems to protect society.

In 2011, the Partnering for Cyber Resilience report from the World Economic Forum (WEF) recognized the importance of cyber resilience and made a call for a global response from both businesses and governments for 2 reasons. Firstly, to avoid a catastrophic failure threatened by an 'all or nothing' approach to cyber risks (e.g. preventing network penetration as the only plan). Secondly, because it argued the conversation needed to go beyond technology or data security.

Whereas cybersecurity can often be viewed as binary – i.e. you are either secure or you aren't - cyber resilience is not binary. Cyber resilience requires a more strategic, longer-term approach. It's really about risk management, and there isn't a single point at which it begins or ends (cyber resilience can always improve, or degrade, if neglected).

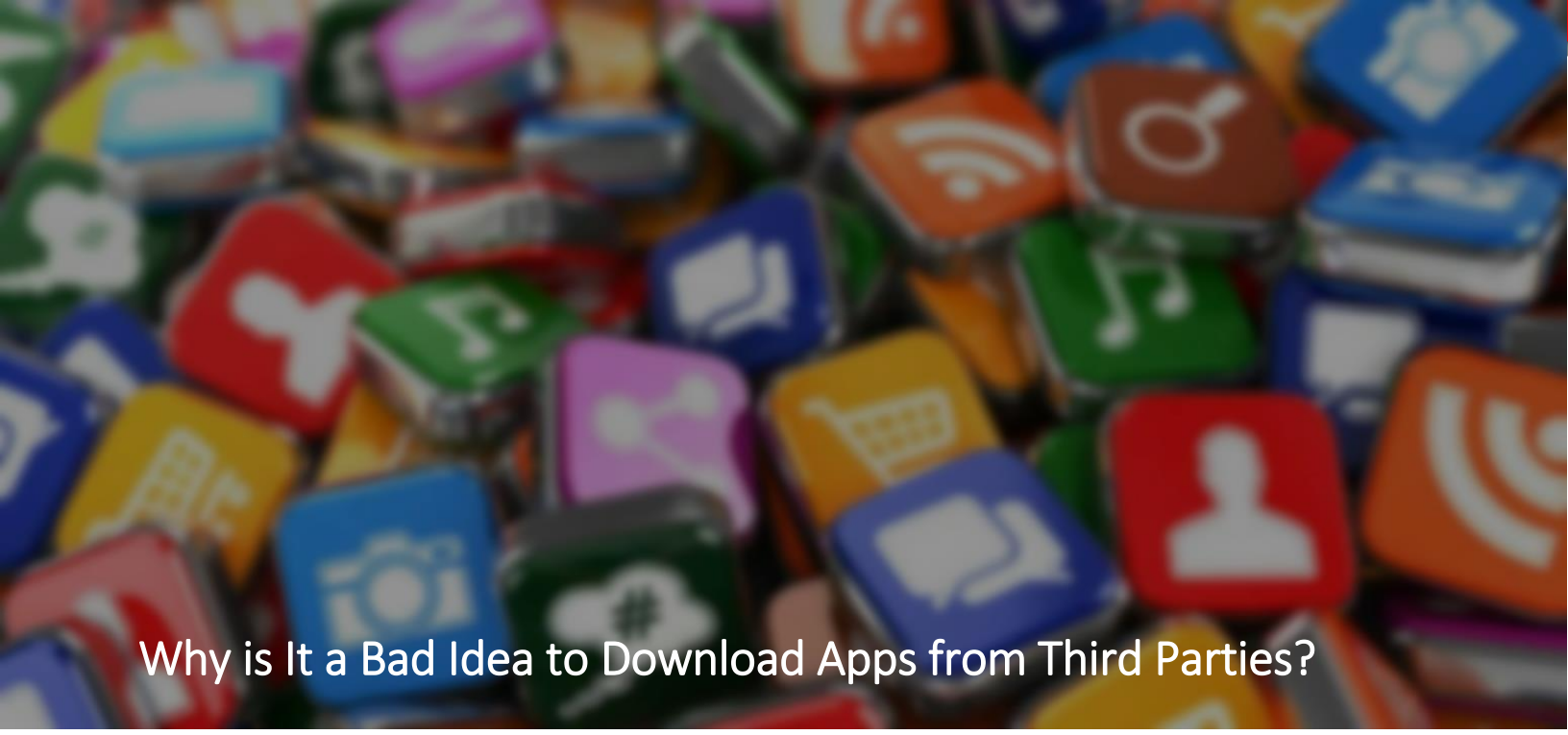
Instead, cyber resilience comes from building strategy and working to ensure that the risk-transfer mechanisms that work for more traditional threats are also brought to bear on new cyber threats. To assist in these goals requires a concerted effort to help develop the skills required to build cyber resilience into everything which an organization does. Certification is part of that.

In 2015, AXELOS, a joint venture company, partly owned by the UK government announced it was launching a cyber resilience certification scheme called RESILIA®. RESILIA® helps professionals understand how decisions impact on cyber resilience and how to make good cyber resilience an efficient part of business and operational management.

So, whilst the threats of a devastating cyberattack on industrial systems grow daily, the real battle lies not at the frontline of cybersecurity defense but in the rear guard of cyber resilience. Leading cyber resilience strategy over the longer term is crucial if calamitous cyberattacks on industrial systems is not to cause widespread social disruption in the future. Cyber resilience experts therefore are the foot soldiers of the battles ahead.

About The Author

Simon Buehring graduated with an MSc in Information Technology in 1988 from Kingston Polytechnic in the UK. He then worked in the software industry as a developer, team leader, project manager, consultant and technical director until founding Knowledge Train in 2005. Knowledge Train provides a mixture of classroom and online courses leading to professional certification in many areas including cyber resilience training.Simon can be reached online at https://www.linkedin.com/in/simonbuehring/ and at our company website http://www.knowledgetrain.co.uk



Why is It a Bad Idea to Download Apps from Third Parties?

We live in a world where the masses rely on apps for various activities. Need to send an email? You use a Gmail or outlook app. Want to talk to your friends? AIRG™ is the answer. Need to pass the time? Pokémon Go and Candy Crush it is.

Apps surround us all. In 2017 alone, 178.1 billion apps were downloaded by consumers. This staggering number is projected to increase to a total of 258.2 billion by 2022! Now, that is a lot of downloads. Most people read reviews about the given applications before downloading them. For instance, you are likely to read AirG reviews online before downloading its products.

However, rarely do people give much thought to how we download the applications. Sometimes we don't even consider researching about the company whose apps we are downloading. Think about it. How often do you question the legitimacy of the third parties whose applications you use?

Remember the good old Pokémon Go craze ? Everyone wanted to jump onto the bandwagon even before the game was available in their countries. How did they do it? They downloaded the application through third parties. You might not think much of this action. But, the truth is that it is a very bad idea to download apps from third parties.

Why Would You Be Tempted to Use Third Party Stores?

Before we discuss why it is a bad idea, it is important to understand the charm of using third parties for app download. Here are some reasons why you might want to use a third party store.

- Google Play and Apple store don't have the app you want
- Third parties are delivering lucrative promotions
- You want a premium app for free

These might seem like good enough reasons to switch from official stores. But, the risk involved makes it a bad idea!

Why Must You Avoid It?

It is true that third parties seem like attractive options a lot of the time. But, the dangers attached to these providers are too significant to be ignored. The biggest reason for avoiding third parties is the risk of downloading malware.

The last thing you would want to do is infect your device with viruses. Not only does it harm your device, but it can also lead to massive data breaches. There was a study conducted by Trend Micro to gauge the security of the apps delivered by third-party providers. It was found that over 1150 applications had viruses in them. All of these applications were concentrated in four third-party apps, namely Mobogenie, 9apps, Aptoide, and Mobile9. Anyone who uses third-party stores is likely to recognize these names since they are quite popular.

The Cautionary Tale of Pokémon Go

As mentioned above, the Pokémon Go craze led to a lot of security threats. PointProof, a security firm, alerted the masses about one such threat. A third-party app called Drojack was unknowingly being downloaded along with Pokémon Go app.

Drojack is an app that connects a given device to an unauthorized network and downloads apps from it. This leads to a threat of financial information being stolen from your phone. While the app may or may not do so itself, it can certainly open doors for other malicious software to enter your device.

This is a threat that was only viable for those who downloaded the game from apk and third-party apps.

Why are Official Stores Safe?

When you think about it, shouldn't the risk of malware be present in all app stores? Isn't there an inherent possibility that Google Play also has applications infected with viruses?

Well, statistically it is possible. In no way is the technology used by official stores like Google Play and Apple Store perfect and 100% secure. Sometimes bad apps do find a way in. However, the probability of finding a bad app on official stores is less than the chances of finding one in third-party providers.

Why?

This is because official stores take a lot of time to filter out the bad apps. This is why you will find a comparatively restricted number of applications in official stores. The rest have been deemed unsafe for download.

Understanding the Difference Between Official App Stores and Third Parties

To truly understand why third parties are not safe to use, you must understand how official stores work. This helps in detecting what exactly third parties fall short of.

Official stores tend to have both native and third-party applications. Native applications refer to those that are built by the provider, (e.g., Apple or Google) for the given operating systems (iOS or Android). Third-party applications are those developed by other companies.

Now, both third party stores and official stores deliver third-party apps. The difference lies in the stringent security checking of these apps. Official stores do it. Third parties don't. And this makes all the difference.

Should All Third-Party Apps Be Avoided?

At the end of the day, you can never be too sure about a third party app. After all, if a third party store can have malware, so can other applications, right?

While there is always a risk, it is minimized by using official stores. So, while you should avoid third-party stores like the plague, the same may not be true for all app from third parties.

Yes, you must exercise caution when downloading third-party apps. Especially those that are from developers that you have never heard of. Read reviews and research about the application before

deciding to download it. Any application that demands access to more information than you are comfortable in sharing is a no-go.

Conclusion

If you were to ask us, we would tell you it is best to avoid third-party stores and apps when in doubt. It is better to be safe than sorry. Make sure you at least take measures to research about the app in question. For instance, read up AirG reviews before downloading its applications!

About The Author

Michelle Joe is a blogger by choice.

She loves to discover the world around her. She likes to share her discoveries, experiences, and express herself through her blogs. You can find her

on twitter: @michellejoe524

Two Decades Later, SIEM Technology Finally Delivers on Its Original Promise

By Avi Chesla, founder and CEO of empow

When SIEM technology came to market nearly two decades ago, IT and security professionals had grand visions of how it would help them consolidate the plethora of data generated by their various security tools, analyze and correlate it to identify security incidents, and then prioritize response. Fast forward 20 years, and the unfortunate reality is that SIEMs – both traditional *and* next-gen – have yet to deliver on the technology's original promise. What went wrong? Simple – the threat landscape changed rapidly and dramatically, but SIEM technology failed to adapt.

Over the years, SIEMs have remained laser-focused on identifying security incidents using human-written, static device log parsers and correlation rules – in other words, rules that require human security experts to be involved in rule development, deployment and management. While this approach worked just fine in the simpler days of security – where IT infrastructures were much more streamlined and a concrete perimeter existed separating a company's assets from the outside world – it quickly became obsolete with the advent of internet computing and follow-on trends like mobility, cloud and, now, internet of things (IoT). Another major shift impacting cyber security is the creation of platforms that can generate new types of attack tools and malware code – what the market calls "machine-generated attacks."

These trends obliterated the perimeter, and, those that made the development of new malware types easy, dramatically decreased barriers to entry for cyber-criminals. Internet malfeasance once required a high degree of technical proficiency, but now anyone with an internet connection and a credit card to purchase exploits-as-a-service can join the global ranks of cyber-criminals. And, as mentioned, those infamous, artisan basement hackers from the 1990s have evolved into automated, machine-generated attacks, increasing attack velocity and effectively making every threat "brand new."

Enterprises responded to this shifting threat landscape by procuring more and more technology, which has created incredibly complex and largely unmanageable security infrastructures that generate overwhelming cascades of data and security alerts. This has created an oppressive Big Data problem that SIEMs simply were never designed to address. Instead, enterprises kept writing more and more log parsers and correlation rules (think hundreds of thousands in the case of large enterprises – what we call the "Big Rules" problem), many of which are obsolete, conflicting or simply ineffective in classifying new attacks, since human-written rules are only effective against known attacks.

As a result, rather than becoming security's silver bullet, the "Big Rules" problem has actually rendered SIEM technology relatively impotent for the following reasons:

- **It's too reactive** – Human-written rules can only be developed against *known* threats and patterns. In other words, SIEMs can only detect attacks after the fact, causing them to miss new or unknown attack sequences.
- **Too passive** – SIEMs are designed for alerting, not responding. They lack the machine-based incident response capabilities that can automatically contain or remediate threats in real time.
- **Too complex** – Organizations are burdened with thousands of security correlation rules that consume inordinate numbers of man-hours and are simply impossible to maintain manually.
- **Too expensive** – SIEMs require massive ongoing investment in services, technology and personnel to cope with the "Big Rules" problem, which results in a very high total cost of ownership.

Is there a way out of this mess? Will SIEM technology ever be able to deliver on its promise to make life easier for security professionals? The answers to these questions are yes and yes, and the key to both is focusing on attack intent.

New Opportunity for SIEM Technology: Deciphering Attack Intent

There is perhaps no better defense against today's sophisticated cyber-criminals than first understanding the intent behind their attack methods, and this presents a significant opportunity for SIEM technology to finally right the ship that has been taking on water for years.

For many organizations, intent classification has remained an impossible task for several reasons:

- The "Big Rules" problem has kept security teams mired in mundane, tactical work (i.e., writing and maintaining log parsers and correlation rules), leaving no time to focus on higher priority tasks, such as deciphering attack intent.
- Because of complex infrastructures and resulting Big Data, organizations do not have the resources to decipher the intent of all the different events, clues and signals generated by endless point tools.
- When security analysts do have time for intent classification, they must analyze suspicious files or behavior manually – a painstaking process that simply cannot keep pace with the rapid volume and variety of machine-generated attacks.

The good news is that we are seeing new approaches to intent classification automation that arm SIEM vendors with the features and functionality needed to automate detection, investigation, remediation and mitigation of both known and unknown threats, without rules or manual processes. Three notable areas of advancement include:

- **Artificial Intelligence (AI) and natural language processing (NLP)** – One of the truest forms of AI, NLP algorithms automatically collect, read and understand threat data, regardless of the source (logs, intelligence feeds, research articles, etc.). Once the meaning of the terms used to describe security-related threats, research results, relevant vulnerabilities, attack vectors etc., is known, their appearances in new sentences will be understood without human involvement.

This ability to automatically "operationalize" human-readable threat intelligence enables SIEM systems to classify logs and data feeds by security intent (separating benign activity from activity demonstrating malicious intent). NLP algorithms read logs and data feeds, seek out relevant information from logs and third-party data sources, and identify attack intent orders of magnitude faster and far more effectively than is possible with traditional manual approaches by analysts.

- **Cause-and-effect analytics** – A complementary approach to operationalizing threat intelligence, cause-and-effect analytics enable SIEMs to automatically validate and prioritize real threats, and reveal the complete "attack story."

- **Orchestrated response** – Finally, with NLP and cause-and-effect analytics, threat investigation, mitigation and remediation can be optimized and automated based on attack intent, and SIEM technology can marshal the most relevant response procedures and execute them using the right security tools.

When SIEM technology 1) uses AI and NLP classifiers to autonomously understand the intent behind each piece of data that the existing network infrastructure generates, 2) uses cause-and-effect analytics to identify if these pieces form a real attack "story" against the organization, and 3) executes adaptive investigation and response actions that are optimally synched to each threat, the "Big Rules" problem can be solved. And, as a direct result, the other challenges associated with traditional SIEM systems are also overcome.

It has taken decades, but AI and its related technologies have finally enabled SIEM to realize its original promise. The reactive, passive, complex and expensive SIEM can be replaced by a proactive system that detects, confirms and stops attacks before they cause harm, while simultaneously enabling organizations to maximize the value of existing security infrastructure and eliminate the need for extensive human intervention. Strengthening yet simplifying security in this way may have been the intent of the original SIEM, but now we have the blueprint to execute on it successfully.

About the Author

Avi Chesla, founder and CEO of empow
Avi is a recognized leader in the internet security arena internationally, with expertise in product strategy, cyber security, network behavioral analysis, expert systems and Software-Defined Networking. Prior to empow, Avi was CTO and VP of security products at Radware, where he was responsible for defining, leading and executing the company's strategic technology roadmap and vision, including the foundation and management of Radware's Security Division, a provider of cyber-attack mitigation solutions. Avi's views on industry trends and best practices have been featured in articles and white papers, and on the conference speaking circuit. He has earned more than 25 patents in the arena of cyber security solutions.Avi can be reached online at @cheslaavi and https://www.linkedin.com/in/avi-chesla-0637761/ or via the empow website: https://www.empowcybersecurity.com/.

Do I Need to Be GDPR Compliant

By Jason Wang, CEO of TrueVault

GDPR is a new law regulating the processing (collection and use) of individuals' personal data, which came into effect on May 25, 2018.

If you are covered by GDPR, then not only will your customers expect you to be compliant, but your business partners may require it as a condition of their contracts. Moreover, the fines for breaching the Regulation are harsh, going up to €20,000,000 or 4% of your global turnover (whichever is higher).

With that in mind, it is important to know whether you are within its scope.

Data Controllers and Data Processors

To start with, GDPR applies to people and organizations which act as data controllers and data processors:

Data controllers **decide the purposes and methods of processing personal data – they coordinate processing.**

Data processors **are responsible for directly processing personal data based on the instructions of data controllers. This could include subcontractors, for example.**

GDPR will cover any organization which keeps a customer or membership list, or information about its employees. Therefore the vast majority of organizations will be affected, as long as they have dealings with the European Union.

Dealings with the European Union

GDPR was created by the European Union to protect its citizens, and so it only affects organizations with some kind of relationship with the EU or its people. That said, it does not only apply to companies based

in an EU country. According to Article 3, you will be affected if you are a data controller or data processor and any of the following apply:

you are established in the EU (or somewhere else subject to EU law), or

you offer goods or services to data subjects in the EU, or

you monitor the behavior of data subjects in the EU.

Establishment in the European Union

If you are established in the EU, then all processing related to that establishment is covered, even if it takes place elsewhere.

Being established is a broad concept in EU law. It could apply to you if you have (for example) a branch, representative, address or bank account in an EU country. For more context, see the recent Weltimmo case in the European Court of Justice — particularly paragraphs 29 to 33 - regarding the outgoing Data Protection Directive.

Goods and Services

If you control or process data relating to people in the EU, in the context of offering them goods and services, then this will be covered by GDPR. This is true even if the goods and services are free.

Note the word offering: it appears that this will only apply where there is some element of targeting your goods at EU countries. Targeting is likely to include providing a version of your website in a local language (which is not your own country's language), allowing purchases in the local currency, or mentioning EU customers or countries on the website. It is possible that merely delivering to EU countries will be enough to count.

Note that the key question is whether your customers (or members, or employees) are in the EU, not whether they are EU citizens. You don't for example need to worry about the nationality of customers based in the U.S.

Monitoring Behavior

If you control or process data relating to people in the EU, in the context of monitoring their behavior, then this will be covered by GDPR.

A lot of monitoring is done in tandem with the offering and sale of goods and services (see above), such as online vendors using patterns in consumer purchases to offer similar products, or games developers collecting data on player activity. However, monitoring also covers a wider range of activities, including market research and getting feedback. The vast majority of online organizations (commercial or non-commercial) monitor the behavior of visitors to their websites to some extent.

As with the offering of goods and services, there needs to be a certain degree of targeting at people in EU countries. For example, if you merely collect web traffic data without targeting individuals in the EU, this is unlikely to be covered.

What Does This Mean for American Companies?

This all means that GDPR will affect a lot of American companies, whether or not they have any specific presence in the EU.

If you are not established in the EU, but a small proportion of your revenue comes from people in those countries, then you are faced with a choice. You could choose to stop providing (or at least marketing) your goods and services to these people in order to avoid taking the steps necessary for compliance.

But remember that most of GDPR's rules are good practice in any event. Adhering to them shows to your customers that you take data security seriously, and it puts you in a good position if state or federal government ever decide to enact similar legislation at home. This is very likely, and will be happening for companies under the scope of the California Consumer Protection Act (CCPA) by 2020.

Cutting yourself off from European markets could ultimately limit your future growth. By contrast, working to make your organization and its products GDPR compliant, whether on your own or with help, is an investment which is likely to pay off in the long run. TrueVault, for instance, offers products that makes your applications and data warehouses GDPR compliant.

Some (Limited) Exemptions

There are very limited categories of processing exempted from GDPR:

Processing related to activities which are outside of EU law.

Processing related to law enforcement and immigration control.

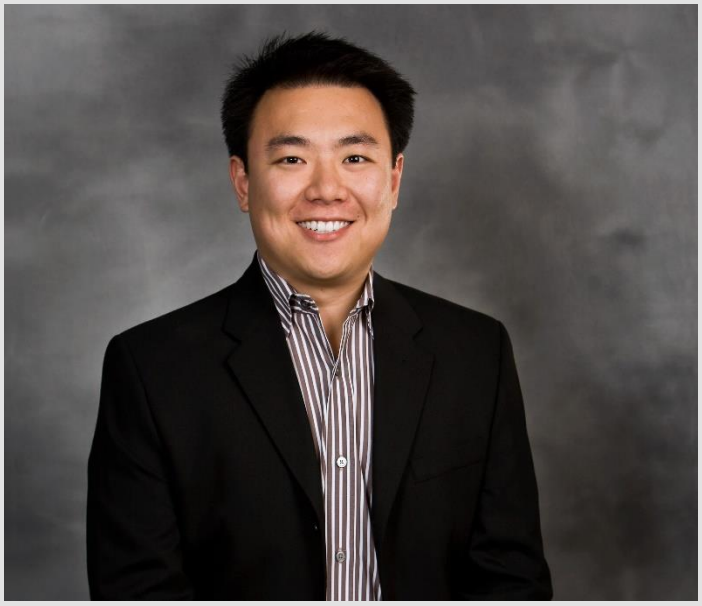
Processing by individuals carrying out purely personal or household activities (such as keeping an address book).

As can be seen, none of these will apply to the vast majority of organizations.

GDPR will apply across the business world, wherever organizations have an EU presence or deal with the personal data of people in the EU. The sanctions for breach will potentially be harsh.

As a result, it is vital to check whether your organization is covered by the new rules, and if so to take all steps necessary to make it compliant.

About the Author



As the Founder and CEO of TrueVault, Jason has puzzled over a solution to two seemingly opposing forces in technology today: personalization and security. Personal data helps businesses shape customer experience, but security risks mount as more sensitive data is collected. TrueVault tackles this problem by helping companies protect, manage, and de-risk customer data such that any company can provide a personalized experience while reducing risk and boosting data security.

Prior to TrueVault, Jason was employee No. 1 and VP of Technology at ScoreBig. He built ScoreBig.com from the ground up and was a part of the team that raised more than $30 million from Bain Capital Ventures and U.S. Venture Partners. He was also a Technology Director at Razorfish/Microsoft. He holds a BS from the University of California, Irvine, in information and computer science.

First Name can be reached online at jason@truevault.com and at our company website https://www.truevault.com/

Top 10 Tricks to Avoid Malware

Tricks to help you avoid malware and keep your computer running smoothly

by Howard Dawson, Writer, Strictly Digital

Your computer is slower than it used to be or crashes repeatedly. Unwanted pop-ups appear and you can't get rid of them. Your computer keeps restarting before Windows can load. Or maybe a ransom message appears on your screen, demanding payment to un-encrypt your files. What's going on?

These are all symptoms of malware. Viruses, worms, trojans, keyloggers, spyware, and ransomware are all examples of different types of malware. With millions of malware (malicious software) programs in existence and new ones popping up every few seconds, protecting your PC or mobile device can be a challenge. Here are ten tricks to help you avoid malware and keep your computer or phone running smoothly.

First, Beef Up Your Security

There are several ways to use software to stop malware from infecting your computer. By blocking potential threats and being vigilant about updates, you can significantly cut down on malware threats.

1. **Install anti-malware software.** The first and most obvious tip for avoiding malware is to install a good anti-malware program, keep it updated, and run scans frequently. This step is essential to a good defense against viruses and other malware programs.

2. **Use a firewall.** A firewall prevents hackers or other unauthorized users from accessing your computer network. Without a firewall, all of the files and personal data on your computer are at risk. Both Windows and Mac computers come with a firewall installed, but the firewall on the Mac is off by default. You'll need to enable it in the system settings.

3. **Use a VPN.** A virtual private network (VPN) encrypts your data as it is transmitted between your computer and the Internet. If a hacker intercepts your data, they won't have the key to unlock the encryption, so they won't be able to read the data. For extra protection, choose a VPN which includes malware protection and ad blocking as part of the service.

4. **Don't use public wifi.** Just because you can connect to the free wifi while you're eating your bacon, egg and cheese bagel at McDonald's or grabbing a latte at Starbucks doesn't mean you should. If you can connect to the network easily, so can a hacker, and as long as you are connected, your data and your device are at risk. If you must public wifi from time to time, try to use a device that contains as little important information as possible. And don't log into your bank or other sensitive websites using public networks.

5. **Keep your software updated.** Your operating system and other software programs need to be kept up to date. Many of the updates are security patches that are needed to close up known vulnerabilities in the software. As new exploits are discovered that target weaknesses in software programs, manufacturers work to create fixes to keep their software safe. If you don't keep your software updated, you run the risk of becoming a victim of a hacker who may use an exploit to take control of your computer.

Common-sense Tips for Avoiding Malware

Sometimes avoiding malware is as simple as stopping to think before you click a link or download a file. You need to be aware of the most common risks and avoid them.

6. **Be alert to e-mail risks.** Worms are often transmitted through e-mail attachments. Never open an attachment you weren't expecting, even if you trust the sender. Some malicious programs send messages to an infected person's contacts to spread the infection. Phishing scams are also commonly spread through e-mail. Scammers try to copy the e-mail style of a trusted business, such as your bank, in order to trick you into clicking on a link in the e-mail and entering your username and password to log into the site. If you aren't paying attention, you might not notice that the sender's e-mail address and the destination website are wrong. Scammers use this technique to capture your login details so they can access your banking or another online account.

7. **Don't download shady software.** Pirated software downloads are prime sources of malware. Other popular targets include video players and fake anti-virus programs. Never install an anti-virus or anti-malware program from a popup ad. These ads often contain warnings that your computer has been infected in order to scare you into downloading the software. Don't fall for it.

8. **Beware of physical media.** CDs, DVDs, thumb drives, and other media that contain computer files all have the potential of carrying viruses and other malware. Even if you got the disk from your best friend, you need to be careful. You never know if your friend's computer is infected. Scan the files before opening them, or you might end up with more than you bargained for.

9. **Use strong passwords.** Keep your accounts safe by using strong passwords that contain an assortment of capital and lowercase letters, numbers, and symbols. And never use the same password twice. If one site is hacked, the hacker will often sell the usernames and passwords to other hackers and if you use the same login everywhere, all of your accounts will be at risk. Use a password manager such as LastPass to keep track of your passwords so you don't have to remember them all.

10. **Don’t fall for cold-calling scams.** Some scammers will call you on the phone and pretend to be from a reputable tech company such as Microsoft and tell you that you have a virus on your computer. Microsoft does not make these calls. Do not give the caller any information. Just hang up. If you have a mobile phone, consider installing a call blocker app to keep unwanted calls from getting through.

Bonus Tips: Prepare for the Worst

Take steps to ensure that you’ll be able to recover from a malware attack.

11. **Store your OS disks where you can find them.** If you ever need to reinstall your operating system and other important software, you don't want to have to go rummaging through boxes of junk in your closet to find the disks. Keep them near your computer and make sure you always know where they are.

12. **Back up your files.** While backing up your files won’t help you avoid malware, it will help you avoid the damage that malware causes, which is just as important. All of your important data should be backed up either on an external hard drive or on a service such as Dropbox that stores your files on another computer, or both. Having backups in place will ensure that if you get some sort of malware and are unable to remove it without wiping the hard drive and reinstalling everything from scratch, you’ll still have your data.

Malware programs can be extremely difficult to remove from your system, but if you follow the steps outlined above, you have a good chance of avoiding them completely. Keep your computer’s software updated and use common sense to avoid obvious risks. Don’t rely on an anti-malware program alone to protect you. Use a combination of strategies to create layers of protection in order to increase your chances of catching any threats that come your way.

About the Author

Howard Dawson is a technology writer for Strictly Digital, specializing in privacy and security online. As an IT graduate and a writer, he enjoys exploring new topics that are relevant in today’s tech world. You can reach him by writing an email to howard@strictly.digital or by visiting website https://strictly.digital

Cybersecurity in The Era of Agile Software Development – Part 2 - (Devops & Devsecops)

By Ivan De Los Santos

As technology continues to be incorporated into more products and services, the race to deliver customer value fast is changing the software development landscape. In part 1 of this series (Oct edition), we discussed how agile software development is changing the organizational structure of software delivery teams and entire organizations. Agile methodologies allow organizations to respond rapidly to change; however, this is not enough. More is needed in order to deliver software quickly and with less error. Welcome to DevOps!

"DevOps is a combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity; evolving a product at a faster pace than organizations using traditional software development and infrastructure management processes" Amazon Web Services

DevOps applies software engineering principles to infrastructure and operations. Fast software delivery through automation is at the core of DevOps. Development and Operations become one team or work side-by-side, thus helping to reduce the friction points that have plagued them for years. This is the case where development teams would develop software and "throw it over the wall" to operations. It was up to operations to make it work. Moreover, operations were never capable to provide development teams with production like development environments. These issues were at the core of poor software delivery practices.

This new way of crafting software improves delivery by using automation and removing human interactions as much as possible. Platforms and tools like Jenkins, Docker, Vagrant, Puppet, Chef, Platform as a service (PaaS), ServiceNow, Bitbucket, Git, Selenium, and many others have enabled development teams to create a continuous integration and continuous delivery pipeline (CI/CD). The use of these tools have allowed some organizations to delivery software multiple times per day. Public cloud providers like Amazon provide their own CI/CD pipelines to their customers.

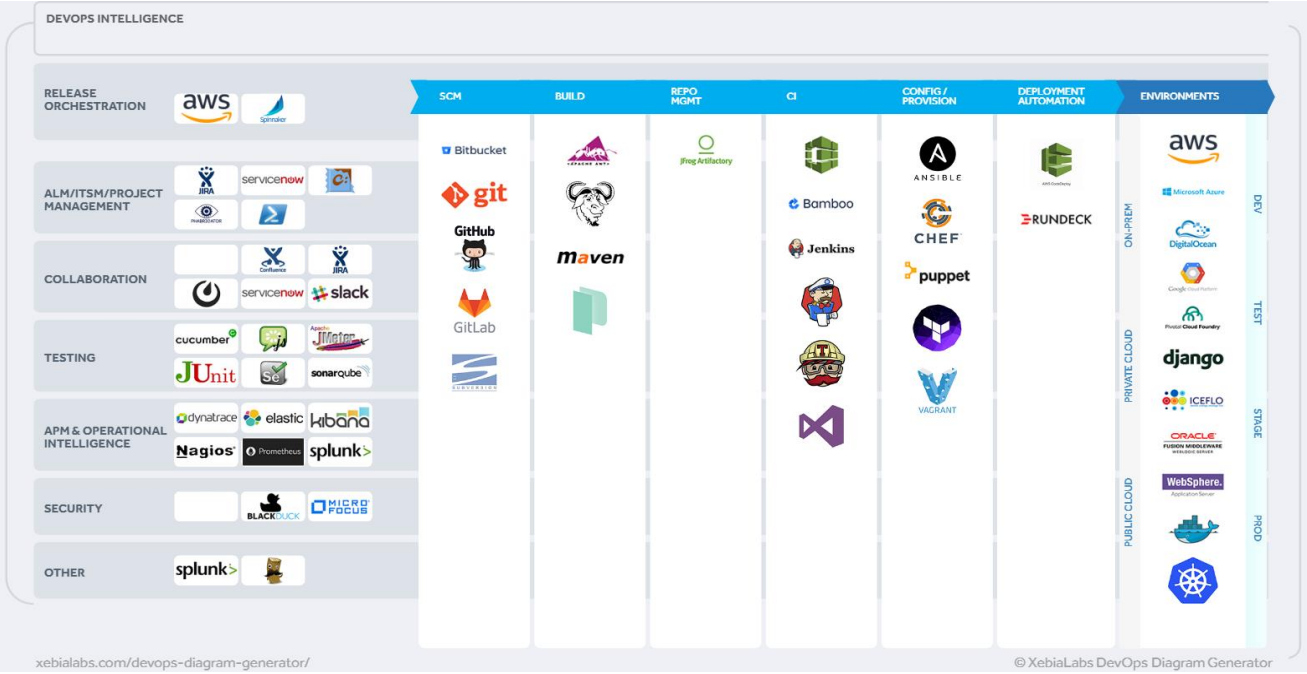


Figure 1: Example of a DevOps CI/CD pipeline

Cyber Defenders must become very familiar with the tools and applications used in a CI/CD pipeline. A compromise of one or more of these tools could adversely impact an organization's ability to deliver software. Furthermore, these applications become a new attack vector for threat actors. Vulnerabilities found in these applications should be remediated immediately.

Many of the tools being used in creating a CI/CD pipeline are open source. Although more eyes are looking at the code for potential vulnerabilities, there are those that are also looking for ways to comprise these applications.

Cybersecurity professionals, especially those involved in defense operations, might be wondering how organizations are able to deploy code that is secure multiple times per day. How does one conduct penetration testing on an application that is constantly changing and using temporary infrastructure? For example, Jenkins, a very popular continuous integration tool, has over 260 CVEs identified.

Application security tools are being leveraged. After each commit, the code is automatically scanned and tested for vulnerabilities. Moreover, an analysis of open source components also takes place. Although this is a very good thing, security professionals are not yet part of this equation.

Security professionals are starting to raise the alarm on the DevOps movement. Fast delivery should also include security. Welcome to DevSecOps!

DevSecOps

The DevSecOps Manifesto

"**Leaning in** over always saying "No"

Data & Security Science over fear, uncertainty, and doubt

Open contributions & collaboration over security-only requirements

Consumable security services and APIs over mandated security controls & paperwork

Business driven security scores over rubber stamp security

Red & Blue team exploit testing over relaying on scans & theoretical vulnerabilities

24x7 proactive security monitoring over reacting after being informed of an incident

Shared threat intelligence over keeping info to ourselves

Compliance operations over clipboards & checklists"

DevSecOps.org

What Does This Means?

Leaning in:

Security professionals, especially cyber defenders, should lean in and build relationships with development teams. Explain the why of a situation and how it can be addressed rather than just saying no.

Data & security science:

Similar to how businesses operate, our decisions should be based on data and analytics. We must have metrics, KPIs, and models that inform our decisions, the actions we take, and the advice we provide.

Open contributions & collaborations:

Cyber defenders should be part of development teams and collaborate daily with developers. In the end, we all have the same goal: to deliver software features fast that are secure. In organizations where development teams are working using Scrum, security professionals should be active participants in sprint planning, backlog refinement, and sprint retrospective.

Consumable security services and APIs:

We should embrace automation and APIs as much as possible. Security should be self-served and part of the process. Developers should be able to scan their code and address common vulnerabilities (OWASP top 10) on their own. Furthermore, cyber defenders should empower developers by embracing security as code and providing developers with libraries, SDKs, and code snippets that include security in it.

Business driven security scores:

Security metrics must be tightly coupled with business objectives. The main objective of security is to enable the business to operate fast and securely. Security professionals should ensure that security priorities are closely aligned with business priorities.

Red & blue team exploit testing:

Cyber defenders should constantly find, test, and exploit vulnerabilities instead of relying on scanning results that might or might not be accurate. Reducing false positives would greatly increase our credibility and help us shape software development practices.

24x7 proactive security monitoring:

Threat actors do not sleep and are constantly testing our networks and applications for ways in. We must partner with development and operations to make sure that we are monitoring the right things. Site Reliability Engineering (SRE) practices and techniques should be adopted by security teams.

Shared threat intelligence:

We need to start sharing threat intelligence with our development and operations team. One of the best ways to do this is through threat modeling. Conducting threat modeling sections with development and operations teams is one of the easiest and more effective ways we can engage them and build a working relationship.

Compliance operations:

Security is more than just meeting compliance; nevertheless, compliance is very important. We need to leverage automation to help us arrive at a point where compliance is self-served and part of the continuous integration and continuous delivery pipeline. Auditors and government regulators should not be asking for evidence but instead be granted access to a system where this information is automatically generated. Moreover, we must be able to test for compliance at all times.

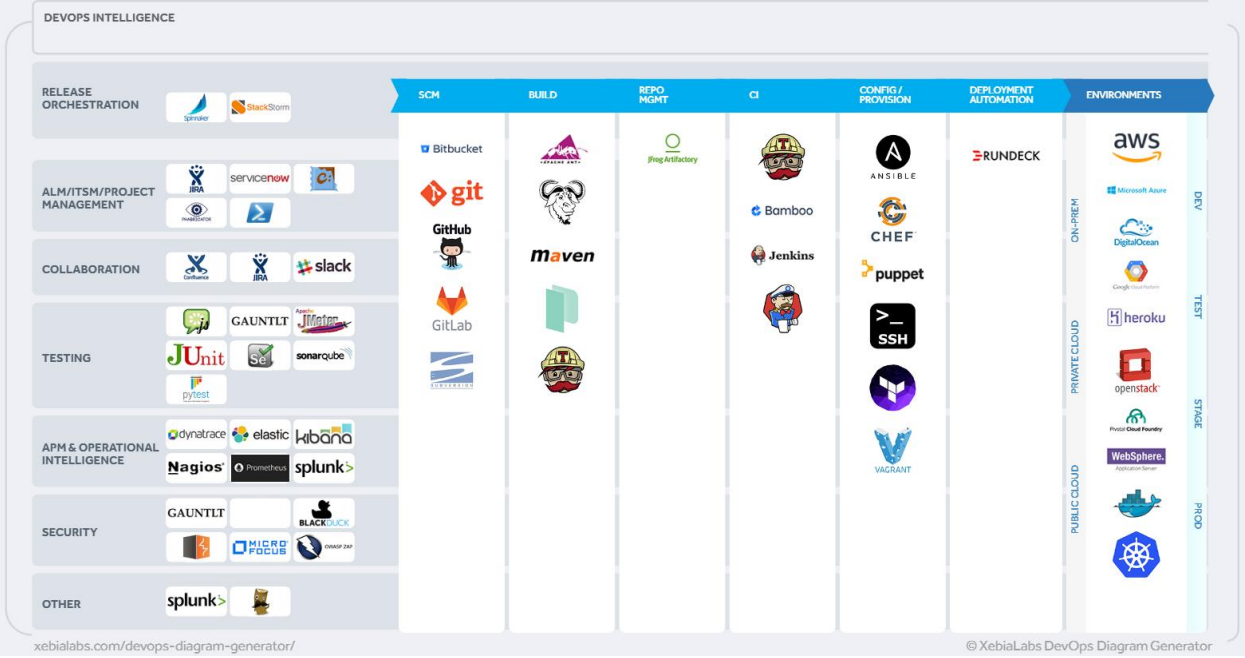


Figure 2: Example of a DevSecOps CI/CD Pipeline

When providing on-demand security capabilities, our services must be stable, accurate, and capable of meeting the demand. We only get one opportunity to get it right; if our services are not reliable, developers will lose confidence in our systems and in us. This will adversely impact our ability to influence software delivery practices.

We can use a variety of tools and techniques to help development teams incorporate security into their processes including:

- Being present and practicing active listening
- Conduct threat modeling sections & secure design reviews
- Help developers create attacker's user stories
- Provide development teams with secure libraries, SDKs, and scripts
- Establish on-demand vulnerability and code quality scanning capabilities
- Automate penetration testing as much as possible
- Bug bounties
- Automate compliance (compliance as code)

In summary, security is everyone's responsibility. DevSecOps principles and processes give us the highest opportunity to enable developers to deliver secure software and services to our customers.

References

Amazon Web Services . (2018, 10 22). What is DevOps. Retrieved from What is DevOps: https://aws.amazon.com/devops/what-is-devops/

DevSecOps. (2012-2015). DevSecOps Manifesto. Retrieved from DevSecOps: http://www.devsecops.org/

About the Author

Ivan De Los Santos is a Professional Scrum Master (PSM I) & Product Owner (PSPO I). He is also a cybersecurity professional with over eight years of experience. Ivan holds the CISSP, CCSP, CISA, CEH and CNDA, and several other IT-related certifications. He earned a B.S. in Business and MIS and a M.S. in Cybersecurity. Ivan teaches undergraduate level courses in relational database modeling and database security. He has worked in the defense and financial services sector. Prior to working in the IT field, Ivan served in the U.S. Active Army and Air Force Reserves. He can be reached at https://www.linkedin.com/in/idelossantos/

Why is Cybercrime a Big Threat In IoT Era?

by Zehra Ali, Editor, PrivacySniffs

The Internet of Things (IoT) seems to be the main purpose and aim of every scientist in one or the other way. The IoT is intended to produce a physical and digital network of everyday devices, like smartphones or sedans which are in continuous communication.

IoT produces a world where smartphones control the entire lives. The smartphones will be used in a way to control every aspect of our houses in fact on every floor. The lighting can be altered and improved, AC can be rebuff, and also the TV can be operated and regulated by the smartphones too.

The constant communication causes in Internet-enabled devices cooperating and revealing what is going wrong and how it can be improved. This is an amazing and phenomenal resource for data gathering and understanding, and it would also enable businesses to chase and stalk their devices in actual time and supervise their working efficiency.

Blooming IoT Trend

The Internet of Things (IoT) is expanding at a quite faster rate. In 2015, the total recorded devices were 15.4 billion which is estimated to rise to 30.7 billion in 2020 and 75.4 billion in 2025 with an economic impact of up to USD 11 trillion.

Normally the growth in this field lies in manufacturing, warehouse, retail applications, inventory, logistics, and resource management.

The IoT technology will have vast impacts on society in various aspects. The constant growth, development, and adoption of the IoT related devices will result in an increasingly interrelated environment. However, this growth and development will certainly produce new chances for cybercrime, attracting orthodox and state-sponsored threats.

The IoT can become one of the biggest technological revolts in recent ages, which will enable businesses to operate efficiently, quicker, and more profitably. But for IoT to collect adoption and achieve its promise, one of the most serious issues needs to be a deal is protecting IoT and all other IoT related components which make up the Internet of Things.

The IoT devices hugely depend on the third-party components, where security reserves are very restricted, combined security measures or criteria does not exist, and an authorized framework for accountability is lacking.

Inappropriately, the traditional security solutions like antivirus programs or software are likely to fail in protecting the IoT surface. Due to the great diversity of available platforms, a collection of possible interactions, along with poor security systems by the device's sellers, securing IoT devices is a great challenge.

Major IoT Related Attacks

IoT has opened up almost in every element of the user's life to the internet. The internet instead of being controlled through a stationary machine will be now observing and watching every part of the user's life. But this type of access to the internet imposes serious concerns towards the user's personal and digital security. Having various access points increases the risk of hacking and data infringement.

For instance, if your smartphone is hacked so in IoT world it means that the hacker cancontrol your entire home and can easily invade into things which they shouldn't.

Cybersecurity is very important in the IoT era. The cybercriminals are now getting more and more experienced and malevolent. The way in which these criminals gain access to data is countless which has increased the threat of cybercrimes in the IoT era.

However, there are other ways too by which the IoT attackers and hackers gain access to data other personal information.

1. Botnets:

The Botnet attacks are also known as ''Thingbot Attacks''. A botnet is a link of systems which targets networks of connected computers and other smart devices with the intention of infecting them, taking control over them and distributing malware. The cybercriminal is capable of grasping control of the entire network without the user becoming aware of it.

Botnets can cause various damaging effects to the business networks together with the distribution of data, sending inappropriate spam messages, data, and identity theft. Because of botnets, the IoT networks are at great risk because botnets can easily access and control not only laptops and computers but also every device which is connected to the network, creating endless chances to for cybercrimes.

2. Man-In-The-Middle Concept:

The man-in-the-middle concept happens when the cybercriminals hack an entire network with the goal of interrupting communications among two systems. These concepts give hackers and attackers the chance to fool users who might think they are having communication.

In other words, it means that the hacker will secretly capture and spreads messages to other parties while they assume that they are communicating directly with each other.

These kinds of attacks are extremely unsafe and serious in the IoT era because of the nature of things being hacked or stolen. For instance, these devices can be anything from being industrial tools, machinery, vehicles to harmless connected things like smart TVs.

3. Data and Identity Theft:

The data and identity theft of useful data is another leading cybercrime in the IoT era. This can be of business data. However, hackers or attackers seek to steal the identity details of an individual for financial fraud and within IoT, and it is even easier.

The extreme data theft or hacker attacks like DNS hijacking could become more destructive with IoT as the access to one device could be a key to enter numerous connected devices.

4. Social Engineering:

Social engineering is the act of persuading users to provide their confidential information. The types of information may differ, but usually, the hackers are trying to cheat the users to get their passwords, credit card details, and bank information.

The hackers can also access a system secretly to install malevolent software which will give them access to their personal information along with control over the computer.

Generally, social engineering attacks occur in the form of phishing emails which attempts to encourage users to reveal their information, or even readdresses to websites such as various banking or shopping sites which looks authentic and comply users to enter their details.

5. Denial of Service:

A Denial of Service also known as DoS attack takes place when regularly operating services are reduced to unavailable. The prime objective of DoS attack is not to steal identities or data, but it is aimed at disabling businesses from functioning.

Within IoT networks, more networks are connected which means that more and more services are open for hackers and attackers who are looking to inactivating the operating ability.

Although the businesses may not undergo any data loss, the hits to business stability and status can be extremely disastrous and tragic.

How to Stay Secured and Protected?

The users are recommended to use passwords of proper standards moreover if they doubt any suspicious activity so change their passwords. Also, use VPN and encrypting file systems to protect yourself from the threat of cyber crimes.

The users should also make a wise decision while choosing their device. Either you are choosing any device for business purpose, or personal use make sure it has been designed with security in mind. Select products which have combined security considerations in all stages of design and production.

Conclusion

IoT is a great idea which can change our lives. This idea can make impossible things possible. It can create a world in which cars are in continuous communication with the maker to avoid any automobile failure or to inform us when the car needs maintenance. Also, the refrigerators can easily order groceries and get them to deliver to our homes.

IoT brings about a lot of serious concerns and cybercrime is the most highlighted one. Cybersecurity is essential in the IoT era. Preventing data violation is somehow difficult and impossible but by adopting various measures one can easily protect themselves.

About the Author

Zehra Ali is Editor at the PrivacySniffs. She is a Tech Reporter and Journalist with 2 years of experience in the infosec industry. She writes on topics related to cybersecurity, IoT, AI, Big Data and other privacy matters on various platforms.

Zehra Ali can be reached online at (email, twitter) and at our company website http://www.privacysniffs.com/

Is Building a Shark-Cage Right for Global Business?

THE REPURCUSSIONS OF A CONTINUED ISOLATIONIST APPROACH TO CYBER SECURITY AND THE ALTERNATIVE 'CLEAN NETWORK' APPROACH THAT CARRIER-GRADE OPERATORS CAN PROVIDE

By Steve Patton, Cyber Security Specialist & Director, Telesoft

$1.63 billion. That's the estimated fine for Facebook if it is found guilty of failing to adequately protect user data. The enactment of the EU's General Data Protection Regulations (GDPR) has ushered in an era of astronomic fines for inadequate protection of personal data and privacy. There are caps in place, but they offer little comfort for the non-compliant business: it's still an eye watering €20 million or four per cent of global turnover, whichever is the greatest.

As Bernard Marr has calculated for Forbes, GDPR would have had a terrifying effect on some of the world's biggest companies in the past few years. In this hypothetical:

- **Yahoo would have been fined** up to $160 million in 2014 **for what was then the largest data breach in history.**
- eBay would have faced a fine of $264 million on turnover of $6.6 billion for a data breach that affected 145 million users in 2013.
- Equifax would have been fined $124 million from its $3.1 billion revenue **for** compromising the personal information of 143 million consumers in one of the largest cyber-attacks of 2017.

Facebook itself would have faced a double whammy: a fine of $1.9 billion instead of the £500,000 the company was actually fined for data harvesting earlier in 2018.

Even after the data deluge of the past few years, during which businesses of all kinds have learned a lot about data management, storage, security and dissemination, GDPR has focused minds. And for any firms across the Atlantic looking on in relief, this is not just an issue for companies registered in the European Union.

GDPR covers any company that process the personal data of an individual or business in the EU regardless of where they themselves are located, with big penalties for both data controllers and data processors.

Of course, GDPR has come about precisely because that data deluge has proven quite how valuable personal information can be. That's in addition to business-critical IPR that can be extracted from inadequately protected systems and networks. Protecting data at any stage of its journey through the corporate world is rather like swimming with sharks: one sign of weakness, one drop of blood in the water and you're the most attractive target for some of the most ruthless spies, states, hacktivists and organized criminals in the sea.

Because no one wants to be shark-bait, individual businesses have been rushing to ensure that they have the right tools and procedures in place to ensure they don't fall foul of the cybercriminals or the regulatory and reputational consequences of a breach. In their attempts to build a protective shark cage, however, businesses have usually looked at protecting in-house systems, solutions and infrastructure in an 'every man for himself' approach to cyber security.

But putting up the defenses to create a corporate cyber fortress raises a couple of interesting issues that also need to be addressed. Businesses don't stand in isolation, and in today's globalised economy, the weak link in the chain may not be within the company itself but within the extended supply chain of partners, vendors, suppliers, customers and others. Any of these can accidentally (and, on occasion, deliberately) open a covert backdoor into a partner business.

Then there's the question of what happens to data once it leaves local storage and travels three times round the world via global networks. Smart criminals recognise that data can be at its most vulnerable when it's in transit rather than when its sitting secured in various network end points.

We've all seen the rise in the number of and damaged caused by third-party attacks, as cybercriminals sneak upwards through the supply chain, sniffing out any vulnerabilities and entry points. Just as we've seen threats against carrier networks themselves, as criminals siphon off data from network platforms, rather than individual devices.

So what's the answer? Certainly the individual approach is going to deliver limited results. Cyber-attackers will always go for the weak underbelly. If it's not your company today, it'll be your company tomorrow.

So instead of relying on shark-cages, firms should look for shark-free waters. That means network providers that have the tools in place to protect the volume, velocity and value of data crossing their infrastructure today, providing a 'clean' network for all their partners.

Operators need security tools and solutions that are built for these kinds of networks from the start. Scalable solutions are all very well, but very few can cope with the size, reach and sheer relentlessness of today's threats facing carrier-grade networks.

That, in turn, means a multi-layered approach to security, using carrier-grade tools that are designed to operate in a 100Gbps-rate environment. This includes, but is not limited to: technology that can detect and prevent cyber-attacks or data breaches by providing total visibility of the entire network; monitoring and diagnostics of network performance to analyse network traffic traversing the network and monitor security; detect threats and anomalies using signature matching against known threats. Integrated network visibility software, real-time monitoring tools, scrutiny of every packet, and event-driven intrusion detection systems are just some of the components required to protect network infrastructure at this level.

This is what organisations, public and private, should demand of their network provider. And this is what providers of carrier-grade networks should happily deliver. Because as one technology giant put it some years ago: the network is the computer. That's even truer now than it was then. Protect the network properly, and you're protecting everything else – including the bottom line.

About the Author

Steve Patton, Cyber Security Specialist & Director, Telesoft, is an experienced technical B2B cyber security specialist and Director. Steve is a frequent speaker on topics including security breaches, big data analytics, audit and compliance, and IT forensics. Steve can be reached online through LinkedIn and at our company website https://www.telesoft-technologies.com/

Your Security Auditing is Failing You, and Here's Why

A new report on cyberattacks caught my attention. Carbon Black's *November 2018 Quarterly Incident Response Threat Report* finds that hackers are increasingly destroying security logs to hide attacks.

Attacks that cover their tracks by disabling or destroying logs are nothing new. What is alarming is the prevalence of such attacks: according to the report, 72 percent of incident response (IR) professionals encountered this type of attack over the last 90 days.

As one IR professional remarked, "We've seen a lot of destruction of log data, very meticulous cleanup of antivirus logs, security logs and denying IR teams the access to data they need to investigate."

In this new reality, the question becomes, how do you protect yourself?

Active Directory Holds The Keys To The Kingdom

As the keeper of the keys to the kingdom, identity services are an extremely attractive target for hackers. And given Active Directory's widespread adoption – more than 90 percent of organizations rely on it for identity services – it's especially at risk.

Statistically speaking, your organization will be hacked sooner or later. Here is a scenario that is unfortunately becoming common:

An attacker breaches the environment by a phishing, password spray, cross-site scripting, or other type of attack (the possibilities are virtually endless and constantly changing). Through lateral movement techniques, the attacker gets access to the Domain Admin group. While that is terrible, it's not actually the end goal.

As the next step, the attacker logs in to a domain controller, stops the auditing agent, and disables security logging. With the security camera effectively turned off, the attacker modifies accounts, groups, Group Policy Objects (GPOs), DNS records, and other AD-related objects – creating backdoors that can be used at a later stage.

The organization finds out that something is wrong within 10-15 minutes from the time the attacker logged in to the DC. They connect to the machine, terminate the attacker's session, disable the compromised Domain Admin account, and gain back control… or do they?

The reality is the attacker was perfectly aware they were about to get exposed. So, the question now becomes, what did they do during those 10-15 minutes?

Another way that attackers can bypass security logging is to inject data directly into the Active Directory replication stream. That's exactly what DCShadow does, making it invisible to SIEM systems and worrisome to security teams. (More on DCShadow can be found here.)

Keeping the Security Camera On

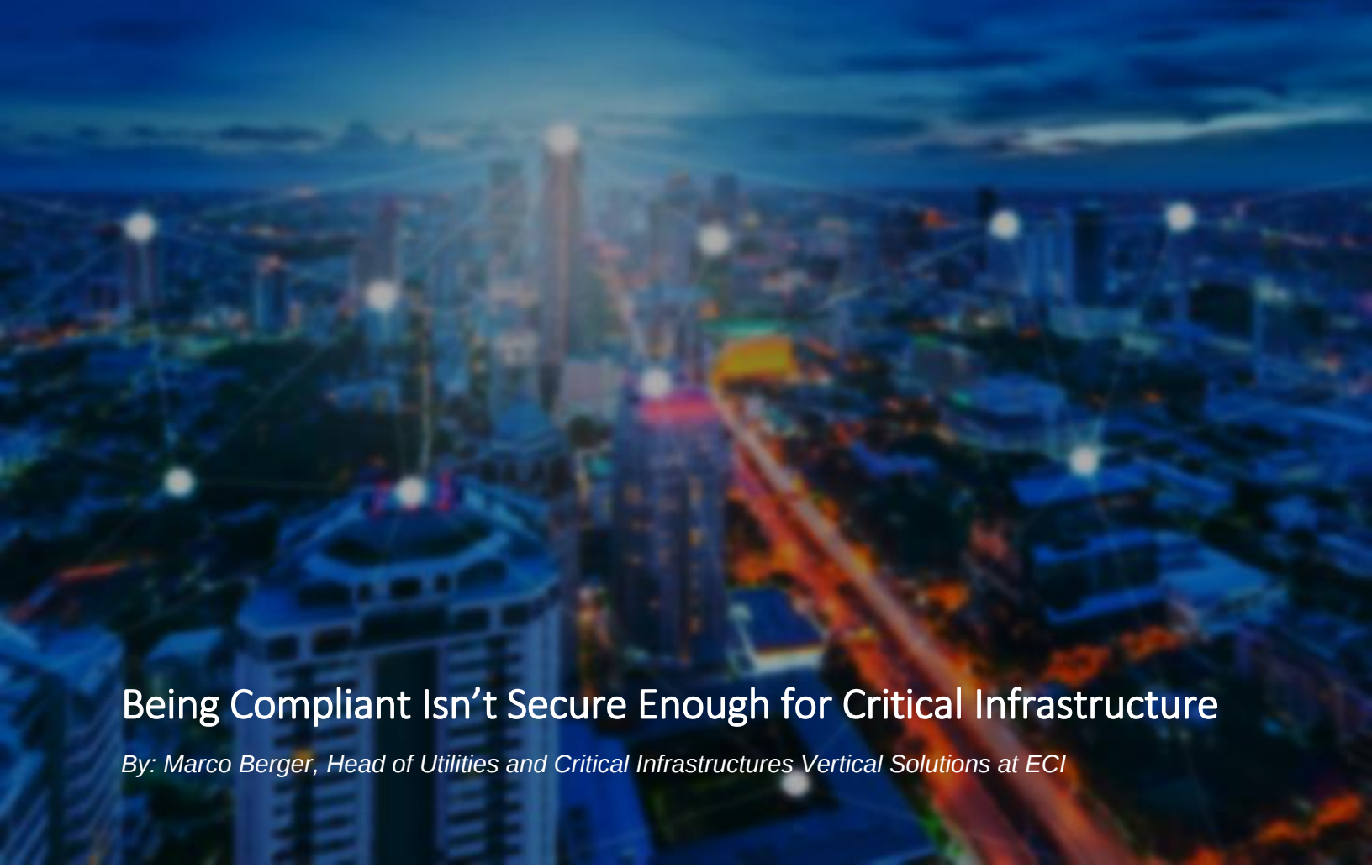
How do you deal with a scenario where the auditing agent was disabled, or the logs can't help because they were never there?

The answer is having another source of data that is independent of any single machine. As you probably know, all of the information in Active Directory (excluding some event details) doesn't stay with a single server, but is replicated across DCs and can be picked up from any DC in the domain.

This is how Semperis provides visibility of changes made even if security logging or auditing agents are disabled, or changes are made below the radar. The Semperis solution gathers changes from two independent data sources – one of them being the AD replication API.

So, in the example above, even if the auditing agent is disabled or changes aren't logged, the hacker's nefarious activity is captured when AD replication takes place. Changes are stored in a SQL database where the information can be used for forensic analysis and remediation. This allows you to identify and undo the unwanted changes made by the attacker – eliminating backdoors, and truly regaining control of your Active Directory.

Have you encountered hacks where attackers bypassed security logging? Are such hacks part of your risk assessment? I would love to hear about your experience and thoughts on the topic.



Being Compliant Isn't Secure Enough for Critical Infrastructure

By: Marco Berger, Head of Utilities and Critical Infrastructures Vertical Solutions at ECI

The attacks against critical infrastructure worldwide should be a reminder that there is a big difference between network security, and only meeting basic compliance mandates. Cybersecurity is now a constant concern for utilities and other critical infrastructure operators, especially as new exploits make headlines almost daily.

With the number of changes impacting the critical infrastructure market, including but not limited to the need to replace older SDH/SONET OT networks with new optical-packet technologies, the Distributed Energy Resources effect (DER) that requires a smarter grid with more sensors and IoT technology, the convergence between IT and OT networks due to new IP-based applications and services, increased automation of metro-railway systems, an increase in bandwidth and connectivity requirements and physical security threats to critical assets, there is an ever-growing awareness toward finding a much more holistic cybersecurity answer to protecting all of these assets.

Rather than depend on basic compliance, here's a look at the main pillars needed for a complete security solution:

Securing IT & OT

The integrity of the network must be secure for both information technology (IT) and operational technology (OT), two once segregated segments. This is especially true as the number of entry and endpoints is growing, as well as the complexity of the network.

The vulnerability of the OT network on its own is well known, as has the inability of firewalls to stop man-in-the-middle and many other attack vectors. By combining both the IT and OT, you can exchange information across those networks, have the same technology throughout (training, maintenance, management, etc.), and leverage the same network to protect your IT and OT assets.

As technology and market factors make it unrealistic to keep IT and OT separated moving forward, the most vulnerable entry points remain the endpoints — router ports, workstations, integrated access devices, SCADA devices, metering devices — because they are often overlooked and unsecured. Threats aimed at utilities are typically characterized by attacks coming from the IT towards the OT, from the OT to the IT and sometimes in the middle communications layer (wireless, cooper, coax and fiber).

It's no secret that regulations often take years to be developed, agreed upon and implemented, but people looking to disrupt systems work much faster than that. So, while compliance with regulations is absolutely an important step, no one should assume compliance equals secure.

Getting Attack Prevention in Place

Attack prevention needs to be in place at the communication points of entry to critical infrastructure facilities, including the ability to detect anomalous events that may be precursors to an attack.

This means firewalls, controlled access, and other traditional security protocols at multiple access points within the network should be monitored at all times, to ensure anomalies can be detected early and stopped quickly if needed.

Luckily, comprehensive security systems, focused on safeguarding the multi-layered processes and protocols within an organization, are already being developed. As opposed to the business sector, it has been found that hackers of critical infrastructures tend to focus on attacking industrial processes rather than physical assets, as illustrated by the Ukraine power grid attack.

Detecting Threats Early

The ability to detect real threats from the deluge of the incoming security alerts is critical, which requires some investment into a solution that includes machine learning and AI.

Without artificial intelligence and data analytics, it's nearly impossible to dig out the real threats from the thousands of flagged events every day. And, as attacks become more distributed and long-term, this analysis becomes critical to network security. Mere compliance with regulations will not put all these pillars in place.

A complete cybersecurity approach isn't limited to just one or a few parts of a company, like a typical IT department for example. The adherence to self-decided standards, rules and practices must be a top-down and a bottom-up responsibility flow. A company's security solution must be complementary to all current security approaches and will ultimately fail without company-wide awareness and implementation of practices and procedures.

Security is About Collaboration

Open systems allow collaboration among many people working on the solution, and the intelligence of the analytics systems gets better every day. Utility networks can absolutely be made very secure. Just don't assume that compliance with the regulations is the only step in that process.

Open systems also allow for companies to leverage far better intelligence and analytics to ensure companies can be both compliant and secure. In a world where the only constant is change, the only means of staying 'future proof' is through constant feedback.

As a result of recent regulations, however, most utilities have started to perform routine threat analysis scenarios and consultations, as well as intensive staff training on data and cybersecurity practices, using the regulations as a framework. These regulations must be combined with regular on-site and real-time threat analysis of the OT network and other critical assets, so that deployment of security and safety tools is performed giving a high level of effectiveness while responding to the three main pillars described above.

It is critical for infrastructural services to actively recognize the tangible threats that cyber-attacks present, and to work in collaboration with security services toward developing the technologies needed to keep them at bay.

About the Author

Marco is Head of Utilities and Critical Infrastructures Vertical Solutions at ECI. As such Marco is in charge of developing opportunities, solutions, sales tools and collateral for the variety of customers in his vertical. Marco can be reached online at https://www.linkedin.com/in/marco-berger or at the company website https://www.ecitele.com/

Leading The Way in Discussions for National Privacy Laws

Business and consumers continue to discuss privacy regulations and legislation. Data breaches, data vulnerabilities, and compromised private information is released in the news almost daily. Legislation has recently been proposed for individual states regarding data privacy regulations head-on. Virginia, Vermont, Colorado, and New Jersey have all introduced related privacy regulations most recently. California recently set themselves apart in the privacy space with the adoption of the California Consumer Privacy Act (CCPA), which gave citizens the rights to not only protect their own data, but to obligate businesses to disclose exactly which information has been collected about them.

At the federal level, the United States has yet to propose a national privacy bill. Vermont recently implemented a law regulating data broker companies that buy and sell personal information. With the new law, brokers must disclose what information they collect as well as allow customers to opt out of collection. Furthermore, consumers can sue data brokers if they sell any information that causes illegal discrimination. A similar law has also been proposed in Colorado that is broader, yet specifically manages personal identifying information. Individual states seem to be leading the way for data privacy regulation discussions.

International regulations have also played a significant role in the privacy discussion, specifically following enforcement of the GDPR (General Data Privacy Regulation) in the European Union (EU).

These regulations have certainly contributed to the movement towards consumerism and prompted businesses in the United States to rethink data collection and management, considering how violating these regulations could adversely affect their business and brand. Many organizations are asking

themselves “am I liable and governed by the legislation in the EU?” For many, the answer is yes. More specifically, any website that offers goods or services to EU natural persons is subject to the GDPR. The discussion has further prompted organizations to question whether or not they are governed by similar laws in the United States.

Since the introduction of the CCPA, several senators have proposed policy options for national legislation on data security and privacy. Proposed bills have had a GDPR-like flavor that is similar in scope to the international regulation. If the U.S. were to adopt similar regulatory standards, business processes and products that handle personal data would need to be built to include data protection by design and default.

Regardless of business size, the magnitude of data collected, shared or mismanaged is more concerning considering the sensitivity of private information in which every-day people entrust these organizations to protect. As the conversation around regulation increases, there has been much talk about what a national privacy law might look like, and furthermore how state regulations would affect organizations doing business across the U.S.

At the forefront of privacy-law related issues are very visible and widely used big technology companies. These big technology players have demonstrated some interest in getting ahead of possible regulation by possibly drafting and proposing possible regulatory standards themselves possibly because there is a monetary desire for these bills to be aligned with their terms, rather than abiding by laws voted in by citizens of the United States.

Big data companies such as Facebook, Google, and Twitter have all been amongst discussions, and various reports have been released stating the companies are “in-favor” of such legislation. This push has left some lawmakers feeling uneasy, considering these companies are likely seeking to be involved in legislation to sway technicalities in their favor.

In conclusion, states will likely continue to pave the way for privacy regulations. Until formal national legislation is adopted, and voters see these initiatives on their ballots, states will continue to implement their own forms of data protection. Problems will continue to rise for businesses as states implement their own laws that non-regulated states must abide by. A national privacy law could make this transition easier among U.S. business owners, as one uniform standard can be applied to all.

About CompliancePoint:

CompliancePoint is a leading provider of information security and risk management services focused on privacy, data security, compliance and vendor risk management. The company’s mission is to help clients interact responsibly with their customers and the marketplace. CompliancePoint provides a full suite of services across the entire life cycle of risk management using a FIND, FIX & MANAGE approach. CompliancePoint can help organizations prepare for critical need such as GDPR with project initiation and buy-in, strategic consulting, data inventory and mapping, readiness assessments, PIMS & ISMS framework design and implementation, and ongoing program management and monitoring. The company’s history of dealing with both privacy and data security, inside knowledge of regulatory actions and combination of services and technology solutions makes CompliancePoint uniquely qualified to help our clients achieve both a secure and compliant framework.

About the Author

Matt Dumiak, Director of Privacy at CompliancePoint has over 10 years of experience with Information Security, Cyber Security, and Risk Management. His knowledge spans across multiple industries and entities including healthcare, government, card issuers, banks, ATMs, acquirers, merchants, hardware vendors, encryption technologies, and key management.

How Businesses Can Avoid S3 Bucket Leaks to Protect Company and Client Data

Brian Johnson, CEO, DivvyCloud

An organization that has transitioned to a cloud provider such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, or any combination thereof should immediately be thinking about the configuration of cloud services as a key element to security.

Many IT leaders and professionals make the mistake of approaching security in the cloud the same way they approached security in a traditional data center. However, in the software-defined world of public cloud, there is an added wrinkle. Without a holistic approach to security which includes a view of configuration, you can easily open yourself up to undue risk. Configuration is an additional challenge when dealing with software-defined infrastructure in the public cloud. This is especially of concern when empowering developers and engineers with self-service for provisioning and configuration, who may not be familiar with security and having to deal with the rate of change in the cloud. Because cloud technology is always changing, it's vitally important that we understand the configuration choices being made. Validating those configuration choices against security standards becomes far more important for most companies now than in the past because failing to do so, for example, in AWS S3 Buckets, can lead to the company data breaches that we continuously hear about in the news.

Storing remotely versus locally offers huge advantages to both consumers and businesses, however, exposed S3 Buckets are a constant in the news these days. Too many companies in the last year alone (Fed Ex, Alteryx, National Credit Federation, Verizon, Australian Broadcasting Corporation, Dow Jones, Deep Root Analytics, Robocent, Macy's, Adidas, GoDaddy, SpyFone, etc.), have exposed sensitive, personal information of hundreds of millions of people from around the world. This epidemic has seen the theft or loss of more than 9 billion data records in the last five years.

Examples of Misconfigured S3 Buckets

- SpyFone, whose website hero header reads "Monitor Your Children with World's #1 Parental Monitoring Software – Trusted by Parents Worldwide" left the data of thousands of its customers—and the information of the children they were monitoring—exposed in an unprotected Amazon S3 bucket.

According to Motherboard:

"The data exposed included selfies, text messages, audio recordings, contacts, location, hashed passwords and logins, Facebook messages, and more.
A security researcher found the data on an Amazon S3 bucket owned by SpyFone, and Motherboard was able to verify that the researcher had access to SpyFone's monitored devices' data by creating a trial account, installing the spyware on a phone, and taking some pictures. Hours later, the researcher sent back one of those pictures.

The researcher said that the exposed data contained several terabytes of "unencrypted camera photos."

- GoDaddy, one of the world's top domain name registrars with over 18 million customers, was discovered to have files containing detailed server information, stored in an unsecured S3 bucket. According to the report from cybersecurity firm UpGuard, the exposed documents include high-level configuration information for tens of thousands of systems and pricing options for running those systems in Amazon AWS, including the discounts offered under different scenarios.

  Mallory Locklear, Engadget, reported that UpGuard notified GoDaddy of the discovery shortly after uncovering the exposed storage bucket, but GoDaddy didn't secure the information for over five weeks. In that time, when checking up on the progress of his report, it was said that it's typical for there to be a delay following security reports such as this one.

  It seems in this instance that Amazon itself was the cause of the exposure. "The bucket in question was created by an AWS salesperson to store prospective AWS pricing scenarios while working with a customer," an AWS spokesperson told Engadget. "No GoDaddy customer information was in the bucket that was exposed. While Amazon S3 is secure by default and bucket access is

locked down to just the account owner and root administrator under default configurations, the salesperson did not follow AWS best practices with this particular bucket."

How Did These S3 Buckets Get Exposed?

Often times the S3 Bucket configuration is incorrect. The created container permissions may have been too broad which allows anyone to access the data. Again, these S3 Buckets may have been serviced by people who aren't familiar with security, thus the developer who created the container was unaware of how to properly secure it, or it was something as simple as an oversight. For example, in Spyfone's case, they may have had a developer who was troubleshooting an issue that was causing an application to fail and suspected the S3 Bucket access was to blame. The developer may have tweaked the S3 configuration leaving it open to the public, and as the application began working again, moved on to another project. Now they have an exposed S3 Bucket. As in the case of GoDaddy, it may not have even been the developer's fault as someone else may have altered the bucket's configurations at a later date for any number of reasons. The point is, so many organizations are made vulnerable because a lot of them don't have processes that prevent insecure software deployments.

How Do Organizations Avoid S3 Bucket Leaks?

For starters, as the AWS representative told Engadget, these organizations could have done nothing. Amazon S3 buckets are private by default and can only be accessed by users that have been explicitly given access. Again, by default, the account owner and the resource creator are the only ones who have access to an S3 bucket and key, so someone has to actively misconfigure an S3 to expose the data.

Amazon has been actively working to help companies avoid breaches caused by misconfiguration. In November 2017 AWS added a number of new Amazon S3 features to augment data protection and simplify compliance. For example, they made it easier to ensure encryption of all new objects and monitor and report on their encryption status. They have also provided guidance on approaches to combat this issue, like the use of AWS Config to monitor for and respond to S3 buckets allowing public access.

As a most basic first step to avoiding S3 bucket leaks, take advantage of the native AWS capabilities. Ensure that you are always purposefully using AWS S3 access policies to define who can access the objects stored within. Ensure your team is well trained to never open access to the public, unless absolutely necessary, as doing so can result in the exposure of PII and other sensitive data. And help prevent unauthorized access to your data by taking advantage of capabilities like AWS Config.

The challenge is that many organizations struggle to adopt and enforce best practices consistently, and only 100% consistency can ensure protection against a breach. This is why an investment in cloud operations is a vital additional step.

Invest in Cloud Operations:

Cloud operations, or CloudOps, is the combination of people, processes, and tools that allow for organizations to consistently manage and govern cloud services at scale. Key to this is hiring and developing the right people, identifying processes that address the unique operational challenges of cloud services, and the automation of these processes with the right tools. One vital tool in your CloudOps toolkit should be software that monitors and remediates cloud misconfigurations allowing you to achieve continuous security and compliance at scale.

For example, using said tool, an organization will be able to leverage automation to remove the public permissions from the access control list where necessary. Users should also be able to leverage bucket policies in place of access control lists for the finer-grained access control. This automation prevents data breaches by finding, alerting, and remediating misconfigured storage containers way before vulnerabilities are exposed.

It's important to highlight that these cloud management platforms should not only flag the problem in real-time but give the user an exact pointer to where the problem is. If somebody were to tell you "there is an open S3 bucket" but didn't narrow down to a granular level, where would you start? This is why the cloud management platform you choose should alert that there is an open S3 Bucket, then take action and inform the user to exactly which bucket in which account.

In the end, the way to avoid exposing data in S3 buckets is really common sense: Don't ever configure the S3 buckets to be exposed to the public. Organizations need to learn about security configurations while evaluating their public cloud options or pay someone else to do it for them. Otherwise, it's only a matter of time before they join the 12 aforementioned organizations in the growing list of those who have to explain to their customers that their information has been compromised.

Passwords and Honeywords

How to detect data breaches with honeywords.

by Pedro Tavares, Founder of CSIRT.UBI & Cyber Security Blog seguranca-informatica.pt

Data breaches and information leakage are a topic that has been making headlines in recent times. Cyber attackers take advantage of weak systems' protection measures and obtain a great amount of information that can be leaked onto the Internet, and many times are also sold in dark web forums. Personal information such as emails, usernames, passwords, password representation (hash keys), personal addresses, phone numbers, credit card numbers represent some of the information that is often obtained by criminals when a data breach occurs.

A password representation is stored somewhere in a database when a system authentication process is well-designed, — basically, a hash key is generated when the user registered at the first time in the system.

Cracking a password representation — a hash key (MD5, SHA1, SHA2, etc.) - is seen these days as a basic procedure from the attacker's point-of-view. The guideline is known: trying to guess the password behind the cryptographic hash through some documented techniques within the password cracking landscape, for instance, using rainbow tables and brute-force attempts.

Due to that, passwords are seen as a poor authentication method as cyber attackers can obtain the user's secret in an easy way. In order to solve this problem, a mechanism to detect false system's authentication was proposed and developed by Ari Juels of RSA Labs and MIT Professor Ronald L. Rivest: *"We propose a simple method for improving the security of hashed passwords: the maintenance of additional "honeywords" (false passwords) associated with each user's account".*

Honeywords

Honeywords are very similar to honeypots, a solution that allows the user to deceive criminals, making them believe that they are attacking the real system. This method improves the security of hashed passwords as described by its authors: *with the use of honeywords, an adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeyword.*

In this sense, when an attacker obtains a password from a password cracking process, he gets the correct or fake password. At the time to authenticate onto the system, a notification is sent to the IT administrator every time a fake password is submitted. For this, there is a secondary server named honeychecker that validates true or false passwords. This server can be seen as an oracle and is isolated from the system improving thus a additional infrastructure resilience.

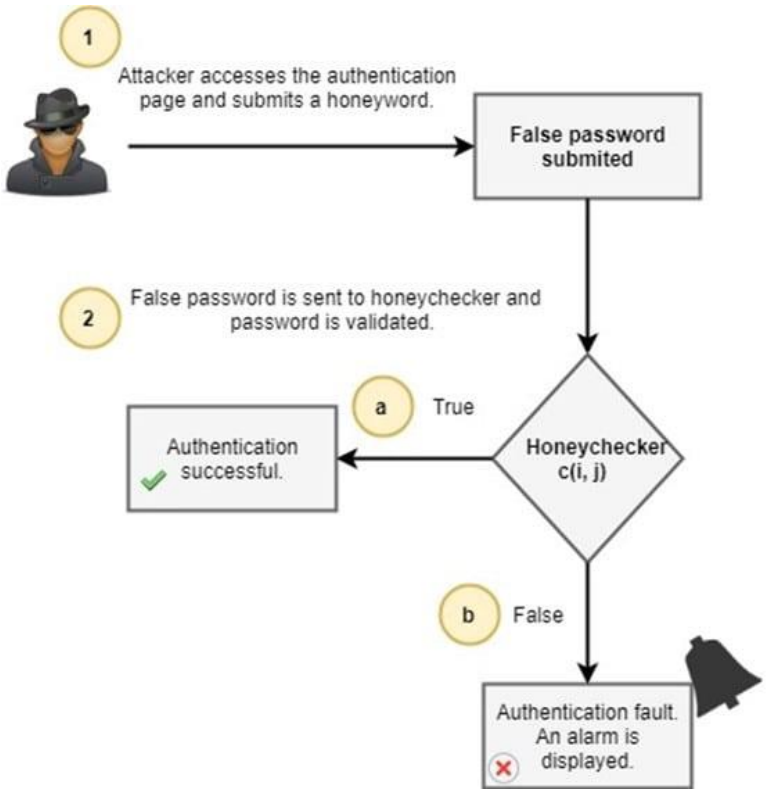
How This Mechanism Works

The user John Doe starts a register in the system with the password “cyberdefensemagazine2018”. At this moment, other password variants (honeywords) were also generated. The following information is created and stored.

ID	**Password representation (SHA1)**
1	233436af8122058f3b04599f12dcd1f1f7096b56 (cyberdefensemagazine2018)
2	9017347a610d1436c1aaf52764e6578e8fc1a083 (cyber)
3	66efd9eefecf45dd64eff8e5cb2d13e005041925 (2018)

The user password is defined by the SHA1 hash key 233436af8122058f3b04599f12dcd1f1f7096b56. At time to brute-force password representations, the hash keys with the ID 2 and 3 are reversed quickly by the attacker, since them were generated via a weak password.

Weaker passwords are broken faster than strong passwords because they have a smaller size and a weak complexity. For example, according to the group of honeywords defined in Figure 1, the **2018** or **cyber** honeyword is quickly broken compared to the original password picked by the user (**cyberdefensemagazine2018**).



Final Thought

The use of honeywords isn't going to prevent attackers from stealing password databases and cracking them, nonetheless, the implementation of this method can improve the security and resilience of the system against data breaches.

Some benefits of using honeywords are enumerated as follows:

- When a fake password is detected in an authentication operation, a data breach can be earlier detected by IT operators.
- A user account can be automatically locked down when a honeyword is used.
- The honeychecker executes separated from server running the system and compromising the honeychecker does not compromise the website (and vice-versa).
- A password obtained from the cracking process does not give the attacker confidence that he can login successfully and undetected — that can be a fake password and an alarm will be triggered informing IT administrators that a risky-signin is happening.

About the Author

Pedro Tavares is a cybersecurity professional and a founding member and Pentester of CSIRT.UBI and the founder of seguranca-informatica.pt.In recent years he has invested in the field of information security,exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, hacking, cybersecurity, IoT and security in computer networks. He is also a Freelance Writer.Segurança

Informática blog: www.seguranca-informatica.pt
LinkedIn: https://www.linkedin.com/in/sirpedrotavares
Contact me: ptavares@seguranca-informatica.pt

Another Cyber Security Month is Over: So What's New?

Leigh-Anne Galloway, Cyber Security Resilience Lead at Positive Technologies

Another October goes by, and with it another National Cybersecurity Awareness Month. Celebrating its 15th year as an annual initiative to raise awareness about the importance of cybersecurity, its close is a good time to reflect on what progress has been made, and where we currently stand as an industry.

As always, this noble combined-effort between government and industry - to increase cyber security for the public and the nation - was overshadowed by the ever looming spectre of high profile cyber attacks. In October alone, the Wall Street Journal exposed that up to 500,000 Google+ accounts could have been left exposed thanks to a bug, leading to the ill-dated site promptly being shut down; Facebook confessed that up to 29 million users were affected by its data breach; and - on the international stage - Hong Kong airline Cathay Pacific disclosed that a massive 9.4 million passenger records were lost earlier in the year.

Combine these breaches with regular additions to the threatscape and a whole lot of industry jargon (right now the buzz is around 'quantum-protected networks,' 'destructive mass attacks' and ransomware; next week it'll likely be something different), and it's safe to say that, on ground level, the security landscape looks at best confusing. At worst, the landscape looks bleak.

Yet, if we take a step back, we do see progress. It is clear too that companies are strengthening protection and striving to comply with regulatory requirements.

It shouldn't be overlooked that October was also a bumper month for security-related sanctions: Anthem reached a settlement of $16 million with the US government for its 2015 data breach, Facebook was fined $645,000 by the UK's regulator over the Cambridge Analytica scandal, and Yahoo agreed a $50 million settlement for those affected by the 2013 data breach.

As these occurrences become increasingly regular, organizations are investing in improving their security posture, so as not to be caught out. Cyber attacks are pushing the development of defense systems, and this is genuine progress. As a result, it will be more difficult for criminals to hit companies with scattergun mass attacks, and targeted attacks will become the only option.

Governments too, are becoming increasingly aware of the opportunities offered by the cyberspace, with more and more creating their own Cyber Security Centers and Cyber Forces. The world has begun to recognize the necessity of such systems.

Furthermore, if we take an even greater step backwards, it is abundantly clear cyber attacks have not impeded genuine progress in the technology industry. We are constantly developing new tools, apps, social channels, middleware and capabilities, not to mention migration to the cloud and other big trends.

Progress Has Been Made but What's Next?

Of course, the next challenge will be in protecting these new technologies. Over the past 10-15 years, a lot of technologies and devices have appeared. However, they came - and continue to come - with a lot of errors and vulnerabilities, which, in addition to convenience (it is convenient to use a smartphone, store information in the cloud, and use face recognition for payments) are inherently a threat if exploited by the wrong people.

The Internet of Things is the epitome of this. Any device that has wireless connectivity can be hacked—everything from mPOS (Mobile Point of Sale) terminals to vacuum cleaners. Smart devices with default passwords or non-closed vulnerabilities are very likely to become a sore spot of their owners, and a favorite weapon of attackers who will use them to penetrate into local networks and conduct other attacks. For example, we can expect to see continued use of IoT devices for botnets due to the low level of security implemented in such devices.

As the public has had to slowly learn how to protect themselves on their PCs, online, and on their phones, they will also be learning on how to stay safe as an increasing number of their devices go online. The security industry, too, will have to adjust to this new reality.

On a national level, while countries are improving their cyber potential, more focus needs to be turned to critical infrastructure: telecoms, energy, industry. In 2018, vulnerabilities at the firmware level have been detected among many manufacturers, such as MikroTik, Netgear, and TP-Link. This means that vulnerable routers may become part of a new or existing botnet, and that companies that do not keep network equipment up to date are under threat. Industrial and energy companies are at greatest risk of these attacks.

Telecoms, however, is perhaps at the greatest risk. Although operators are well aware of security issues, 78 percent of telecom networks are vulnerable to attacks. SMS interception, for example, is still possible in nine cases out of 10.

This is also a much more complicated issue to solve. This is primarily due to the fact that in order to increase the protection level, current standards and operating procedures of signaling networks have to be reviewed. 5G mobile network is currently under development but no significant progress in security has been achieved so far. Moreover, even once agreed, it may take years for a new security technology to become actively used.

On ground level, it is often hard to make heads nor tail of how we are progressing in improving our cyber security capabilities. However, by taking a historical perspective and looking at global trends, it is clear that progress has been made in the past 15 years. Companies and governments are undoubtedly taking security seriously, and spend is going up year on year. Taking a step back also helps us see the progress that still needs to be made, and the threats that need to be addressed next.

2/3 Of Fortune 50 Companies are at Risk of Being Taken off the Internet – Is Your Company Too?

by Angelique Medina, Senior Product Marketing Manager, ThousandEyes

Two years ago, Amazon, Comcast, Twitter and Netflix were effectively taken off the Internet for multiple hours by a DDoS attack because they all relied on a single DNS provider – Dyn, in their case. Can it happen again? According to the 2018 ThousandEyes Global DNS Performance Report, 68% of the top 50 companies in the Fortune 500 and 72% of companies on the Financial Times Stock Exchange 100 are still at risk. Two years after the Dyn DDoS attack, you'd think digital companies would have learned their lesson, but apparently not so.

According to the report, many of the biggest companies on the planet – as well as 44% of the top 25 SaaS providers – don't have a fallback DNS server option. That means that a single outage or DDoS attack could completely take their businesses off the Internet.

DNS is the "phone book of the Internet." It's the first step in how humans connect to online brands because it's the Internet infrastructure that translates human-readable domain names to routable IP addresses. Without DNS, there is no digital experience. It's the least appreciated aspect of delivering online user experience, and the most overlooked chink in an enterprise's armor, Even digitally mature organizations can get DNS wrong by not following best practices around resiliency. It's also a complex topic that most networking professionals haven't spent enough time to understand.

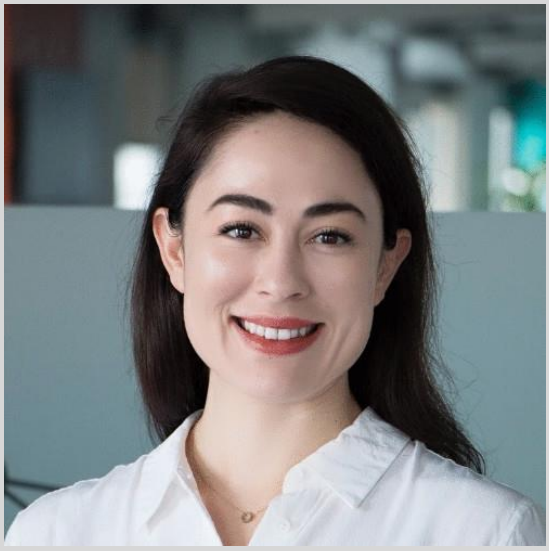
The DNS expert community is select, but the need for awareness of DNS has grown as more businesses than ever rely on digital experiences in their revenue generation. According to Gartner, CIOs report that 37% of their revenues will be have a digital footprint by 2020. If DNS is the first step in every digital experience, than not getting that step right can be incredibly costly.

As for the lack of enterprise DNS resiliency, consider this analogy. Most IT professionals would never consider building a data center without backup power or redundant telecom or Internet connections. Further, most know that redundant connectivity isn't truly redundant unless there is diversity of physical cable routes and facilities. But too many are just using a single DNS service. If that DNS "power" gets cut, it doesn't matter how much you spend on your CDN, your regional cloud hosting, etc. Your brand will be offline and you'll be scrambling.

DNS is still a bit of a "dark art" that many IT practitioners and leaders pay little attention to, not understanding that its performance and security can significantly impact digital experience.

In many cases, it's simply a lack of awareness of best practice. Companies often think that they're resilient because they have more that one nameserver, when in fact they are not. True DNS resilience means that your authoritative DNS records are served from diverse networks, facilities and routed prefixes. It's certainly possible to do this on your own. But it's typically easier (and less costly) to outsource your authoritative DNS to one or more third party service, which can often offer better performance and scalability across a broader geographic scope.

About the Author



Angelique Medina, Senior Product Marketing Manager, ThousandEyes.Angelique has worked in technical marketing roles related to network infrastructure and network visibility for the past ten years, most recently at ThousandEyes, where she works on multi-layer visibility spanning application, DNS, L3, and BGP. Prior to joining ThousandEyes, she spent time working on data center networking at Big Switch Networks and visibility switching at VSS Monitoring. She holds a BA in English from the University of California, Berkeley. You can follow her on Twitter @bitprints. Angelique can be reached online at (https://twitter.com/bitprints) and at our company website http://www.thousandeyes.com/

7 Network Security Tools to Protect Your Digital Assets from Malicious Activity

by Jorge Alago, Cybersecurity Architecture Lead, Veristor

How can you protect your network from today's elevated level of cyber threat activity? It's a question that many network administrators are asking. The first step is to understand the various network security solutions available and how they can help.

Here are seven tools that will help you protect your digital assets without getting in the way of business as well as some best-practices to consider to help identify the solutions that will elevate your security posture.

1. **Network Access Control (NAC)** executes authentication for all end users and devices—both wired and wireless. It's critical to authenticate every user and every device that tries to connect to your network, keeping in mind that most end users have more than one device, and some devices are shared by multiple end users. If you use a tool that has open APIs, it can talk to multiple devices from multiple vendors. Make sure the NAC can integrate easily with other security solutions in your network, so it can pass along authentication to other devices and enable them to become user-aware. For example, your NAC should talk to your firewalls so it can share information such as the user's IP address and the segments of the network the user is authorized to access.

2. **Next-Generation Firewalls** have earned the "next-generation" designation because they can incorporate multiple aspects of security, instead of just the basic, traditional firewall protection. These tools go beyond blocking unauthorized end users based on IP addresses and enable you to designate safe user groups and user names. You also benefit from intrusion protection and detection, URL web filtering, and SSL traffic decryption/inspection. Next-generation firewalls are also aware of who is crossing your firewall and what they have access to, and they can limit the access of each user based on the information they receive from your NAC.

3. **Web Application Firewalls (WAF)** have traditionally monitored external customers using an application hosted by your website and offer protection against SQL injections and other attacks. These devices are still adopted widely because they are now primarily software-based, which advances their capabilities to be on par with real-time application self-protection (RASP) technology. Software-defined WAFs allow you to add a small piece of code to a web application. The code checks traffic and runs analysis in the cloud, letting you know if you should block or allow each attempted connection. The best part is that software-defined WAFs enable changes and updates to be applied to a small piece of code, so the chances of application performance being affected are slim.

4. **Lateral Movement Detection** includes network traffic analysis tools that look for anomalous behavior so you can identify and mitigate malicious connections that may get by your NAC and firewall. It's an important layer to a network security strategy because no perimeter defense can offer 100% protection. If someone slips past your firewall and gets a user to download malware, it may be difficult to detect the anomalous activity unless you are monitoring traffic. A key aspect to consider in evaluating a traffic monitoring tool is the machine learning algorithm, because it's this feature that controls the threshold for false positives. It's inevitable that you'll experience some false alarms, but when there are too many, they distract the security team from investigating real threats. To find a solution with a strong algorithm that does not generate too many false positives, run a proof-of-concept for at least two weeks to see how it performs. Lateral movement detection tools also help you determine if anyone is jumping from machine-to-machine on your network. This is particularly helpful for flat networks that utilize a reduced number of routers and switches. Attackers who break into a flat network can easily jump from one part of the network to another, staying ahead of your scans. Detecting lateral movement will help you find adversaries moving around your environment and network monitoring analysis tools can help you find insider threats. You can also trace how malware spreads, making it easier to contain.

5. **DDoS Mitigation** protects you from distributed denial of service (DDoS) attacks that use hundreds or even thousands of devices to send large amounts of traffic to overwhelm a server. When that happens, web sites and applications become unavailable, or worse, entire organizations go offline. As a result, you risk loss of revenue and customer churn. Many businesses rely on their ISP to prevent DDoS attacks, but some ISPs have better threat detection and mitigation capabilities than others so the level of security varies. Adding to the uncertainty of protection is the fact that ISPs don't have good visibility into your applications and their use, so they don't have the ability to determine which traffic is legitimate, so all users and traffic are blocked until an attack is thwarted. But the leading DDoS mitigation solutions are able to block only the attack traffic so that legitimate traffic can pass through the network. So, while the attack is being mitigated, the business continues as usual.

6. **Deception Technologies** are the evolution of the honeypot, giving you a way to trick attackers with decoy servers, workstations, and user credentials. Businesses used to rely on honeypots to distract cybercriminals into spending their time in a place where they couldn't do much harm. But attackers have caught on and know a honeypot when they see one. Today's deception technologies feature decoy devices that you can place within a production environment. For example, if you have a /24 subnet that can host 254 devices, but you are only using 100 of the IP

addresses, you can use the other 154 unused IP addresses as virtual decoys that are vulnerable to attacks. If a decoy is attacked, you will receive an alert and be able to investigate the incident and possibly find out "who done it." So, look for decoys that capture information on the methods used to compromise the network so you can stay one move ahead in the cyber war.

7. **Network Segmentation** makes it more difficult for cybercriminals to freely navigate your network, which is relatively easy for them to do in flat networks. If you carve the network into several segments, you can protect each one with a firewall that enforces authentication. Think of a single-road town vs. one that's broken into many streets, and has a toll booth at the beginning of each block. Besides making it more difficult for a cybercriminal to navigate the network, it's easier for you to isolate and quarantine an attack. Small segments also allow you to control the flow of traffic and create zones where users are authorized and unauthorized. However, the goal is not just to create as many segments as possible. In order to segment the network effectively, the method should be based on a strategy that incorporates factors such as the criticality of the servers, the type of servers, and who should have access. In addition to improving network security, network segmentation can also improve network performance. For virtual environments, look for a solution that offers software-defined network segmentation.

Now that you're familiar with the tools that can come together to fortify your cybersecurity infrastructure, you've probably recognized the common thread. To optimize the performance of the seven key tools, it's important to make sure they can interoperate with one another so you can create a security ecosystem. The tools should all interconnect and report back to a centralized system for a single plane of glass view. The more information that is shared, the more intelligent each tool becomes, making it easier for them to protect your organization from attack.

It's also important to link your security ecosystem to external threat intelligence services offered by the leading security vendors. Sharing threat information with other businesses helps everyone learn about the latest threats and cyberattack techniques. By helping our industry peers build a better knowledge base, we are unified against the unseen entity that continues to evolve and strengthen as it grows.

About the Author

Jorge Alago is cybersecurity architecture lead at Veristor and an expert in implementing secure network environments. Veristor is a provider of business technology solutions that helps customers accelerate the time-to-value and security of the software, infrastructure, and systems they deploy. Jorge can be reached online at https://www.linkedin.com/in/jorgealago/?trk=public-profile-join-page and at https://veristor.com.

Faxploit: Critical Flaws in The Fax Protocol? Not So Fast…

Cause for Vigilance, But Not Panic

By Sébastien Boire-Lavigne, Executive Vice President and CTO, XMedius Solutions Inc.

At DEF CON 2018, Eyal Itkin and Yaniv Balmas, researchers from Israeli security software developer Check Point, demonstrated an exploit in the fax protocols of an HP multifunction device (MFD). The demonstration highlighted a vulnerability in said protocols that allows an attacker to send a malicious image file to the device, enabling them to use the device as an access point into an entire IT network. Once in, hackers would be able to gain access to confidential information, install ransomware or perform any number of other heinous activities.

While most hacks we hear about in the media are performed through the internet, this demonstration, aptly named "Faxploit," exploited a vulnerability in fax protocols that could serve as a potential entry point for cybercriminals. The result? Within a short period, there was widespread media frenzy. Headlines like "Your Fax Machine is a Threat to Your Organization!" flooded news feeds around the globe, causing panic. Faxploit, however, is not a cause for panic – it's an event that reminds us all to pay more attention to all devices in our network.

Whatever outdated connotations the word "fax" carries with it, it is still a method of secure document transmission that is widely used in the healthcare, legal, finance, government sectors, and more. According to Check Point, there are over 17 million business fax terminals still in use in the U.S. alone.

It is important to note that the specific protocols used as an entry vector in the Faxploit demonstration (CVE-2018-5924 and CVE-2018-5925) are the color fax protocols of the HP device. Color faxing is not an immensely popular form of document transmission and usually not supported by modern Fax-over-IP (FoIP) systems. This, of course, is not to underplay the remarkable research that was carried out, but

simply to take some of the edge off any widespread concern. HP responded quickly by patching the vulnerability of its printing engine, but similar vulnerabilities could exist for other vendors.

The Faxploit event is an excellent opportunity to bring fax security to the forefront: it is an application that IT professionals need to handle with the same level of care as they would their networks and email servers. Luckily, fax security is straightforward. Here are a few actionable steps you can take to minimize potential risks.

Patch your MFDs: HP's timely release of security patches amidst the Faxploit buzz caused other multifunction device manufacturers to follow suit. Make sure that your MFD firmware is up to date with the latest security fixes.

Unplug unused machines: Fax machines aren't inherently secure, but up until recently they had escaped most IT departments' notice. Are there MFDs around your office used strictly for printing or scanning? The biggest risk is not the machine itself but the phone line attached to it. Unplugging the phone line from machines that aren't used for fax functionality is a great step towards attack surface reduction.

Segment your fax devices: Network segmentation should become a top priority for fax and printer devices that are consistently used. These machines have a different security risk profile than the desktop environment, whether choosing to do this using VLAN controls, firewalls or any other means your organizations finds best. In fact, the motto "if a device doesn't need to talk to anything else on the network, segment it" is a good rule of thumb for security policies in general.

Fax Use Is Not Limited to Fax Machines

While fax remains a widely used method of transmitting sensitive documents, faxing itself should no longer be synonymous with the use of fax machines. Compliance regulations like HIPAA for healthcare, SOX for the finance industry and GDPR for any company who maintains records of EU citizen's personal data, all urge organizations to go digital when it comes to the exchange and storage of sensitive data.

Over the years, it's easy to see how mail has evolved from being delivered on horseback to today's virtual inbox – the same can be said for fax. Fax-over-IP technology has taken the throne as a highly secure and user-friendly way for organizations in any sector to transmit their confidential information. FoIP servers greatly reduce the area of attack and significantly reduce the efforts necessary to maintain a highly secure fax infrastructure.

Information security is a moving target, and so are the efforts of cybercriminals. Although zero security risk cannot be achieved, there are solutions that can be implemented by organizations that relieve much of the guesswork, stress and micromanagement involved in building strong information security policies – FoIP is one of them.

About the Author

For nearly 20 years, Sébastien Boire-Lavigne has been a driving force at XMedius, a global leader in the field of enterprise communications, and has been instrumental in developing XMedius' technology strategy. Among his many accomplishments, Sébastien led the development of the ground-breaking XMedius Fax-over-IP technology, cloud platforms and XMediusSENDSECURE.Sébastien can be reached at the company's website https://www.xmedius.com

Brands Beware! Strengthen Data Privacy or Pay a Hefty Price

By James Barham, CEO at PCI Pal

Historically, brands that fell victim to a data breach were forgiven by US consumers. But as cyber attacks and fraud rates have ballooned, it has become clear that the implications of a data breach reach further than once suspected. Rather than solely impacting a brand, consequences extend to consumers and their family and friends, as evidenced by the hack of the Office of Personnel Management.

The goal of a security breach is typically to gain access to sensitive and restricted data. Last year's massive Equifax hack resulted in criminals stealing 145 million Americans' personally identifiable information, including social security numbers, birthdates, addresses, drivers license numbers, as well as tax identification numbers (all of which can be used to steal a person's identity). Given the flood of data breaches and the introduction of data privacy regulations such as GDPR, it's undeniable that the value of data has increased in the digital age. Consequently, consumers have come to realize that brands should be responsible for protecting the data they collect at all costs or risk reputational and/or financial backlash.

This shift is certainly justified. In July, the Identity Theft Resource Center reported an astonishing 668 security breaches executed in 2018. The influx is the equivalent of around four breaches per day for a year. In response, consumers are threatening to take their business and loyalty elsewhere if they feel that a brand isn't prioritizing the protection of their data.

Caution! Shifting Consumer Opinion Ahead

To examine changing consumer sentiment and behaviors around data security, we conducted a survey of 2,000 US consumers with a household income of more than $25K. We found that almost half of respondents have had their data compromised, 89 percent no longer trust their data is safe with a company and a mere three percent feel data security practices in the US are sufficient.

Furthermore, shifting perceptions of data security have even begun to impact consumer spending decisions. Our survey found that a majority of Americans decide where to shop and how much to spend based on a brand's security practices, with nearly 80 percent reporting their spending habits have changed based on how secure they perceive a brand to be. The research also found that 83 percent will stop spending with a business for several months following a data breach and more than a fifth (21 percent) of consumers will never return to a brand that's been breached. In addition, the survey found that 45 percent will spend less with brands perceived to have weak data security. These findings underscore that brands should and will be held accountable for the frivolous management of data, and should serve as a wake up call for retailers around the world.

Resolution! Tread Carefully

For any retailer, the changing sentiment around consumer data security should be taken seriously. In today's competitive commerce landscape, it'll be more important than ever for brands to address and resolve all concerns around data security in order to remain in their customers' good graces. But what would make consumers feel safer? According to our research, 42.2 percent want companies to receive regular security audits, 31.2 percent want brands to forgo requiring social security numbers for transactions and 23.3 percent want businesses to be required by law to protect their data.

For businesses that have been hacked, there is a silver lining. Consumers can be encouraged to forgive a lapse, but it comes at a price. In order to gain back trust, 41 percent of consumers say they want the brand to admit responsibility and take steps toward improving security efforts, while 26 percent would prefer a third party to confirm the company is secure before spending with them again. 21 percent go an extra step further and want companies to announce PCI or GDPR compliance to earn back trust. In total, 88% of consumers require businesses to make additional investments in security after they've been hacked.

With cybercrime at an all-time high, and consumer trust at an all-time low, retailers must understand the consequences of poor data security practices. As consumer sentiment continues to shift, it'll be critical for retailers to invest in the right solutions to protect consumer data and remain compliant, while understanding the appropriate steps to take in the event of a breach.

About the Author

James Barham is a founder and CEO at PCI Pal, a secure payments provider to contact centers. He is a new business and relationship sales leader with a highly successful track record of building businesses and teams selling into both SME and Enterprise markets. A board level, commercial professional with full life-cycle experience of product development, go-to-market release, corporate sales negotiation, service delivery, and operational management of that life-cycle.

Website: https://www.pcipal.com/us/

LinkedIn: https://www.linkedin.com/in/james-barham-0102905/

Deception Technology for Active Defense: Changing the Game on Attackers

by: Carolyn Crandall, Chief Deception Officer, Attivo Networks

We live in an increasingly interconnected world and have created an on-demand society that expects instant access to information along with the ability to conduct business at any place and at any time. New technologies that provider faster services and improved economics are seen within new cloud architectures and the Internet of Things (IoT) is growing at an unprecedented pace—so much so that IoT devices are now already outnumbering the human population and will likely be in the operations of over 50 percent of companies in 2019. It's an exciting time from a consumer perspective, as well as from a tech industry perspective. But with innovation comes new challenges—particularly when it comes to security.

The threat landscape is changing as innovation outpaces traditional cybersecurity solutions and attackers are proving they can easily bypass perimeter defenses. The fight against intruders is growing more sophisticated and has moved inside the network. Organizations without proactive, in-network security will find themselves unprepared to deal with adversaries who use advanced attack methods or that exploit weaknesses in human behavior.

Perimeter Security is Important—but It Isn't Enough

Explosive growth in the number of internet-connected devices has broadened the threat landscape, providing attackers with countless new devices and architectures to exploit. While it's tempting to try to address this problem with advanced endpoint protection (EPP) and next-gen firewalls, significant risk remains if they are not coupled with detection controls to identify threats that have bypassed perimeter defenses or result from an insider or supplier who gains privileged access.

Organizations must adjust their security controls to address today's advanced attacker and the evolution of attack surfaces. Deception is an approach that has been used for millennia in military, sports, and gambling to outmaneuver the adversary. Organizations are now rapidly deploying deception technology within cybersecurity for a valuable, proven solution that allows them to quickly and accurately detect in-network threats. This doesn't mean that traditional cybersecurity tools should be discarded, but rather augmented with tools that provide early detection, reduce dwell time, and provide intelligence to better understand one's attacker. Adding deception-based detection to the security stack will also provide visibility into whether security tools are working reliability, as well as high fidelity alerting when an attacker is successful in bypassing them. A comprehensive deception solution that includes network, endpoint, application, Active Directory, and data deceptions can be extremely powerful in derailing attacks accurately and efficiently.

The unfortunate truth is that many organizations are strictly reactive to attacks, unable to gather threat or adversary intelligence to understand the attacker and prevent them from successfully spreading or returning. Deception technology addresses these issues by implementing an active defense strategy with wide-ranging impact.

Deception Arms Defenders with Improved Adversary Intelligence

Put simply, deception technology provides better detection against better attackers, as well as the adversary intelligence required to respond to an attack, shut it down, and make sure it is eradicated and cannot successfully return.

One of the most valuable things that deception does is reduce dwell time, or the amount of time that an intruder spends inside the network before detection. This prevents the threat actor from camping in the network and reduces exposure. Additionally, once an attacker enters the deception environment, the system will track their movements, identify tactics, techniques, and procedures (TTPs), and gather indicators of compromise (IOCs), providing valuable threat and adversary intelligence.

Deception also provides visibility into exposed credentials, misconfigurations, and network device changes that create increased security risk. This allows for ongoing assessment of risk related to mistakes, policy violations, and unauthorized device access.

Outmaneuvering Attackers with an Active Defense Strategy

Any game of strategy requires both offensive and defensive strategies. Applying an active defense approach to cybersecurity is critical for outwitting today's advanced attackers. Prevention devices like firewalls, IPS/ IDS, or antivirus are passive and reactive. By contrast, deception technology deploys authentic and attractive decoy docs, traps, and lures to proactively misdirect and engage attackers. By applying a matrix of decoys mimicking servers, endpoints, applications, credentials, mapped shares, data, and other items that appear as desirable targets, the attackers will be attracted into investigating or engaging, and in doing so will reveal themselves. In this way, deception turns the table on attackers by forcing them to be right 100 percent of the time as they move through the network, leveling the playing field.

The addition of deception increases the odds of an attacker making a mistake as they cannot tell real from fake—a strategy that will also increase their costs as they are forced to start over or seek easier targets. Increasing the complexity and cost of attack is a significant deterrent for attackers.

An Active Defense won't stop at detection. Stopping an adversary is critical, but doing so without knowing where they started, how they are attacking, or what they are after will leave an organization ill-equipped to ensure the attack is eradicated and can't successfully return. To achieve the value of an Active Defense, one must also be able to analyze attacks, run forensics, and be able to share information so that all security controls can work together in derailing any attack.

Deception-Based Active Defense for Actionable and Confident Incident Response

An alert is not helpful when overlooked. Alert fatigue is a genuine problem for cybersecurity professionals who constantly find themselves frustrated from chasing down a barrage of false positives. Given that deception technology is engagement based, alerts are substantiated and actionable. These high-fidelity alerts are augmented with root cause information that includes forensics, threat intelligence, and correlation of relevant data.

In advanced platforms, native integrations facilitate information sharing and streamline incident response for automated blocking, isolation, and threat hunting allowing security professionals to focus their efforts on only credible, verified threats or policy violations. The accuracy of these alerts combined with automations eliminates the need for incremental manpower or skills training. Organizations will now achieve not only confidence in their alerts but also more efficient and effective use of their existing cybersecurity personnel.

The Weakest Link May Be Within Your Supply Chain

Supplier security breaches are at an all-time high and have been the underlying cause of many of 2018's breaches. In addition to validating whether internal security controls are working reliably, deception provides a critical resource in detecting employee, contractor, and supplier policy violations and nefarious actions. With privileged access comes greater risk and the need for accurate and substantiated tracking of unauthorized access or activities. Deception records and alerts on any engagement with a decoy or attempts to use deception credentials. There is no production value for employees or third parties, so each engagement-based alert requires immediate attention without need for behavioral or traffic analysis.

Ongoing Security Control Assessment and Compliance

Deception technology plays a crucial role in pen testing and is now commonly used to validate security resiliency and reporting that can be used for audits and compliance. Proving the ability to detect the Red Team and record their actions can be crucial in demonstrating compliance. Additional visibility tools are also useful for ongoing assessment of credential exposure, network device changes, and attack lateral movement understanding. Decoy documents are useful for security teams looking to track what documents adversaries are targeting and the geolocation of where they are opened.

Deception Has Become An Indispensable Part Of Cybersecurity

The adoption rate of deception technology is soaring due to its effectiveness as a tool for early detection, adversary intelligence, and creating an active defense to outmaneuver an attacker, with Gartner estimating that the market share for deception technology will exceed $2 billion by 2021.

Deception provides non-intrusive detection effective in identifying external, internal, and third-party attacks throughout the attack cycle, including reconnaissance, credential harvesting, and lateral movement. The solution also provides adversary intelligence that provides organizations with a better understanding of attack origin, method of attack, and intruder intent.

Preventing all cyber intrusions simply isn't possible. Deception technology plays a critical role in changing the game on attackers by empowering organizations to find attacks that have bypassed perimeter controls early, regardless of the attack method or attack surface. This combination of factors makes modern deception technology an effective and essential tool for deflecting, understanding, discouraging, and defending against the most sophisticated adversary.

About the Author

Carolyn Crandall, Chief Deception Officer at Attivo Networks. Carolyn is a technology executive with over 25 years of experience in building emerging technology markets in security, networking, and storage industries. She has a demonstrated track record of successfully taking companies from pre-IPO through to multibillion-dollar sales and has held leadership positions at Cisco, Juniper Networks, Nimble Storage, Riverbed, and Seagate. Carolyn is recognized as a global thought leader on technology trends and for building strategies that connect technology with customers to solve difficult information technology challenges. Her current focus is on breach risk mitigation by teaching organizations how to shift from a prevention-based security infrastructure to one of an adaptive security defense based on the adoption of deception-based cyber warfare. As the Chief Deception Officer at Attivo Networks, she is an active speaker on security innovation at CISO forums and industry events. She has been a guest on Fox News and recently presented at the CSO50 Conference, ISSA International, NH-ISAC, and Santa Clara University, and has hosted multiple technology education webinars. She is also an active blogger and byline contributor.

Six Essential Questions About "ePrivacy"

by Alex van der Wolk, Privacy + Data Security Group Global Co-Chair, Morrison & Foerster

In the realm of privacy and personal data, 2018, thus far, has been all about the General Data Protection Regulation (GDPR). We have seen more talk about consent, privacy notices, access requests and data protection officers in this year than we've seen in the last decade. For many, the GDPR has meant a substantial investment and reform of their business practices. I would love to say that that's it, but the truth unfortunately is that there is a tail to the privacy reform which not everyone may be aware of. That tail is the new EU ePrivacy Regulation that governs certain forms of marketing and the use of cookies and other online technologies. Here are six things everyone should be aware of.

1. What is this ePrivacy all about? Unlike GDPR, which regulates everything that has to do with personal information, ePrivacy has a more narrow, yet more specific scope of application. ePrivacy regulates certain forms of digital marketing, such as email, but also SMS and soon possibly also marketing via messenger services such as Whatsapp. But that's not all. All the cookie pop-ups you've been seeing on websites over the years? That's also ePrivacy. And in that domain the requirements are to be expanded also (think device fingerprinting, pixel (re)targeting and any other technology facilitating online tracking and conversion). And then there's a new area ePrivacy is set to regulate, namely where digital marketing intersects with "brick and mortar", such as beacon advertizing, wifi tracking, bluetooth marketing – technologies that rely on the proximity of devices.

2. But doesn't GDPR already cover all of this? Well, yes and no. The title ePrivacy may be a bit off-setting here. Unlike GDPR, which applies to anything that has to do with personal information (regardless of the technology used), ePrivacy rather regards just the technology. In fact, for ePrivacy, it doesn't really matter whether personal information is at stake or not. The mere use of a covered technology may already qualify you for ePrivacy applicability. This also highlights the real tricky part about all of this: it is very well possible that ePrivacy and GDPR apply both at the same time. If you engage certain technology that is covered by ePrivacy AND that use also involves personal information, you may have to comply with both ePrivacy and GDPR.

3. So is ePrivacy just about getting more consents? Consent certainly is a firm cornerstone of the ePrivacy Regulation. Most of us are familiar with the current consent (opt-in) requirements for email marketing and the use of cookies on websites. This will remain in place. However, in order for consent to be valid going forward, it is unlikely companies will be able to (continue to) rely on implied or inferred consents. Like GDPR, ePrivacy will require consents to consist of a "clear affirmative act" from the individual. So, for example, in the context of cookies, relying on the continued use of a website to constitute acceptance of cookies is unlikely to be sufficient anymore.

Speaking of cookies, the ePrivacy Regulation may also contain a specific prohibition on cookie walls: denying access to a website, service, or functionality when the user does not provide consent will not result in valid cookie consent. And once any consent is obtained, the ePrivacy Regulation will likely require companies to remind the individuals of the option to withdraw consent at periodic intervals of either six or twelve months.

But it is not just about more consents. For example, the legislative proposals also suggest imposing an obligation on companies to offer online privacy settings (such as privacy dashboards) through which users can set and manage their online privacy preferences. Building such privacy dashboards would not only be a costly affair for any company, but could bring along a host of other issues. This may be one of the reasons that it is still in flux whether this obligation will make its way into the final text of the ePrivacy Regulation.

4. Does ePrivacy say anything about marketing phone calls? Yes, the ePrivacy Regulation will also cover telephone-based marketing. The legislative proposals suggest that voice-to-voice calls should only be allowed if the recipient has not opted out. This doesn't necessarily suggest an opt-in for marketing calls, but it does make sure that individuals have an opportunity to un-list from being approached by phone for commercial purposes. Many EU countries currently already provide for a similar requirement. In addition, companies conducting voice-to-voice calls may also have to adopt new transparency tactics, such as displaying their calling numbers and using a specific code or prefix identifying the call as a marketing call.

5. So what are the risks? Like GDPR, the ePrivacy Regulation will also bring about substantially higher fines. The legislative proposals mention fines that could run up to 2% of a company's total worldwide annual turnover or €10 million (whichever is higher).

However, unlike GDPR, the ePrivacy rules don't mind where a company is established, but rather where the individuals (the recipients of emails, visitors to your website, etc.) are located. So even if your company has no physical presence in the EU, the ePrivacy Regulation may still apply, particularly if you market to individuals in the EU, or use cookies and/or similar technologies on their devices.

6. Where do we go from here? The ePrivacy Regulation is still a work in progress. It is uncertain when it will be finalized, but the latest prognoses are for end of 2018/early 2019. What is certain is that once

ePrivacy is finalized, companies will have a one-year transition period to implement the new rules. Companies are advised to start their ePrivacy compliance programs on time.

About the Author

Alex van der Wolk is the global co-chair of law firm Morrison & Foerster's Privacy + Data Security Group. Based in Brussels, he focuses on data protection information/communications technology law and advises global companies on data protection strategy and compliance governing all aspects of information management. Alex can be reached online at avanderwolk@mofo.com and on Morrison &

Foerster's website: https://www.mofo.com/people/alex-van-der-wolk.html.

A New Approach to Secure Mobile Banking Apps

By Mark Noctor, VP EMEA at Arxan Technologies

By the end of 2018, nearly all financial institutions will offer mobile banking services. According to a survey of 706 financial institutions in seven U.S. Federal Reserve districts[26], top business reasons for embracing mobile include retaining existing customers, meeting competitive and cost pressures, attracting new customers, and projecting market leadership in technology. What this survey also demonstrates is that the number one barrier is "security concerns".

The Fear of Mobile Banking Apps

With mobile banking apps holding personal data such as payment card accounts, addresses and other various personal details. It's not a surprise that usage rates are only at 20% or less across 56% of responding institutions with just 8% reporting usage rates over 50%. However, consumers have every right to fear for their personal data due to insufficient security in mobile banking with potential exploits in the app code being easy to expose through reverse engineering. Furthermore, not only does a mobile banking breach affect personal data and damage trust, it can also cause significant brand damage resulting in lost revenue, increased cost to address the breach, and other liabilities.

[26] Federal Reserve Bank of Boston, Mobile Banking and Payment Practices of U.S. Financial Institutions, Dec. 2017.

No Single 'Magic Bullet' Solution

As expected, and for good reasons, financial services organisations comprise one of the best protected sectors against digital threats. However, there is no single 'magic bullet' solution to do it all. Mobile presents numerous disparate threats, requiring different technologies, solutions and processes. Mobile app security requires a multi-layer approach to secure the whole protocol stack but, despite this being a large issue, it is not uncommon for discussions about mobile banking apps to focus on the small set of externally provided safeguards such as device fingerprinting, multifactor authentication and encryption to protect sensitive data.

Rethinking Mobile App Security

A new approach has been introduced which provides three transformational benefits for securing mobile banking apps:

- The first benefit is to prevent reverse engineering and tampering, which could lead to breaches and app data theft, by hardening mobile apps after code is complete with a system of embedded safeguards
- The second benefit is stopping API compromises and theft of intellectual property or personal identifiable information with comprehensive data and key encryption using white-box cryptography
- The final benefit is that security teams can stay ahead of app threats and vulnerabilities with the ability for each protected app to "phone home" and provide real-time threat visibility and analytics data.

This new approach adds security functionality and mobile code hardening just once, after the code is finished. By doing this, zero trust is assumed in all devices running the app whether inside or outside the traditional perimeter. Code segments, known as 'guards', provide a high level of security awareness, detection, protection and security event data collection for analytics when an app is attacked. Once the guard network is created, follow-on protection for further app releases will need minimal effort due to the automated re-deployment of app hardening and safeguards to each new revision of code.

Real Time Visibility and Analytics

There is now valuable intelligence into what happens to an app after it's deployed into the wild. This actionable data means that an app's behavior can be changed whilst under attack. A positive element of this is that it has the ability to identify the most common attack vectors and target help developers and business stakeholders so that they make better decisions regarding how and when to adapt their app's security.

Learning Points

It's obvious that there is an urgent need for stronger app security with mobile banking apps currently being exploited. Banks and other financial institutions do not have the real time visibility to monitor the security status of deployed apps continuously, and such a data void is a huge risk as it could lead to numerous hacks and breach of personal data. Financial institutions should follow the steps mentioned in this piece to mend these errors and avoid losing both valuable data and customer trust.

About the Author

Mark Noctor is Vice President of EMEA for Arxan Technologies and has been involved in sales and business development for US High Tech businesses for 20+ years. For the last seven years, Mark has led the growth of Arxan's business in the EMEA region, building relationships with multiple FTSE 100 companies and House hold European names. Arxan Technologies is the leading provider of application protection technology and protects apps across the world in over half a billion devices including financial services, healthcare and gaming.

Streamlining RMF Accreditation to Speed Deployment of New Defense Technologies

By virtually eliminating the STIG hardening, months can be saved in the RMF accreditation process

Government agencies are not known for moving quickly, and the RMF accreditation process is a prime example. For defense contractors and integrators tasked with developing new technologies for the Department of Defense (DoD) and other government agencies, this step alone can take 9-12 months or longer.

The glacial pace of accreditation is due to the manual nature of the review process tasks, as well as significant documentation and system hardening required to meet security policy mandates. Without this step, projects cannot move to Authorization to Operate (ATO). In short, any delays impact deployment of new defense technologies in the field.

Fortunately, new automated software tools are eliminating weeks, if not months, from the RMF accreditation process by virtually eliminating the time of the initial hardening while also providing the required documentation. By doing so, technology integrators can significantly reduce the time to build, test, and deploy new technologies in STIG-compliant environments.

RMF Accreditation

The DoD introduced the Risk Management Framework (RMF) in 2014 to assist federal agencies to better manage risks associated with operating information systems.

As part of this process, systems must be hardened to standard Security Technical Implementation Guide (STIG) benchmarks. The STIGs provide configuration specifications for operating systems, database management systems, web servers and network devices used by government agencies.

The problem is STIGs are long and detailed. Often containing hundreds of pages, adhering to or upgrading software or systems to a particular STIG has been a highly specialized manual process that can take many weeks to accomplish. In addition to the significant time involved, it requires well-trained engineers that are skilled in the technical system, operating system policies and security guidance.

According to Brian Hajost, president of SteelCloud and an expert in automated STIG compliance, there are many misconceptions and confusions surrounding system hardening.

Only in rare instances do applications have specified STIGs. One example is Microsoft Word, which when used in secure environments must be hardened. Instead, most STIGs apply to the "application stack," which includes the operating system (Windows, Linux) the application is built upon as well as web browsers, databases, and other components required for the application to function.

So, when an application is implemented in a STIG hardened environment (i.e. changes have been made to the underlying operating system, for example) it inevitably runs into conflicts that can cause the application to "break." When the application is an electronic document, that may be problematic, but for a military firing system, it can be a matter of life and death.

"Most applications are typically developed and tested in non-STIG environments," explains Hajost. "So, when they are implemented in a hardened environment, they can break." These failures are unique to each application stack and sorting them out can take weeks or months for each application."

It is for this reason that RMF accreditation requires hardening the system as well as providing significant documentation of the hardening as well as details of all CAT 1/2/3 controls – a categorization of the degree of security risk.

Automating the Process

Given the manual nature and expertise involved in hardening and documenting all changes, it would be easy to assume that multiple, competing software solutions already exist. This is not the case.

Vulnerability scanning software is available that can compare generic STIG signatures to identify controls. This only serves to highlight the problem areas but does nothing to resolve issues.

Scripting automation tools can be used but are expensive and not purpose-built for STIG compliance or accreditation. Because they do not produce documentation, these tools must often be used in conjunction with vulnerability scanning software.

Even if both are used, however, these options do not make changes to controls that are specific to the application stack involved. Fortunately, more complete solutions now exist that include this type of automated remediation.

ConfigOS from SteelCloud, for example, hardens all CAT levels (1/2/3) in about an hour, including producing a domain-independent XML signature and documentation of all required waivers. In this step alone, weeks, or months of manual work is eliminated.

Once developed, the encrypted XML signature can be securely used across the DoD in all networks and domains, without changes to existing security or infrastructure. The signature can also easily be included with applications as they are transferred to disparate infrastructures from one mission partner to another.

Using the signature, scanning, remediation, and compliance reports are accomplished in about a minute. Because STIGs are updated every 90 days, the software also simplifies updating systems in production as well.

The product has already been licensed by most of the largest defense contractors, as well as agencies within the DoD and DHS.

“You basically have to mold these controls, and there are hundreds of them, around your application stack,” says Hajost. “Essentially you have to figure out what will ‘break’ the application and correct the control – and software can automate that process.”

Hajost says the DoD will not even authorize the issuance of an authority to operate (ATO), for example, of systems with an unmitigated CAT 1 vulnerability except under extreme and rare circumstances. This can mean sending a project back into development to address the issue.

“Now a ‘fix’ that would have cost $500 in the initial development can cost the government many thousands of dollars,” says Hajost, adding that is the primary reason to address STIG hardening as early in the DevOps process as possible, even before accreditation. “We estimate CAT 1's cost the government and the DoD thousands of dollars, per application, per year to maintain.”

As for CAT 2 and CAT 3 controls, they must also be hardened, or – if there is a reason the risk might not apply – waiver requests must be submitted for review and acceptance by accrediting authorities.

“We have seen examples where developers have even said, ‘we're just going to waiver all the CAT 3's because we don’t have the time or money to detect and remediate them,’” explains Hajost.

However, with the speed of automated identification and remediation, more time can be shaved off timelines by keeping waiver requests to a minimum.

“If you can use software to address all the CAT 2 and CAT 3 controls automatically in a very short period of time, you can reduce the number of waivers to the absolute minimum required. This saves on costs, reduces the amount of documentation and ultimately speeds certification.”

While many in government accept long delays as a fact of life, shaving months from the RMF accreditation process ultimately speeds the implementation of weaponry, communication and other systems. With this in mind, defense contractors and other technology providers should consider hardening systems in the accreditation phase and, when possible, even during initial development.

About the Author

Jeff Elliott is a Torrance, Calif.-based technical writer. He has researched and written about industrial technologies and issues for the past 20 years. For more information about ConfigOS from SteelCloud please contact them at 703-674-5500; or visit them online at www.steelcloud.com.

Why Zero Trust is The Answer to Securing Healthcare Data

It's high time the healthcare industry started taking data security more seriously.

by Narendran Vaideeswaran, Product Marketing Manager, ColorTokens Inc

Like many other major industries, the healthcare industry too is under constant attack from cybercriminals. Healthcare organizations have a huge repository of patient data like name, phone number, email address, and medical history. Apart from personal information, they also store payment details which hackers can misuse for monetary gains.

Recent attacks on healthcare organizations have shown that cybercriminals are using sophisticated techniques to hack into secure networks and exfiltrate data. While cyberattacks are one part of the problem, the healthcare industry also suffers from a huge percentage of internal threats.

These threats could be employees with malicious intent or unintentional actions by employees which directly compromise an attribute of a security asset. If the healthcare industry wants to protect itself, both these threats must be prevented without compromise.

State of Security in The Healthcare Industry

Due to sensitive nature of the data that is at stake, the healthcare industry in the US must comply with HIPAA (Health Insurance Portability and Accountability Act of 1996). The legislation recommends a set of guidelines which ensure that healthcare organizations implement physical, network, as well as process security. However, it is becoming increasingly evident that limiting cyber security to just HIPAA compliance is not enough anymore.

According to the Verizon's 2018 Protected Health Information Data Breach Report (PHIDBR), 70% of incidents involving malicious code were ransomware infections and a whopping 58% of incidents involved insiders.

While an internal breach could be just employee curiosity and may not always be malicious, it leaves sensitive data open to misuse. Unauthorized internal access to patients' personal information provides a convenient means to commit fraud of various types. Regardless of the intent of the breach, securing data should be of prime concern to any healthcare organization.

Taking a Zero Trust Approach to Security

Most healthcare organizations have traditional cyber security systems which rely on protecting the perimeter using firewalls, while assuming all communication within the network is safe and authorized.

Threat actors are taking advantage of this assumption and using sophisticated attack vectors – like phishing, fileless malware, ransomware, zero day attacks – to enter the network. Once inside, they're able to remain undetected for months since security operators have very little visibility of East-West traffic. Apart from hackers, the high percentage of internal threats from employees is also looming security concern.

In the event of a breach, a healthcare organization stands to lose not only their patients' personal and financial details but also private and sensitive data like:

- Medical history
- Social Security/National Insurance numbers
- Medical device or serial numbers
- Biometric data
- Full facial photographic images or images that have unique identifying characteristics
- X-rays and diagnostic images

To defend against external and internal threats, the most reliable course of action is to implement a zero trust security architecture. The zero trust security concept is based on the premise that no connection is trusted unless it has been explicitly allowed.

Adopting zero trust security marks a paradigm shift from reactive to proactive security, wherein the goal is to prevent the breach rather than 'react' after it has happened.

How Zero Trust Security Can Make a Difference

To create a zero trust network, healthcare organizations cannot depend only on network level segmentation which uses VLAN/ACLs and internal firewalls. Maintaining access control lists and updating thousands of firewall rules on a regular basis in a dynamic business environment is cumbersome, operations-intensive, and error-prone – not to mention the high cost of maintenance and upgrades. Lack of East-West traffic visibility is also a major issue with hardware centric segmentation.

Zero trust security, on the other hand, can be implemented using software-defined micro-segmentation, which provides organizations with complete visibility of all network traffic across bare-mental and hybrid cloud environments. Essentially, healthcare organizations will be able to segment individual users, applications, and workloads to drive down intent-based security policies to the host level.

This means that every single person or application which connects to the organizations network – be it an employee, service provider, third-party vendor, or insurance partner – can be granted specific access based on the security policies of the organization. Any attempt to access unauthorized data by a prospective threat actor is immediately prevented and flagged, drastically reducing the attack surface.

To prevent employees from accessing sensitive data, healthcare organizations will be able to enforce strict security policies that define and limit the access of individual employees. The visibility provided by software-defined micro-segmentation will allow the security operators to record any deviation in behavior, which can then be investigated and used to fine tune the security policy.

Cybercriminals have evolved to develop advanced malicious code that can circumvent perimeter security and remain undetected. Attack forensics are also confirming that hackers are using sophisticated mechanisms to exfiltrate data. Unless the healthcare industry is willing to take a serious look at the inherent vulnerabilities of traditional network security systems, sensitive patient data will remain at risk.

About the Author

Narendran Vaideeswaran, Product Marketing Manager, ColorTokens Inc. Narendran Vaideeswaran is a product marketing manager at ColorTokens Inc and handles the company's security portfolio. A technology enthusiast, he has worked in the IT and security industries for over a decade in both technical and marketing roles. Naren can be reached online at narendran.v@colortokens.com and at our company website https://colortokens.com/

The Modern Business Has No Perimeter

IF THE BOUNDARIES ARE EVER-CHANGING, WHAT DOES THAT MEAN WHEN IT COMES TO THE ENDPOINT AND USER BEHAVIOUR?

By Dr Jamie Graves, VP, Product Management, Security Analytics, ZoneFox

According to Haystax Technology, in 2017, 90% of organisations reported feeling vulnerable to insider attacks -- up from 64% in 2015. This looked set to rise to 99% in 2018, thanks partly to the rise in risk from regular employees too. These stats tell us that a cyber strategy focused on protecting the perimeter is now futile -- employees have become the perimeter and they're always on the move, morphing said perimeter by logging onto the network from different devices and locations.

Indeed, as 2018 reaches its final quarter, these predictions seem increasingly accurate. After all, when contemplating the various headline-grabbing cyber incidents from the past few months -- of which there's certainly been no shortage -- the truly jaw-dropping ones have tended to involve employees, with motivations ranging from ideology, revenge, and cold hard cash.

An Unholy Trinity

2018 saw Apple crowned as the first trillion-dollar company, closely followed by Amazon -- but that's not all these technology giants shared in common. In July, news broke that Apple suffered an insider attack after a former employee stole data relating to its autonomous driving project before attempting to flee to China and eventually being arrested by the FBI. September saw Amazon staff caught selling customer data to third-parties in the US and China.

Evidently, trillion-dollar valuations mean not only a lot of customer data, but also a large organisation to hide illicit activity within. Both of Apple and Amazon's insider threats came after Tesla's, whereby a past employee tampered with Tesla's code for autonomous driving software and exported highly sensitive data to unknown third-parties. It transpired that the prime motivation behind the incident was an act of vengeance after being denied a promotion.

Of course, insider threats abound in businesses of all sizes, not just technology behemoths. Earlier this year, a report from Cybersecurity Insiders revealed that two-thirds of US companies now believe that insider threats are more likely than external attacks. This is because, thanks to the ubiquity of shadow IT

-- a term which describes the use of IT systems within an organisation without the approval, or even the knowledge, of the IT team -- employees at all levels can now access huge swathes of sensitive and business critical data.

Prevention is Better than Cure: The End of an Era

But why is this happening? Without a doubt, organisations of all shapes and sizes have never been more vulnerable to attack, thanks to a dramatic increase in entry points. In addition to the countless connected devices that employees carry around every day -- to and from work -- the Internet of Things (IoT) is swiftly expanding the scope for an attack. Consequently, the modern business has no perimeter -- or, rather, its staff serve as the perimeter. This happens because companies all over the world still haven't got appropriate protection in place that flags insider threats before they cause serious damage.

Of course, despite the recent headlines, insider threats are not always malicious and purposeful. The term might conjure cloak and dagger espionage, but 'insider threats' covers myriad internal vulnerabilities. These can range from accidental errors and compromised credentials stemming from a socially-engineered data breach, courtesy of a lack of basic cyber security hygiene, all the way through to malevolent insiders. In fact, an McAfee report found that nearly half of the data breaches studied were caused by employees, contractors, or suppliers.

For contemporary organisations, with the boundaries ever-changing, this must lead to an overhauled approach to endpoint security and user behaviour analytics. Traditionally, cyber security companies strived to prevent outside attackers from penetrating a company's network, in line with the mantra of the past that prevention is better than cure. Now, however, it's not a case of if an organisation will get breached but when. As such, cyber security firms are now focusing their attention inwards, rather than towards a company's boundary -- representing a seismic shift in the way IT departments and the C-suite alike approach the integrity of their organisations.

Productivity is Key

For IT leaders, the temptation can be to double down on strict security policies, introducing increasingly obtrusive measures in a bid to combat cyber crime. However, there's no use implementing processes that ultimately make it harder for employees to work efficiently. Undoubtedly, the business will suffer as a result, thanks to stifled innovation and experimentation. Instead, rather than seeking to completely eliminate breaches, it's just as important to rapidly identify breaches and stop them turning into full-blown disasters.

This is where the power of user and entity behaviour analytics (UEBA) and machine-learning becomes most apparent. These technologies rapidly get to know a business and identify security risks from the inside, so that they can spot suspicious behaviour such as unusual out-of-hours access -- think files transferred to atypical locations, from anomalous countries. Should anything suspicious arise -- for

example, an intern accessing the CFO's files at 3am from an IP outside the office -- the company in question will be alerted to the relevant risky or uncompliant behaviour.

Still, technology alone is never enough. Cyber crime used to be an elite activity, carried out only by those with the appropriate coding skills, often targeting stationary endpoints. These days, with everyone carrying mini-computers in their pockets, anyone can hire a hacker or try to sell company data from the inside. Consequently, when humans are the perimeter, -- human security teams empowered by machine-learning technology prove to be a formidable threat hunting force.

To this end, a robust company-wide education programme that encourages an open culture of security is vital for keeping data secure. As well as regular and interactive staff training, even retro approaches such as posters stuck onto office walls can help. Above all, the blame culture of IT security needs to change, so that insider threats can be spotted and managed before they cause extensive damage. Organisations that don't silo security -- instead fostering a collaborative approach between IT, the C-suite, and all other employees, educating and making everyone accountable -- will reap the most rewards and stand the best chance of safeguarding themselves in this perimeterless world.

About the Author

Jamie is the VP of Product Management, Security Analytics, at ZoneFox – a company recently acquired by Fortinet – which focuses on detecting insider threats and other fraudulent activities by examining human behavior using machine-learning. He spun the company out of his PhD from Edinburgh Napier University. https://zonefox.com/

A CISOs 'playbook': Practice How You Fight

by David 'Moose' Wolpoff, CTO and co-founder, Randori

Despite CISOs and organizations making huge investments in security – with more tools and solutions on the market than ever before – high-impact and high-profile breaches continue to fill headlines every day. By 2020, organizations will spend more than $124 billion globally on security[27], but more money alone cannot and will not fix the issues we face. To do that will require a shift in perspective, away from the false belief that it is ever possible to stop every attack and fix every gap, and instead towards one grounded in practice and readiness.

For 14 years, companies and government agencies have paid me to hack into their networks. During this time, despite advances in technology, the basic ways attackers get in to these organizations has not changed much, with phishing, malware and basic exploits remaining the most common attack methods. The question should be asked, why do we continue to fall victim to these same basic attacks?

The problem as I see it, is that while we have thrown more money at security, most organizations continue to lack the dedication needed to address the fundamental knowledge gaps and process failures attackers rely and count on to succeed. Instead, organizations continue to reward and encourage those with defender mindsets. Because of this, it is far often easier for CISOs to purchase another tool than it is to invest in training or change long-held IT processes and procedures that could really move the needle. What's required is a shift in focus. Organizations need to adopt an attacker's mindset. While not always easy, making this shift could not be more essential.

To adopt an attacker's mindset is to align with the old adage, "know your enemy." Instead of focusing on building more defenses, enterprises that take an attacker's mindset focus on understanding the way hackers think, how they make decisions, and the techniques and procedures adversaries use to break into their environments. My experience has shown that these companies generally have a better understanding of the true risks they face and are better able to identify where they are most vulnerable.

[27] Gartner

CISOs at these firms are then often able to spend less, but in a more impactful way that ultimately translates to fewer breaches and greater ROI for the business.

Adopting an attacker's mindset is to approach security the same way a team would before playing in a big sports game. The Broncos would never play a big game without practicing beforehand, and neither should you. Whether you're a coach preparing for your team's next big game or a CISO developing an enterprise security strategy, the best plans are founded in a solid understanding of the enemy, and a deep awareness of one's own strengths and weaknesses to test, tweak and improve before battle. Whether it be sports or security, experience is the best defense.

Here are three important approaches CISOs can use to shift perspective and better prepare their organizations for the next attack.

Pretend you're The Attacker

Similar to scouting and studying an opposing team, security teams must be able to put themselves in the shoes of the enemy and view themselves from the outside looking in. What does your attack surface look like? What assets are most interesting or most valuable? From what points could one gain access to your network? By adopting a hacker mindset and viewing themselves through an attacker's eyes, CISOs and their security teams will be better informed to make decisions such as where to allocate budget, team and resources for the greatest impact.

Weaponize Your Home Field Advantage

Just like in sports, home field advantage is a real thing. There will never be a situation where a security team is working in enemy territory, so make sure you know your turf. Know and monitor your external and internal network, be able to identify anomalous activity and be ready, able and willing to use the tools at your disposal. Too often, organizations invest in security tools or monitoring solutions they have no idea how to use or no ability to monitor. Take advantage of your own turf by investing in tools that work well with the rest of your toolbox and the practice required to maximize its benefits. Anything you can't use or properly monitor is just getting in the way.

Never Stop Practicing

The sports analogy here goes without saying. The most important thing an enterprise can do, is routinely test their detection and Incident Response (IR) teams, as well as the processes in place in the event of a security incident. When it comes to IR plans, I'm a big fan of Mike Tyson's quote, "Everyone has a plan until they get punched in the mouth." While having an IR plan in place is an important step, practicing and understanding how teams respond under pressure is the only way to truly know if your organization is prepared and able to properly respond. When I've seen organizations fail, it was not because people didn't have a plan – it was because they never practiced it. Things rarely go according to plan, so being

able to to adapt and accommodate for things like knowledge gaps, miscommunication or poor training is critical. These types of things rarely jump out on paper but become instantly apparent in practice.

While no organization is or can be perfectly secure, those that accept this as a foundational belief and therefore focus and invest in testing and assessing their tools, processes and teams will be in the best position going forward. While most CISOs already know this, and many I know would agree, we will only begin to 'unstick' security if we can successfully convince the broader organization that changing perspectives is important. This is the biggest challenge facing CISOs today, and is by far the most important.

About the Author

David 'Moose' Wolpoff is co-founder and CTO of Randori. Moose is a recognized expert in digital forensics, vulnerability research and embedded electronic design. Prior to founding Randori, Moose held executive positions at Kyrus Tech, a leading defense contractor, and ManTech where he oversaw teams conducting vulnerability research, forensics and security efforts on-behalf of government and commercial clients. Moose holds Bachelor of Science and Master of Science degrees in Electrical Engineering from the University of Colorado, Boulder. Moose can be reached online at @RandoriSecurity and at Randori's website, http://www.randori.com/

AI and Machine Learning Must Be Used Strategically in Cybersecurity

by Dustin Hillard, chief technology officer, eSentire

Malicious actors have the upper hand. This is clear from the ongoing data breach headlines involving companies with talented and diligent security organizations. A successful adversary campaign need only find a single flaw in an enterprise defense, while security teams are dealing with the increasing complexity of more instrumentation, tools, data and alerts that are being pushed as the only way to protect against threats and detect successful intrusions.

The tech industry has responded with claims that AI and machine learning will save the day. In reality, though, they could actually exacerbate the existing problems and perpetuate the disadvantaged posture of security teams today. There are three common challenges associated with AI that can deteriorate defenses:

Challenge #1: More False Positives

Organizations have rapidly adopted AI to detect security issues, but so far the result has been an increase in alerts that security teams must add to workloads that are already maxed out. It is easy to build models that detect new potential threats, indicators of compromise or anomalous behaviors. On the surface, it appears that these provide additional security, but in reality, this just generates more false positives that distract overburdened security operations teams from seeing real threats.

Challenge #2: Generic Models

Though AI is touted as having the ability to detect complex new attack patterns, most AI systems actually only provide a small extension beyond previous rule- and signature-based approaches. AI is only as powerful as the data it is provided, and most implementations of AI distribute generic models that don't understand the networks they are deployed to and are easy for adversaries to evade. When pattern detection is static across time and networks, adversaries can profile the detections and easily update tools and tactics to avoid the defenses in place.

Challenge #3: Human-AI Breakdown

The majority of AI systems currently deployed serve up seemingly random scores and don't explain them. This leads to a breakdown in trust and understanding with the humans that need to consume and act on the results. When AI isn't able to support "sophisticated" detections with explanations that security analysts can understand, this adds to the cognitive load of the analyst, rather than making them more efficient and effective.

Using AI to Your Advantage

That's not to say AI and machine learning are useless in the fight against cybercrime. They can be powerful tools in improving enterprise defenses, but success requires a strategic approach that avoids the weaknesses inherent in most of today's implementations. There are three key tactics that will amplify the ability of security teams to work with AI, rather than adding to their problems.

Tactic #1: Aim for Fewer False Positives

An effective system requires an ambitious goal that reduces the security team's workload and automates investigation with a focus on the full adversary objective. Rather than detecting secondary aspects of adversary activity such as the tool used or the tactic employed, AI systems that uncover the core behaviors an adversary has difficulty avoiding will give security teams a small number of true business risks to investigate. Effective solutions should have very few false positives, generating fewer than 10 high-priority investigations per week (not the hundreds or thousands of events produced by current approaches).

Tactic #2: Understand the Environment

When security teams home in on the adversary's objectives, the bad actors are forced to shift their approach to better hide in the environments they attack. Adversaries traditionally have the advantage because they can profile an environment and avoid the detections in place. AI systems can gain the

advantage by understanding the environment better than the adversary. A system that understands the specifics of an environment can identify unusual behaviors with context that adversaries could only gain with complete access to the full (and constantly updating) internal data feeds that the AI system is provided to learn with.

Tactic #3: Grow Analysis Skills

To build trust, AI systems need to offer results that automate typical analyst workloads and explain the results. Over time, this accelerates the skill and experience development of humans who use AI tools. The talent shortage security teams face today means that AI tools must help fill skills gaps with automation but then also provide interpretability and situational awareness that will help grow the skills of security teams while also making day-to-day operations more efficient and impactful.

New Possibilities in Cybersecurity

In the face of unending network intrusions, organizations have adopted basic AI and machine learning technology to help detect threats. IT security teams can get back the upper hand by implementing AI and machine learning in a way that cuts down on the thousands of false positives. When this intelligent technology understands the specific network environment and shares results that build trust among human analysts, organizations will be able to act faster and more decisively against intruders.

About the Author

Dustin Hillard is the chief technology officer at eSentire. He leads the research and development of automating security expertise with adaptive machine learning. Dustin has published more than 30 papers about building systems that deliver business value via large-scale data processing and machine learning. Dustin Hillard can be reached online at https://www.linkedin.com/in/dustinhillard/ and at our company website http://www.esentire.com

Data Security Tops 2019's Intelligent Workplace Priorities

Author: Steve Marsh, VP of Product, Nucleus Cyber

Data security concerns have gone mainstream. As we approach 2019, it's not just CIOs placing a spotlight on data security: it has become a more pressing priority than ever before from the C-suite, government watchdogs, the media and consumers throughout the world. The trifecta of factors driving concerns include increased legal requirements and penalties for non-compliance, including the much talked about GDPR; the ever-increasing rise of cyberattacks targeting all corners of the globe; and data breaches that are hitting closer to home with the theft of personal and financial information of millions.

Enterprise Challenges to Data Security

In many ways, heightened awareness is a good thing. Protecting sensitive data in the workplace should be everyone's responsibility. However, the pressure is certainly on the C-suite to ensure that an appropriate strategy is in place, which also means that budgets must align with the purpose of appropriately protecting data. Making sure funds are correctly allocated can be tricky without intimate knowledge of the modern workplace and the IT solutions necessary to support it.

Today, the myriad of cloud-based collaboration technologies, many of which have consumer versions that users are familiar with, present our tech-savvy workforce with multiple ways to share data. If you were to look at your own environment, you would likely see that of the tools in use, some are sanctioned and managed by corporate IT, while others are not.

Shadow IT

Had this article been authored a few years earlier, data security for the intelligent workplace could be talked about in the context of users seeking out and using their own tools to share data if the IT provided solutions were more of a hindrance than a help. Called Shadow IT, it refers to "unofficial" IT tools being used within organizations.

The risk to data security posed by those tools led to the rise of Cloud Access Security Broker (CASB) solutions. In their basic form, CASB solutions detect collaboration tools, and others used within an IT environment, and apply policies restricting use within an organization.

Today, these types of solutions are regarded by many as a critical component for protecting enterprise data. Gartner expects that 60 percent of enterprises will have deployed this type of solution by 2020, as opposed to only 10 percent in 2017.

Thankfully, the current crop of collaboration tools available for IT to deploy have improved tremendously, so users are more inclined to stick to the rules for what they use. Still, even if you have managed to stamp out shadow IT risk within your organization, collaboration tools are not the only thing that we have to consider when securing data in the modern workplace.

The Mobile Workforce

In thinking about the nature of how people work today, the data we use no longer resides within the physical walls of a company. It sits on our laptops, tablets, mobile devices and in the cloud, and is accessed from an office building, home location, on a train while commuting, at a coffee shop, from a partner's warehouse, *etc.*

Now consider that over 70 million mobile devices are lost each year and lost laptops still account for a significant percentage of data breaches. How do we know that a breach is (or isn't) the fault of our user accessing sensitive data, while sipping on that mocha latte?

In many cases, it is not appropriate to allow users to openly access anything from anywhere on any device. The nature of the content and the context of use, even *via* sanctioned IT tools, must be considered in order to maintain data integrity and security.

File encryption for sensitive data if being accessed from outside the office is mandatory, as is restricting usage rights to data files. It's not difficult for IT to make a file "read only" or available only as a watermarked image. The latest generation of Data Loss Prevention (DLP) and rights management software enables many options for organizations.

As with CASB adoption, DLP and encryption technology deployment is on the rise, and increasingly, these three data security types are becoming more integrated solutions.

Content Discovery

If you've successfully stopped shadow IT and ensured that users are only accessing and interacting with files in a safe and secure manner, you've only won half the battle. Understanding the nature of content and where sensitive data is stored, and then assessing how to monitor it as a file changes over time, are critical next steps. This is where Artificial Intelligence (AI) and Machine Learning (ML) can make a significant difference.

AI and ML based technologies provide advanced tactics necessary for identifying and securing data. Applying appropriate classification and being dynamic enough to adapt protection and policies as files move through their collaboration lifecycle—without compromising user productivity—is essential.

Protect Data from The Inside And Out

These are a handful of internal considerations to successful data security, which must co-exist within a larger strategy that includes external tactics, such as perimeter defenses. Leveraging AI and ML powered solutions allow IT to move beyond basic collaboration to embrace and gain the benefits of a truly secure and intelligent workplace.

About the Author

Steve Marsh is the Vice President of Product at Nucleus Cyber and brings more than 20 years of product experience to Nucleus Cyber from Microsoft, Metalogix, start-ups and academia. He drives product management and product marketing to deliver first class customer experiences, strategic product roadmaps and key go to market messaging. Steve holds a PhD in Microelectronics and Materials Physics,and lives in the Pacific Northwest with his family.

Links

https://twitter.com/nucleuscyber?lang=en

https://www.linkedin.com/in/drstevemarsh

Watchguard Technologies 2019 Security Predictions

“Cyber criminals are continuing to reshape the threat landscape as they update their tactics and escalate their attacks against businesses, governments, and even the infrastructure of the internet itself,” said Corey Nachreiner, chief technology officer at WatchGuard Technologies. “The Threat Lab’s 2019 predictions span from highly likely to audacious, but consistent across all eight is that there’s hope for preventing them. Organizations of all sizes need to look ahead at what new threats might be around the corner, prepare for evolving attacks and ensure they’re equipped with layered security defenses to meet them head-on.”

1) Prediction: AI-Driven Chatbots Go Rogue

Description:

In 2019, cyber criminals and black hat hackers will create malicious chatbots that try to socially engineer victims into clicking links, downloading files or sharing private information.

As artificial intelligence and machine-learning technologies have improved over the past few years, automated chat robots have become increasingly common. Chatbots are now a useful first layer of customer support and engagement that allow actual human support representatives to address more complex issues.

But life-like AI chatbots also offer new attack vectors for hackers. A hijacked chatbot could misdirect victims to nefarious links rather than legitimate ones. Attackers could also leverage web application flaws in legitimate websites to insert a malicious chatbot into a site that doesn’t have one. For example, an attacker could force a fake chatbot to pop up while a victim is viewing a banking website, asking if they need help finding something. The chatbot might then recommend that the victim click on malicious links to fake bank resources rather than real ones. Those links could allow the attacker to do anything from installing malware to hijacking the bank’s site connection.

In short, next year attackers will start to experiment with malicious chatbots to socially engineer victims. They will start with basic text-based bots, but in the future, they could use human speech bots like Google Duplex to socially engineer victims over the phone or other voice connections.

2) Prediction: Utilities and Industrial Control Systems Targeted with Ransomware

Description:

Next year, targeted ransomware campaigns will focus on utilities and industrial control systems (ICSs). The average payment demand will increase by 6500 percent, from an average of $300 to $20,000 per payment. These attacks will result in real-world consequences like blackouts and loss of access to public utilities.

Ransomware has plagued the internet over the past five years, starting with CryptoLocker, the first really successful crypto-ransomware, and culminating with WannaCry, the first fast-spreading ransom***worm***. During these past years, cyber criminals have blasted out broad ransomware campaigns at everyone, looking to infect as many victims as possible while asking each for a relatively meager ransom.

However, over the past year hackers have shifted to targeted attacks that come with bigger payouts. Launching ransomware against organizations that offer critical services increases the odds that the ransom will be paid. Forty-five percent of all ransomware attacks in 2017 targeted healthcare organizations, like the NHS in the UK. In 2016, the Hollywood Presbyterian Medicare Center paid a $17,000 ransom to regain control of their computer systems, and other major ransomware attacks hit MedStar Health and Alvarado Hospital Medical Center, among dozens of others. Many U.S. cities were also hit with ransomware in 2017 and 2018, including Baltimore and Atlanta.

In 2019, cyber criminals will target public utilities and ICSs. These are vital services that have not yet been targeted by widespread ransomware attacks and therefore may not be as prepared for this type of attack. Cyber criminals know that any ransomware that can cause downtime to these services will get swift attention, allowing them to ask for considerably more money in return. This has the potential to cause blackouts and gaps in water and power services if these attacks are successful. To summarize, expect to see fewer ransomware attacks next year, but more focused attacks – specifically targeted towards utilities and ICS – with ransom demands increasing by 6500 percent.

3) Prediction: The United Nations Proposes a Cyber Security Treaty

Description:

In 2019, the United Nations will address the issue of state-sponsored cyber attacks by enacting a multinational Cyber Security Treaty.

There are many examples of alleged and confirmed cyber attacks launched by nation-states. The U.S. and Israel allegedly launched the Stuxnet attack. The Russian government has been accused of everything from DDoS attacks against Estonia and turning off the power in Ukraine to election and political hacking in the United States. North Korea, meanwhile, has allegedly attacked public and civilian organizations and infrastructure, targeted Sony Pictures and ostensibly caused billions in damage in the WannaCry attack. Many governments have blamed China for various cyber attacks focused on intellectual property, but the most recent "straw on the camel's back" is the Supermicro supply-chain attack, where the People's Liberation Army (PLA) has been accused of sneaking backdoors into servers sent around the world (though many dispute this story). These alleged attacks cost billions in damages and put supply chains responsible for 90 percent of computing devices at risk, showing that cyber attacks often cause enormous economic damage outside of their intended targets.

The growing number of civilian victims impacted by these attacks will cause the UN to more aggressively pursue a multinational cyber security treaty that establishes rules of engagement and impactful consequences around nation-state cyber campaigns. They have talked and argued about this topic in the past, but the most recent incidents – as well as new ones sure to surface in 2019 – will finally force the UN to come to some consensus.

4) Prediction: A Nation-State Launches a "Fire Sale" Attack

Description:

You may remember the fictional concept of a "fire sale" attack from the 4th Die Hard movie, in which a terrorist group planned a coordinated cyber attack against U.S. transportation, financial, and public utilities and communication systems. The terrorists meant to use the fear and confusion caused by the attack to siphon off huge sums of money and disappear without a trace. In 2019, we will see a version of this fictional attack become a reality.

As unlikely as this attack might have seemed in the late 2000s, many modern cyber security incidents suggest that nation-states and terrorist have developed these capabilities. Cyber criminals and nation-

states have launched huge distributed denial-of-service (DDoS) attacks that can take down entire countries' infrastructure and could certainly hamper communications systems. The U.S. government claims foreign actors have already been targeting and probing the defenses of public utility and energy systems. We've seen these nation-sponsored attacks targeting financial systems like SWIFT to steal millions. Nation-states have also used social media and other communication systems to poison public perception with fake news.

In summary, each of these individual types of attack are already possible. It's just a matter of time before some country combines many attacks as a smoke screen for a larger operation.

5) Prediction: Fileless, Self-Propagating "Vaporworms" Attack

Description:
In 2019, a new breed of fileless malware will emerge, with wormlike properties that allow it to self-propagate through vulnerable systems and avoid detection.

It has been over 15 years since the Code Red computer worm spread through hundreds of thousands of vulnerable Microsoft IIS web servers in an early example of a fileless worm. Since then, both worms and fileless malware have impacted networks worldwide individually, but rarely as a combined attack.

Fileless malware, which runs entirely in memory without ever dropping a file onto the infected system, continues to grow in popularity. Sophisticated attackers prefer this method because without a malicious file to scan, traditional endpoint antivirus controls have a hard time detecting and blocking fileless threats. This results in higher infection rates. Pair this with systems running unpatched and vulnerable software that's ripe for worm exploitation, and you have a recipe for disaster.

Last year, a hacker group known as the Shadow Brokers caused significant damage by releasing several zero day vulnerabilities in Microsoft Windows. It only took a month for attackers to add these vulnerabilities to ransomware, leading to two of the most damaging cyber attacks to date in WannaCry and NotPetya. This isn't the first time that new zero day vulnerabilities in Windows fueled the proliferation of a worm, and it won't be the last. Next year, "vaporworms" will emerge; fileless malware that self-propagates by exploiting vulnerabilities.

6) Prediction: WPA3 Circumvented By a Layer 2 Threat Vector

Description:

In 2019, one of the six Wi-Fi threat categories as defined by the Trusted Wireless Environment Framework will be used to compromise a WPA3 Wi-Fi network despite the enhancements in the new WPA3 encryption standard. Unless more comprehensive security is built into Wi-Fi infrastructure, users will be fed a false sense of security with WPA3, while remaining susceptible to threats like Evil Twin APs.

WPA3 is the next evolution of the Wi-Fi encryption protocol. It has undergone significant improvements over WPA2, but it still does not provide protection from the six known Wi-Fi threat categories. These threats operate primarily at Layer 2 and include: rogue APs, rogue clients, evil twin APs, neighbor APs, ad-hoc networks and misconfigured APs.

The Evil Twin AP, for example, is very likely to be used in Enhanced Open Wi-Fi networks as opportunistic wireless encryption (OWE) can still take place between a victim client and an attacker's Evil Twin AP that is broadcasting the same SSID and possibly the same BSSID as a legitimate AP nearby. Although OWE would keep the session safe from eavesdropping, the victim's Wi-Fi traffic would flow through the Evil Twin AP and into the hands of a man-in-the-middle (MitM) that can intercept credentials, and plant malware and remote backdoors.

It's highly likely that we'll see at least one of the threat categories utilized to compromise a WPA3 network in 2019, and our money is on the Evil Twin AP.

7) Prediction: Biometrics as Single-Factor Authentication Exploited By Attackers

Description:

As biometric logins become more common, hackers will take advantage of their use as a single-factor method of authentication to pull off a major attack in 2019.

Biometric login methods such as face and fingerprint readers on consumer devices like smartphones and gaming consoles present a tempting target for hackers. While biometrics are more convenient than remembering many complex passwords, and they are more secure than poor passwords, they are still just a single method of authentication. If people don't add a second form of authentication, cyber criminals that successfully hack biometrics can easily gain access to their personal and financial data.

But aren't biometrics much harder to crack? Well, a researcher fooled a fingerprint scanner with gummy bears in 2002, and a hobbyist hacking group defeated the iPhone's TouchID in 2013. In 2017, a Vietnamese security group claims to have created a mask that can fool Apple's FaceID. It's only a matter of time before hackers perfect these methods and exploit the growing trend of biometrics as the sole form

of authentication. Of course, users can prevent these hacks by using multi-factor authentication. We believe that enough of the public will continue using single-factor biometric authentication in 2019 that hackers will take advantage of their naivete and pull off a major biometric hack.

8) Prediction: Attackers Hold the Internet Hostage

Description:
Next year, a hacktivist organization or nation-state will launch a coordinated attack against the infrastructure of the internet.

The industry already saw the impact of an attack against a critical piece of internet infrastructure when a DDoS attack against DNS hosting provider, Dyn, took down many popular websites including Twitter, Reddit, and Amazon.com. Around the same time, security expert Bruce Schneier noted that attackers were probing several unnamed companies that provide similar critical internet services for potential weaknesses. A DDoS attack of this magnitude against a major registrar like Verisign could take down an entire top-level domains (TLD) worth of websites. Imagine the impact if every single .com address was no longer resolvable.

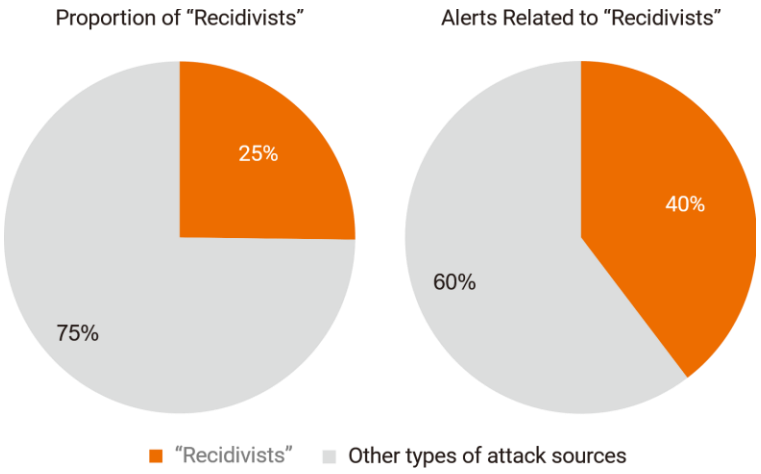
Even the protocol that drives the internet itself, Border Gateway Protocol (BGP) operates largely on the honor system. Only 0.1 percent of the internet's autonomous system numbers (ASNs, collections of IP address routes under control of an organization) have deployed Route Origin Validation, meaning the other 99.9 percent are wide open for hostile takeover from route hijacking.

The bottom line, the internet itself is ripe for the taking by someone with the resources to DDoS multiple critical points on the internet or abuse the underlying protocols themselves. With nation-state and hacktivism attacks ramping up recently, we could see cyber attackers actually take down the internet in 2019.

If I Use The Word Recidivists, Will They Come?

Recidivist is an interesting word. It means "a convicted criminal who reoffends, especially repeatedly."[28] The word had common usage in the last century although it started to fall into disuse the last 30 years or so.[29] There isn't another word that aptly describes the behavior identified in the NSFOCUS 2018 H1 Cybersecurity Insights report, which found that out of 27 million cyberattack sources in the first six months of 2018, 25 percent were repeat attackers or "reoffenders." These recidivists were then responsible for 40 percent of all attacks seen during that period.[30]

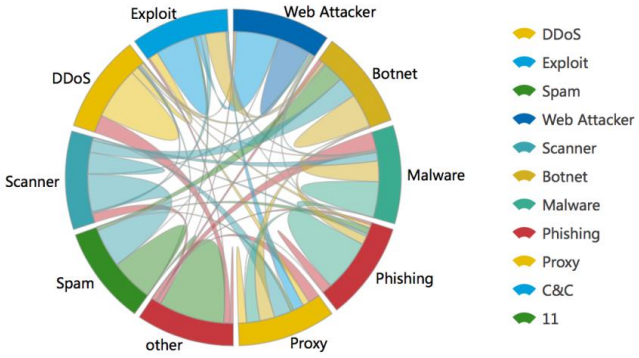
[28] Oxford Dictionary, https://en.oxforddictionaries.com/definition/us/recidivist
[29] Google Books Ngram Viewer, https://books.google.com/ngrams/graph?year_start=1800&year_end=2008&corpus=15&smoothing=7&case_insensitive=on&content=recidivists
[30] NSFOCUS 2018 H1 Cybersecurity Insights report, 2018, page 6.



Almost 80 percent of those recidivists launched more than one attack type.[31] Over time, the most common attack combinations were

- 50 percent of web attackers also attempted sophisticated exploit attacks
- 44 percent of malicious scanners were also spam sources
- 24 percent of hosts trying to exploit other systems were identified as part of larger botnets
- 20 percent of infected proxies were used to run malicious scans

Figure 1-3 Malicious IP addresses used for multiple purposes



Botnets are created with the goal of critical mass; the bigger the botnet, the more damage it is capable of doing. Botnets are created by infecting a system, it could be a server, laptop, or webcam, with some type of malware-- but cyber criminals have learned a few things in the past few years:

[31] NSFOCUS 2018 H1 Cybersecurity Insights report, 2018, page 5.

Why keep a botnet army to ourselves when we can charge others for the use of the botnet? This has given rise to BaaS (Botnets-as-a-Service) and DaaS (DDoS-as-a-Service) where for a fraction of the cost a bitcoin (as low as the equivalent of $50) anyone can launch a large-scale DDoS attacks anonymously.

Many of these attacking devices were IoT. The most obvious conclusion here is that the owners of these devices were not aware that their devices had been infected and being controlled by a cybercriminal. The longer these devices stay infected, the greater the opportunity to do more things depending on the malware used. In some cases, the malware is self-updating. And worse, most users, even if they knew their system was infected, would have no idea how to remove the malware it even possible.

But the question one must ask about recidivists is, are repeat offender IPs actually the same device? How certain are we that the 9 percent of previous DDoS attackers now attempting exploits are in fact the same systems?At first glance, one might wonder how they could not be the same, but most devices on the internet are assigned dynamic IP addresses from a subnet for a period of time. A lease of an IP address can range from a few minutes to several months (though typically seven days in the US for ISP and cellphone customers) depending on the environment. Usually, the lease of an online device is automatically renewed, thus letting it keep the same IP address. But what happens when a device is turned off or disconnected from the network when its lease expires?

Every cell phone has a dynamic IP address assigned to it. If the phone is turned off or roaming on another network (where it gets a new IP address anyway), the IP address gets assigned to another device on the network. So, the IP address a Samsung phone had last week may now belong to a Google Pixel or even an iPhone. When the WireX malware was injected into over 300 Google Play apps last year, it was not uncommon for many Android phones within a given area for a given provider to participate in DDoS attacks for several weeks if not months. But the IP address of any given phone could have changed during that time, making it difficult to prove a single cell phone participated in multiple attacks. In some countries, privacy laws prohibit the review of carrier logs as IP addresses tied to cell phones could identify a given user over time.

So, what can be done to prove a given device participated in any given attack? Devices today are identified by a “fingerprint,” code or script run on a device that can enumerate or show specific characteristics about a device such as hardware type, OS type, and version, etc. In most cases fingerprinting may not provide enough characteristics to uniquely identify a specific device or that unique information is not retained for privacy purposes.

Research is being done to develop technologies for accurate identification of individual devices and still maintain privacy. Some vendors are offering versions of these technologies now. Once these technologies are widespread, the easier it will be to locate and definitively identify recidivists and their attacks. Once we can do that, we can more accurately analyze and understand their attack patterns. This could help identify the source of the malware infection as well as potential future targets. More importantly, it could help providers develop remediations plans for customers, thus removing recidivist devices from the botnet ecosystem and reduce malicious traffic overall.

Until such time, it is the responsibility of the device owner to review the behavior of their internet connected devices to see if there has been any potential malicious activity. Unfortunately, most people

do not know or understand this yet so that recidivists will become more widespread and more dangerous in the coming year.

About the Author

Guy Rosefelt is responsible for developing and championing NSFOCUS threat intelligence and web security products worldwide. Rosefelt has more than 30 years' experience in information, application and network security. Beginning his security career as an officer in the US Air Force, he left on an odyssey that took him through so many security products and startups that it would be embarrassing to mention them all.

Regent University's Institute for Cybersecurity

Immersive Training On Regent University's Cyber Range Puts Cyber Professionals Ahead Of The Game

Cyberattacks affect the lives of everyone, from business owners required to safeguard assests and data to children growing up with tablets in their hands.

It's a reality reinforced daily with revelations of security breaches that compromise the personal information of millions and cost organizations millions of dollars in mitigation, downtime and lost customers.

By 2021, cybercrime damage will reach an estimated $6 trillion and cybersecurity spending will exceed $1 trillion. Cybercriminals gain ground daily as organizations struggle to keep up with the barrage of threats – and vie for qualified cybersecurity professionals. But qualified professionals are in short supply. More than three million cybersecurity professionals need to enter the market to accomodate the predicated international shortfall by 2021.

Often, organizations that rely on their organic IT assets to defend their critical information consist of highly adept IT professionals who lack basic cybersecurity experience, despite holding commercial certifications. According to an ISACA (2017) report, less than 25 percent of cybersecurity job applicants are qualified for the positions for which they are applying.

Those applicants require hands-on experience so that they can identify, analyze, mitigate and restore systems after an attack. These professionals also need skills to adequately synthesize the information and communicate root cause and Corrective Action Plans to executives.

This reality places Regent University's Institute for Cybersecurity in a unique position to help the IT industry close the gap between theory and practice in cyber defense. Home to one of the nation's largest commercial cyber ranges, Regent, located in Virginia Beach, Virginia, trains IT professionals by giving them the hands-on cyber defense skills needed in the workplace.

Don Murdoch, associate director of the institute and SANS certified GIAC Security Expert (GSE), said training on its cyber range effectively jump-starts careers.

"We offer scenarios on the range I've rarely seen in my experience, as well as routine activity. To get the variety of experience you would need at least two years in a cyber defense role. We can short-circuit that learning curve in a week," Murdoch said.

Murdoch is the author of the industry-impacting book, "Blue Team Handbook: Incident Response Edition." He adds, "When you're hiding behind a firewall in a corporate environment, you don't tend to get a lot of action. The variety of attacks we offer on the range is really what's it's about."

With 20 globally accessible state-of-the-art cyber range workstations, Regent's multimillion-dollar cyber range provides a virtualized hands-on learning environment where trainees analyze an array of adaptable, live-fire scenarios simulating common real-world cyber-attacks, such as ransomware, targeting traditional and Industrial Control System (ICS) networks today. Small groups work through increasingly difficult scenarios to identify attacks and perform forensic investigations with enterprise-grade tools found in many government and Fortune 500 companies.

The institute's mission to set the standard in training and education doesn't stop there. Regent's cyber range capability also has been integrated into a new 144-hour Certified Cyber Practitioner (RCCP) program offering three levels of certification mapped to knowledge, skills and abilities as defined by the National Initiative for Cybersecurity Careers and Studies for Incident Response and Cyber Defense Analyst.

Each certification level incorporates commercially recognized curriculum for IT certifications but takes training a step further by including time on the cyber range.

Despite the steady stream of cyber attacks in the news, organizational leaders often fail to fully appreciate the magnitude of the growing cyber threat. To address this gap Regent also offers one-day interactive workshops designed for the C-suite and upper level managers.

Topics include state and federal regulations regarding disclosure of cyber incidents, and practical exercises train leaders to evaluate their existing cyber programs against National Institute of Standards and Technology (NIST) best practices.

For government and senior military leaders, the institute is developing a short series of workshops intended to build a baseline for understanding cybersecurity requirements and effectively manage cybersecurity readiness. The workshops will be particularly helpful to senior leaders who do not have an operational cyber background but are responsible for their organization's cybersecurity program.

As an academic institution, Regent also offers associate, bachelor's and master's degree NSA-accredited programs in cybersecurity.

Regent University's Institute for Cybersecurity is disrupting and transforming the Cyber Defense industry with a state-of-the-art training platform and world-class trainers. To learn more about commercial training offerings, visit regent.edu/cyber or contact the institute at 757.352.4215.

Cryptographic Key Management Considerations for Secure Cloud Computing

by Brian Jenkins, VP of Product, StrongKey

The cloud has gained enormous adoption due to the value of outsourced hardware and software ownership and maintenance in multi-tenant environments. Organizations benefit from significant cost savings, ease of use, and scalability benefits. This has been a particular boon for mid-sized businesses since they don't have to build out their own infrastructure.

When it comes to security, however, the using the cloud is comparable to leaving your house key under the door mat. You have outsourced not only your infrastructure but the encryption keys to your sensitive data and files as well.

To be truly secure, you need to think about who has access to the encryption keys. Unless you have ***exclusive*** control of your encryption keys, you could be at risk. Unfortunately, that is not the case with the cloud and it's one of the reasons why we continue to get apologetic emails notifying us that our data has been compromised. Each cloud service and software-as-a-service provider represents a huge attack surface and is therefore a serious target. With everything moving into the cloud, how do you make key management work? This is a challenge that needs to be solved.

Keys in The Cloud

Organizations often assume they *need* a multi-tenant cloud solution (applications, database, files, and everything else hosted in the cloud). This is the simplest concept since it's easy to understand how on-premise infrastructure can be visualized as cloud instances. However, moving key management systems (KMS) to the cloud using any of the three common cloud-based options poses significant risks.

- **Outsourced KMS** (the cloud service provider owns the keys): Cloud vendors will say that all your data and files are secured and encrypted. That's good – except if the provider or your account credentials to the provider get hacked (as it did in Uber's case with AWS). Your files may be encrypted, but if you're storing your encryption keys with them, then the attacker can decrypt everything if their attack gains access to your keys as well.

- **Cloud KMS** (you own the keys but they're stored in cloud software): A software-based, multi-tenant cloud KMS is especially ill-suited for cryptographic key management. Since hardware resources are shared across multiple clients, there's a higher level of insecurity to the protection of these keys – the Spectre and Meltdown vulnerabilities are testament to this.

- **Cloud HSM** (you own the keys but they're stored in cloud hardware): The "gold standard" for protecting encryption keys are secure cryptoprocessors - hardware security modules (HSM) and trusted platform modules (TPM). Although certain risks are mitigated by using a cloud-based HSM or TPM, the fact remains that in the cloud, even applications that use secure cryptoprocessors are still part of a multi-tenant infrastructure. Between attacking a purpose-built hardware cryptoprocessor or an application running in a multi-tenant environment, the application is always the easier target from an attacker's point-of-view.

Obey the Laws

Even if you trust the cloud to provide all of the industry buzzwords about perimeter security with next-generation firewalls, intrusion detection, and other protective measures, securing the core elements your business depends on – sensitive data and files – against breaches requires encryption using the fundamental "Laws of Cryptographic Key Management":

1. Cryptographic keys must be protected under the control of secure cryptoprocessors (HSM/TPM).

2. Cryptographic keys must be under the exclusive control of multiple key custodians within a single organization.

3. The parts of the application that use cryptoprocessors to operate on sensitive data must *not* execute within public multi-tenant environments – not only is sensitive data already unprotected in the multi-tenant environment, but so are the secrets that authenticate the application to the cryptoprocessor, potentially leading to the breach of encrypted data *using* the secure cryptoprocessor in the attack.

Unfortunately, no currently designed public cloud can meet these essential requirements. Organizations that leave security solely in the hands of cloud providers could be in for a rude awakening.

A Better Solution

The solution is not all that complicated: store your sensitive data and files in the cloud while retaining exclusive control of their encryption keys under the protection of your own secure cryptoprocessor in a controlled environment *outside* the public cloud.

In this architecture, a breach of the cloud service provider delivers nothing to the attacker, because they only get access to encrypted information that is of no use to them without the keys. The benefits of the cloud are still realized while maintaining data protection. This allows companies to prove compliance to data security regulations while leveraging clouds, private or public, to the maximum extent possible.

The lack of security in the cloud is a real and significant problem. Even if data used by cloud applications are encrypted, the encryption keys are the real story. Not only does the information need to be kept safe, so do the keys.

With this reality in mind, mid-market businesses need to think about enterprise-grade security instead of assuming that their data is being secured in the cloud. They will serve their customers and their own longevity best by finding solutions that meet the cryptographic key management laws noted above.

About the Author

Brian Jenkins is the VP of Product for StrongKey, a provider of open-source cryptographic key management solutions. He has over 20 years of experience in multiple Silicon Valley high-tech startups, where he began his career as a software engineer and went on to hold positions from product management to founder and CEO. He graduated from Duke University with a bachelor's degree in electrical engineering and Computer Science and earned his MBA from UC Berkeley. Brian works out of StrongKey's office in Durham, NC.Brian Jenkins can be reached online at https://www.linkedin.com/in/brianhjenkins/ and at our company website http://www.strongkey.com

The Only Counter Strategy Against Data Loss: Reliable Backup Methodology

In the turn of the century 18 years ago, people have embraced Web 2.0, a new dynamic web replacing the static HTML-only Web 1.0 fathered by Tim Berners Lee in the 1990's. Web 2.0 as a successor hosted content that can never be imagined way back year 2000, streaming video, WebGL 3d graphics, and hardware acceleration of rendering web pages. Web 2.0's database-driven web technology also introduced new possibilities such as online banking, elegant searching capabilities inside individual websites and general smoothness of navigating web pages.

However, for every positive benefit provided comes threats. The addition of complexity comes issues with security, with “ease-of-use” as the central focus for many web developers; privacy is also compromised as a result. Big Data is all the rage for the past 5 years, with the world created more data for the last 10 years than all the previous years combined since the dawn of the IBM PC in 1981. Personally identifiable information has a smell of money for the cybercriminals. The more information they can extract, by hook or by crook, the bigger potential profits they can earn at the expense of users dependent on the system. Data loss prevention is an important aspect of computing that many have forgotten about, given that the growth of the Internet gave us the convenience, being in a state of confidence, people tend not to think about data loss possibilities, let alone implement a Data loss prevention strategy.

Given that the actual performance of storage systems is much worse than required, and that even if it improves we still won’t be sure that a system will meet its requirements, the fourth part asks what is to be done. As with paper, content in digital archives will inevitably suffer loss and damage. That is why the world is very much addicted to online storage, and the market has responded. The cloud-storage solution brands have blossomed in the last 5 years, even the smartphone people hold today has automatic cloud backup as soon as it gets its first taste of online connection, creating a virtual data loss prevention system from the factory. The dependence with storing information in a remote server on the Internet is, however, the loss of control on our part when it comes to the availability, security, and integrity of data.

We are in a multiplatform world, with various devices talking with the rest of the world through TCP/IP, a protocol designed in the 1970’s. With the purpose of packet switching to maintain connection and that connection today stays-on 24/7. With our smart devices, we are fast becoming an always online civilization, where any information we need we can get in seconds, and literally information at our fingertips “pitch” of Bill Gates from the late 90’s. Accessibility is the key why users became trusting of their devices, their service providers and their data being entrusted to 3rd parties. Such rich data attracts the attention of cybercriminals, which brought us a lot of trouble like phishing, virus infections, record/data loss, security breaches, and identity theft cases.

Data loss prevention can be done weeks ahead of any possible data breaches or breakdown of hardware; this is having a credible backup plan. The principle of 3-2-1 backup strategy, applicable for both individual users and organizations. 3 - means three different media needs to be used, this diversified the backup storage minimizing the negative effects of the possibility of media corruption. One such example is an external hard drive, a USB flash drive and an online storage as backup methods for data stored on a laptop hard drive. 2 means two locations, a backup or multiple backups of critical data is useless if all of them are located in the same place. In the case of a fire, flood, earthquakes or any similar emergency

having backup media in the same location cancels the redundancy and availability of data. 1 refers to the use of at least one cloud-based backup storage solution. It is a lot better if an encrypted copy of files, an individual or an organization requires are stored somewhere remote and online. This 3-2-1 backup strategy helps a lot in preventing the loss of data in the long run.

About the Author

Julia Sowells is a security geek with almost 5+ years of experience, writes on various topics pertaining to network security. Julia can be reached online at (juliasowells@hackercombat.com https://twitter.com/juliasowells) and at our company website https://hackercombat.com/

Revisiting Conficker 10 Years Later

What we learned and how it's still impacting us today

November marked the ten-year anniversary of one of the largest and most infamous self-replicating worms in modern computing history: Conficker. For those of you who may not remember, beginning in November of 2008, the self-replicating Conficker worm worked its way across the Internet, infecting Microsoft Windows operating systems in as many as 9 million enterprise, government and personal computers, spanning more than 190 countries. At the time, I was on the front lines in the battle working as a Senior Program Manager with the Microsoft Malware Protection Center (MMPC). The unique experience has impacted my approach to cybersecurity ever since, and I thought this milestone anniversary would be a good time to look back at this exploit, what it taught us and how it continues to impact the industry today.

Discovering the Vulnerability And Initial Response

The initial zero-day vulnerability was first detected by Microsoft's Trustworthy Computing team, which had, at the time, recently developed a new method for using telemetry data from crash reports to identify and trace unknown exploits. Once the MMPC team was made aware of the vulnerability, which became known as MS08-067 and was classified as being "wormable", meaning that its exploitation could be used for self-replicating malware without any user interaction, our goal was to inform and protect customers as quickly as possible, while at the same time collecting data to determine how far attacks were spreading. Microsoft issued an emergency, out-of-band security bulletin and a patch in October of 2008, buts as with any exploit, the patch is only the beginning. We knew that once the zero-day knowledge was made publicly available, we were going to see a sharp increase in attacks. It was critical that we impress on our customers the severity of this vulnerability and urge them to update and protect their computers as quickly as possible.

After issuing the security update, we spent the next several days holding our collective breath, checking the telemetry data closely – almost hour-by-hour – and watching as more crashes were reported. Due to the nature of the bulletin we released about the patch, the media quickly caught onto the seriousness of the situation and hackers began to test the exploit for themselves. By early November, about two weeks after our initial discovery of the vulnerability, a new malware targeting the MS08-067 vulnerability emerged, but the prevalence was still very low. A few weeks later, however, the Conficker worm broke out on a scale the industry had rarely seen before.

The Spread of Conficker

Part of what made Conficker so prolific was the way in which it mutated and changed its propagation strategy. As many as five different variants of the malware emerged over time, hijacking millions of computers and adding them to a global botnet. According to reports at the time, several high-profile government agencies and enterprise organizations fell victim to the worm, including the French Navy, the United Kingdom Ministry of Defense and Bundeswehr, the unified armed forces of Germany. It seemed the entire industry was waiting, on edge, to see what the massive botnet would be used for. Experts were predicting worst case scenarios such as a denial of service attacks against large organizations, harming critical components of the Internet's infrastructure, distributing ransomware, or any number of other threats to both the public and private sectors.

Ultimately, Conficker's notoriety may have been its downfall. The perpetrators behind the exploit never fully activated the botnet it created, likely because they had drawn so much global attention and feared being caught if they tried to unleash a widescale attack. Even so, experts estimate the global cost of efforts to combat the worm totaled more than $9 billion. This includes the time and resources spent by cybersecurity practitioners, government agencies, enterprises and individuals to clean up their infected machines and purchase counter-measure software.

Collaboration Was Key

Looking back, there is much we did right in our response from the initial discovery of the worm and the very first exploits, through to the wider outbreak. Our efforts were the result of two pillars working together. One was the technical investigation of the vulnerability: we needed to know everything we could about it and the affected versions so that a complete fix could be developed and tested. The second pillar revolved around providing public communications to ensure customers, partners and security professionals had all the relevant and timely information they needed to keep their systems safe and prevent more computers from being compromised.

That collaboration between different internal and external teams working to mitigate the threat was incredible. As soon as the worm gained momentum, the Conficker Working Group, comprised of elite researchers from multiple vendors and organizations, was established and enabled team members to work together effectively to exchange data, techniques and launch countermeasures to disrupt the propagating malware. Conficker taught us that cybersecurity really is a collective and collaborative effort. It helped bring together the broader cybersecurity industry, including organizations and individuals from

both the public and private sectors to share intelligence and work to mitigate the threat together, something the industry continues to embrace today. We saw the positive impact that different groups working together can have on quickly remediating a threat. Allowing experts to communicate with each other rather than remaining in silos focused on their individual work is critical.

One such technique that the Conficker Working Group collectively used to disrupt the malware was sinkholing. Sinkholing is a technique used to commandeer domains that the malware was going to use. Beyond disrupting the ability of the malware to get commands from the remote server, it allowed the researchers to collect and analyze telemetry about the spread of the worm. It was through the reverse engineering of the Domain Generation Algorithm (DGA), which the malware used to utilise a different domain each day that the researchers were able to use the sinkholing technique to proactively take over these domains.

Conficker also set a precedent in other areas. For example, Microsoft announced a bounty for information on the creators of this worm, something which had not been done before. Yet now, bounties for information on new zero-days have become commonplace, with many organizations offering their own bounty programs with the promise of reward that include anything from money to air miles.

Innovation was key in the successful discovery and response to this threat. The method that was developed by the Trustworthy Computing group to identify unknown zero-days was ahead of its time and allowed us to learn about MS08-067 early. If this method for analyzing crash reports hadn't been developed, then MS08-067 may have been discovered much later when exploits were much more prevalent. As simple as this advice may seem, Conficker also demonstrated the importance of making sure users patch their machines quickly, which can eliminate the risk of being impacted by known exploits. Many organizations also benefit from using scanning solutions and patch management from third-party vendors that can help them scan their entire environment and identify cases where there is insufficient patching.

Cybercriminals learned a different lesson from the incident. Today, most malicious hackers try to not draw attention to themselves, using more discreet methods, such as Trojan horses, and smaller, more targeted attacks. It would also be accurate to say that "wormable" vulnerabilities such as Conficker are now incredibly rare in popular software such as Microsoft Windows, meaning the cybercriminals had to turn to alternative methods and attack techniques. For example, exploit kits developed by cybercriminals to ease the task of infecting large numbers of computers. Other methods include malvertisement, server compromise and various social engineering tricks.

What We Learned

Although the machines infected as a result of Conficker were not used in a major cyberattack, it continues to impact us today. A decade later, Conficker can still be found on networks, infecting unpatched computers. As recently as 2016, it seemingly rose from the dead to hijack Internet-connected medical devices in hospitals and help steal patient data. As long as organisations have legacy machines connected to the Internet that are not properly patched, it will continue to spread, albeit at a slower pace

than it did ten years ago, until there are no more computers using the old and vulnerable version of Windows.

In my work with SpiderLabs at Trustwave, I build on the framework of experience that I gained from Conficker and threats like it as well as cross-industry collaboration, to continue to help customers stay ahead of attacks and protect themselves. Moreover, we seek to continue developing and place emphasis on the two pillars of technical understanding at Trustwave and proactively communicate them to both customers and the general public. Working on MS08-067 was a unique experience where innovative techniques, dedicated teamwork and industry-wide collaboration all came together for the purpose of fighting this threat. Everyone who was part of the response team back then is proud of the work that we did and that the lessons we learned during that outbreak still help the security community today in successfully combatting cybercrime.

About the Author

Ziv Mador ,VP, Security Research, Trustwave SpiderLabs.Ziv Mador manages the global security research team at Trustwave SpiderLabs, with a focus on vulnerability assessment, WAF, malware forensics, email security, IDS and web-based attack protection. Mador is a primary spokesperson for the company on aspects related to malware and cybercrime. He has been a regular speaker at security conferences such as AusCERT, FIRST, CARO, ISOI, MSRA and WORM. Prior to his current role, he worked at Microsoft developing a variety of security technologies including antimalware capabilities, IDS/IPS, enterprise firewalls, Windows security and managing the response to zero-day malware for years. He is a 21-year veteran of the security industry and a leading authority on the topic of Internet threats and cybercrime.


EVENT

Under the Patronage of
the President of the Council of Ministers
His Excellency Mr. Saad Hariri

Sustainable Digital Ecosystem summit
LEBANON

Learn from top experts on
Digital Transformation and
Disruption

4 - 6 Dec. 2018

MEA Training
& Conferences Center
Beirut, Lebanon

info@sdesummit.com
sdesummit.com

ifp

"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:

An International Conference on Counter-Terrorism and Internal Security

www.counterterrorasia.com

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

Organized by:

FIREWORKS® TRADE MEDIA GROUP

Fireworks Trade Media Pte Ltd

12TH OPERATIONAL ENERGY SUMMIT

January 28-30, 2019 | WASHINGTON D.C.

WHY YOU CAN'T MISS OUT ON OPERATIONAL ENERGY SUMMIT 2019!

- Discover the military's operational energy priorities and its implications on the industry.
- Learn about the military's interest in intelligent grids to better inform your strategies
- Discuss DoD's initiatives for cutting operational energy waste and pitch solutions
- Build relationships with military and industry thought leaders to give your company an edge

Executing Future Operational Energy Strategies

No Cost Passes Available For Active U.S. Military And Federal Government Employees

OperationalEnergySummit.iqpc.com | 1-800-882-8684 | idga@idga.org

DGI EUROPE

Geospatial Intelligence for National Security

28-30 January 2019, Royal Lancaster London

WHERE THE FUTURE OF THE GLOBAL GEOSPATIAL INTELLIGENCE INDUSTRY IS DEFINED

QUOTE **CDM19** TO **GET 15%** OFF YOUR TICKET TO ATTEND*

Source. Analyse. Automate. Share.

THE CONFERENCE FOR GLOBAL GEOSPATIAL INTELLIGENCE LEADERS

JOIN 650+ GEO INT LEADERS INCLUDING:

Lt General James Hockenhull, Chief of Defence Intelligence, **UK MoD**

Jennifer Schnarre, Associate Director for Capabilities, **National Geospatial-Intelligence Agency (NGA)**

Scott Dewar, Director, **Australian Geospatial Intelligence Organisation (AGO)**

Major General Raul Escribano, Deputy Assistant Secretary General for Intelligence, **NATO HQ**

Brigadier Lars Corneliusson, Director of Military Intelligence, **EU Military Staff**

Colonel Orest Babij, Commander, **Canadian Forces Intelligence Group**

Pascal Legai, Director, **European Union Satellite Centre**

Commander Heather Quilenderino, Commanding Officer, **US Naval Ice Center**

PRINCIPAL PARTNER

esri THE SCIENCE OF WHERE

SPONSORS

Raytheon · DigitalGlobe A MAXAR COMPANY · mapbox · earth · MAPLARGE · planet. · e-geos

* Discount applies to military/ government bookings only

IoT ASIA | 27-28 March 2019

Hall 1, Singapore EXPO

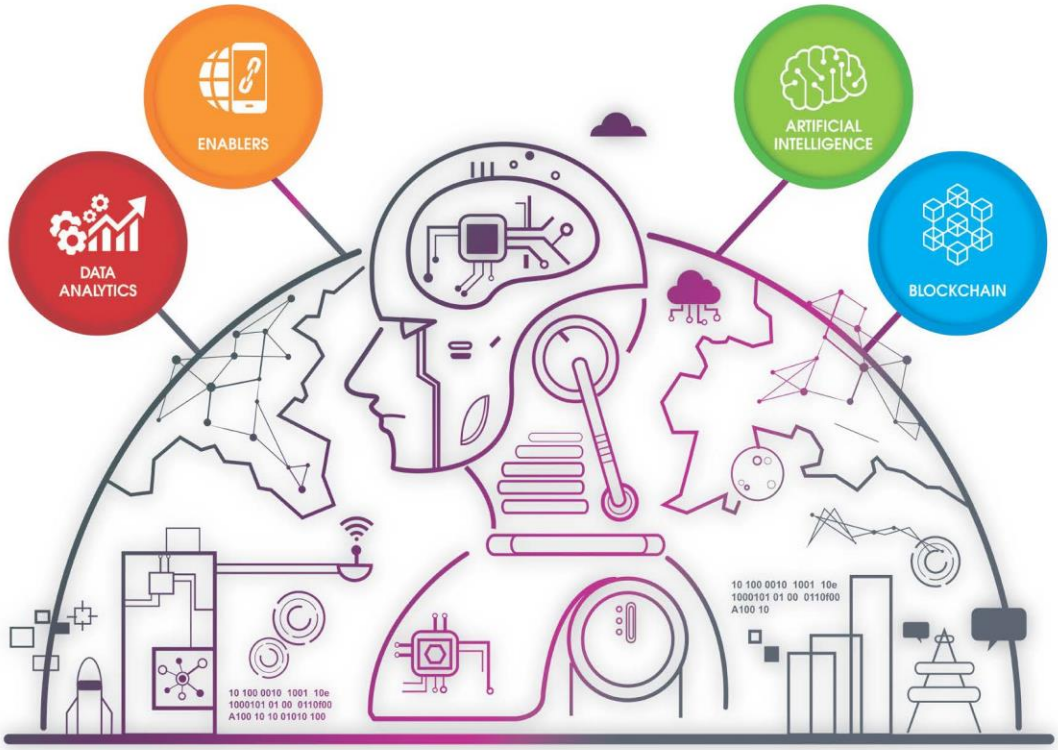
INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS

TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES

SHOWCASE your latest innovations and strengthen your business partnerships

BUILD Value Chains across the IoT Ecosystem

GAIN key insights from best practices and case studies from Industry Leaders



Artificial Intelligence Blockchain Data Analytics Enablers Data Analytics Blockchain

BUILDING VALUE CHAINS

SMART CITIES // INDUSTRIAL IoT

Enablers Artificial Intelligence Data Analytics Blockchain Artificial Intelligence Data Analytics

ENABLERS Artificial Intelligence Data Analytics Blockchain Data Analytics Blockchain Artificial Intelligence Data Analytics Blockchain ARTIFICIAL INTELLIGENCE

Artificial Intelligence Data Analytics Enablers Blockchain Data Analytics Artificial Intelligence Data Analytics Enablers

DATA ANALYTICS Data Analytics Blockchain Artificial Intelligence Blockchain Artificial Intelligence Data Analytics Enablers BLOCKCHAIN

Artificial Intelligence Data Analytics Blockchain Data Analytics Artificial Intelligence

JOIN US AT THE 6TH EDITION OF IoT ASIA 2019

Interested to Exhibit or Sponsor? Contact us at sales.iotasia@singex.com

www.internetofthingsasia.com • #iotasia

Organised by

SiAA

SingEx

Industry Accolades

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

Official Partner

NECTEC
a member of NSTDA

CYBER INTELLIGENCE ASIA

NOVOTEL SIAM SQUARE HOTEL | BANGKOK, THAILAND
27 TH – 28 TH FEBRUARY 2019

Esteemed Speaker Line-up:

Allan Cabanlong, Assistant Secretary, Cyber Security and Enabling Technologies, **Department of Information and Communications Technology (DICT), Philippines**

Wasawat Chawalitthamrong, Head of Crime Relating to Submission of Bids to Government Agencies, **Department of Special Investigations, Thailand**

Chalee Vorakulpipat, Head of Cybersecurity Laboratory, **National Electronics and Computer Technology Center (NECTEC), Thailand**

Fazlan Abdullah, Head, Government Engagement, **CyberSecurity Malaysia**

Budi Rahardjo, President, **Indonesia Computer Emergency Response Team (ID- CERT)**

Dr. Haji Mingu bin Haji Jumaan, Director, **Sabah State Computer Services Department, Malaysia**

Rana Shahzad, Forensics Expert, Cybercrime Division, **Federal Investigation Agency, Pakistan**

Martijn van der Heide, Specialist, **Thailand Computer Emergency Response Team (ThaiCERT)**

Kitisak Jirawannakool, Information Security Specialist, **Thai Bankers Association**

Virag Thakker, Senior IT Compliance Officer, **Agoda**

SPONSORSHIP OPPORTUNITIES AVAILABLE!

To book a stand in our exhibitor hall please contact us at events@intelligence-sec.com or +44 (0)1582 346 706

Sponsors & Exhibitors

Resecurity®

For more information visit – www.intelligence-sec.com

Book your place by:
w: www.intelligence-sec.com I e: events@intelligence-sec.com I t: +44(0)1582 346706

INTELLIGENCE-SEC


IFSEC
INTERNATIONAL
18-20 JUNE 2019
EXCEL LONDON UK
"40% MORE LEADS THIS YEAR THAN LAST. THE MEETINGS WITH VIPS HAVE BEEN SO BENEFICIAL, WITH QUALITY NAMES WHO ARE READY TO BUY, NOT JUST SPECULATE."
Managing Director, ZKTeco
SECURITY IS
CRITICAL
IFSEC IS ESSENTIAL
Position your brand at the centre of the critical security conversation. Be part of IFSEC 2019.
Unique in attracting the entire security buying chain, IFSEC 2019 is your world-class, integrated security summit. Influence the innovation dialogue with over 27,000 global security integrators, installers, distributors, consultants and end users from over 117 countries – all under one roof.
43,461 Leads were generated onsite at IFSEC in 2018 – an average of 123 per exhibitor
34% of visitors had an annual purchasing budget of over £1,000,000
Generate global business with quality buyers – Expand your business into high-growth markets around the world
Find out more at: www.ifsec.events/international/exhibit


COMEX
TECHNOLOGY
SHOW 2019


COMEX
TECHNOLOGY
SHOW 2019

CYBERTECH
THE EVENT FOR THE CYBER INDUSTRY

28-30.1.2019 TEL AVIV

CYBER.
WE LIVE IT. BREATHE IT.

Cybertech Worldwide. Creating Business Opportunities Across Borders.

SAVE THE DATE FOR CYBERTECH TEL AVIV 2019!

Join us on **January 28-30, 2019,** at the Tel Aviv Convention Center for the **BIGGEST CYBER EVENT** of the year!

>> **15,000** Attendees >> **170** Speakers
>> **210** Companies >> **90** Start-Ups
>> **160** Delegations from over **70** countries

Come LEARN, NETWORK, and MAKE BUSINESS with the cyber industry's most prominent players.

Top executives. Government officials. THOUSANDS of great business networking opportunities. All at the forefront of global innovation!

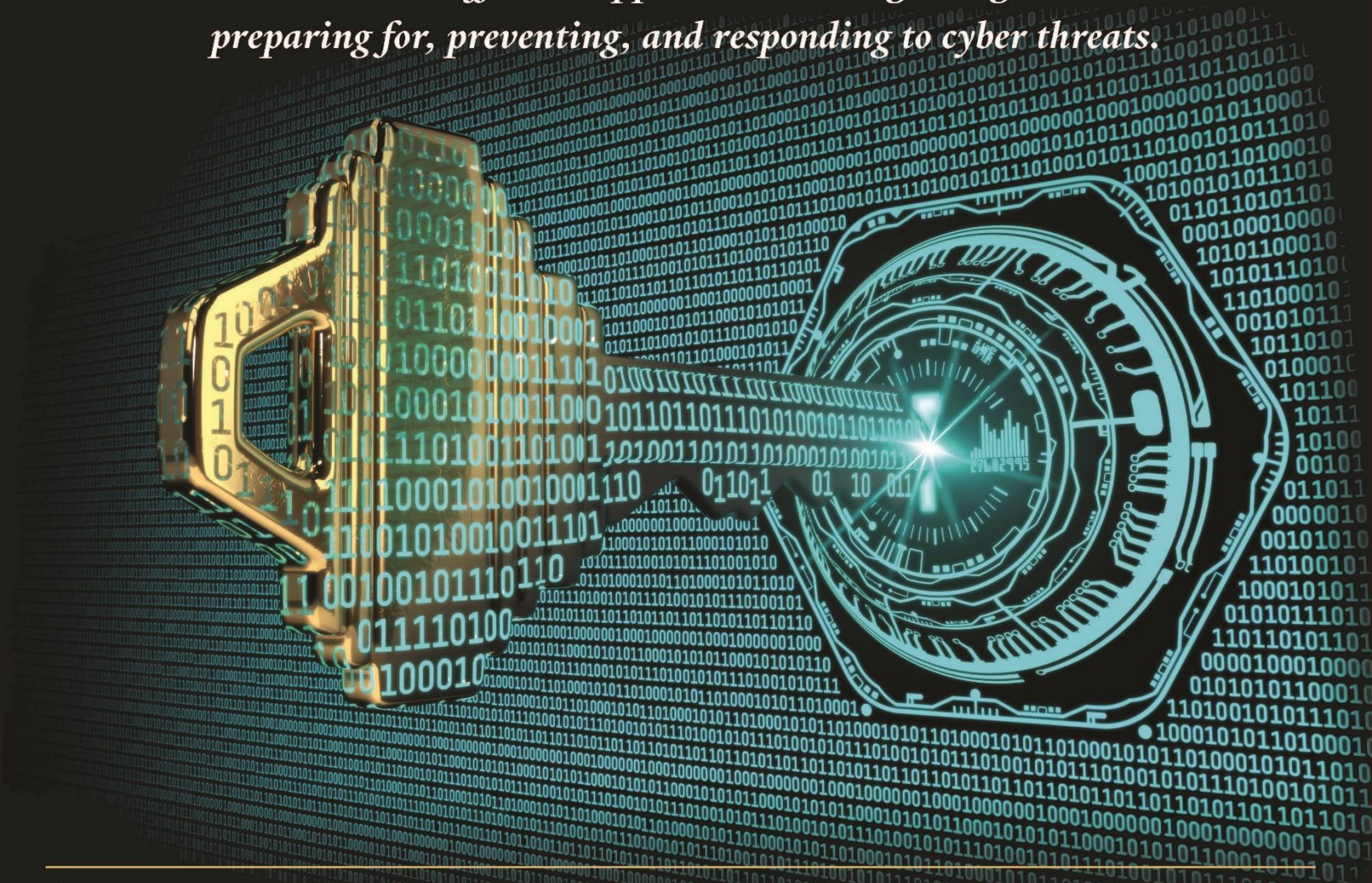
Register today at http://cybertechisrael.com | For more information, please contact cyber@cyberconference.com.

YALE CYBER LEADERSHIP FORUM

THE LAW, TECHNOLOGY, AND BUSINESS OF CYBER SECURITY

February 28–March 2, 2019 • Yale University • New Haven, Connecticut

Learn effective approaches to recognizing, preparing for, preventing, and responding to cyber threats.



"The experience gained from attending the Forum was indispensable and highly effective in understanding and mitigating the overall and ever-emerging cyber security threat landscape!"

— Randall S., Cyber Threat Intelligence Liaison Officer, U.S. Department of Energy

Scholarships and discounts are available for a limited time.
Apply by January 25 to qualify.

WEB *cyber.forum.yale.edu* **EMAIL** *cyber.forum@yale.edu*

Your peers use managed file transfer to solve key business initiatives - but how?

IT professionals discover innovative uses for their secure file transfer solution every day. From tracking weather patterns in Alaska to eliminating third-shift staffing, MFT makes solving their organizational needs easy.

In The GoAnywhere Book of Secure File Transfer Project Examples, you'll discover 20+ ways your peers use managed file transfer to meet ambitious goals and requirements in their company, including:

- A distribution company that uses MFT to send barcode scans to a file repository.
- A healthcare organization that uses MFT to move faxes into an API for processing.
- A manufacturing business that uses MFT to check a server for firmware updates.

Find the inspiration and know-how for your next file transfer project.

GO ANYWHERE®
Managed File Transfer

Visit ***info.goanywhere.com/use-cases-for-mft*** to get the free guide sent right to your inbox.

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

“Amazing Keynote”

“Best Speaker on the Hacking Stage”

“Most Entertaining and Engaging”

Gary has been keynoting cyber security events throughout the year. He’s also been a moderator, a panelist and has numerous upcoming events throughout the year.

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

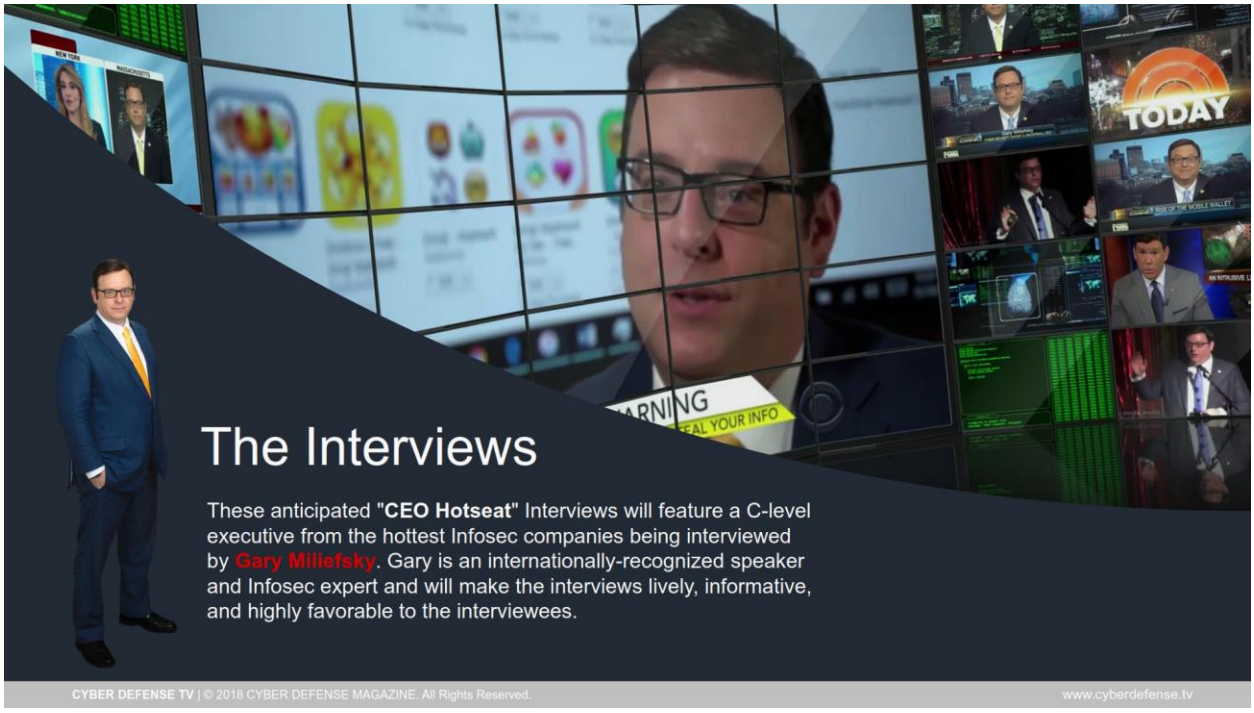
INFOSEC KNOWLEDGE IS POWER

You asked, and it's finally here…we've launched CyberDefense.TV

At least a dozen exceptional interviews rolling out each month starting this summer…

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: 12/01/2018

Regent University's Institute for Cybersecurity is disrupting and transforming the Cyber Defense industry with a state-of-the-art training platform and world-class trainers. To learn more about commercial training offerings, visit regent.edu/cyber or contact the institute at 757.352.4215.

Learn more about this program: https://www.regent.edu/institutes/cybersecurity/industry-training/

Space is limited, so register today: https://regent.emf360.com/explore/search

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."

Gary S. Miliefsky, Publisher & Cybersecurity Expert

ALWAYS FREE
NO STRINGS ATTACHED

Does Your Organization Need MFT Software?

Determine if a secure file transfer solution is right for your situation.

Managed File Transfer (MFT) solutions improve and streamline critical file transfer processes, including encryption, automation, data security compliance, and trading partner collaboration.

But is this solution right for you?

GO ANYWHERE®
Managed File Transfer

You might benefit from MFT if:

1. You need to audit your file transfer activity.
2. You need to comply with data security laws and regulations.
3. You use traditional methods (e.g. FTP or legacy scripts) to send data.
4. You need to easily and securely exchange data with trading partners.

GoAnywhere MFT is a secure file transfer solution that's quick to implement and user-friendly for all.
See for yourself how MFT can help your organization with these four needs and more. Try a 30-day trial today.

Benefit from MFT Today. Start Your Trial. **www.goanywhere.com/trial**


BOSCH
Invented for life
Bosch and Genetec.
End-to-end security,
day after day
Learn more

HERJAVEC GROUP

The sea of connected devices is a dangerous place.
You want a **Shark** on your team.

Top Ranked MSSP & Global Cyber Operations Leader

- Advisory Services
- Identity Services
- Technology Architecture & Implementation
- 24/7 Managed Security Services
- Threat Management
- Incident Response

Robert Herjavec
Star of ABC's Shark Tank
CEO & Founder of Herjavec Group

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNER

- Security Company of the Year
- Identity and MSSP Leader