CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IT Security Myths
Cyber Predictions
Breaches & Encryption
OPSEC Tips

December 2015

MORE INSIDE!

CONTENTS

CYBER WARNINGS

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

PRESIDENT

Stevin Victor
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Ron Hovsepian
Dr. Leo A. Guthart
Michelle Mocalis
Zoran Adamovic
Anna Wehberg
Nimmy Reichenberg
Todd Weller
Rogerio Winter
Rodrigo Ruiz
Chris Pogue
Amir Orad
Ajit Pendse

Interested in writing for us:
marketing@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Magazine: http://www.cyberdefensemagazine.com

Executive Producer:
Gary S. Miliefsky, CISSP®

Will 2016 Be A Year of Better Cyber Security or More Breaches?

Friends,

You might say this is a silly question. I'm guessing most of our readers are thinking what I'm thinking – that we'll continue to face exponential breaches next year. It's been a trend – so why can't we turn it around? Are the cyber hackers and online criminals that much smarter than the average INFOSEC professional or IT staff? Do they know something we don't know? Looking back at 2015, it seems that a common trend in breaches was lack of proper training so that just about any employee could be victimized by a spear phishing attack, with the deployment of a Remote Access Trojan (RAT). In addition, while firewalls are designed to guard the gates, the best cyber criminals are able to 'parachute' their malware in, behind the firewall and easily circumventing even the best anti-virus protection.

Then, there's encryption. As we, at CDM, have been proponents of all time, everywhere encryption, this seems to run counter to the reality of large database breaches such as the OPM.gov and Anthem breach, to name a few (both totaling, together, over 102,000,000 records with much medical and personally identifyable information beyond a typical credit card breach of a retailer). In addition, with the NSA and other international government agencies wanting backdoors into all TELCO and INFOSEC equipment, especially those that use encryption, there's a privacy battle raging, whereby these backdoors end up in security products, not only accessable by governments but by cyber criminals as recently proven in the case of Cisco, Juniper and Huawai firewalls.

So, we leave 2015, looking back at a year of massive cyber security failure. Is it that difficult to convince the Board and CEO and CFO that there should be a budget for regular employee INFOSEC training, especially against spearphishing and other social engineering attacks? Is it that difficult for one of the top 50 anti-virus vendors to have some kind of genius epiphany and actually make an AV system that works? It seems, for 2015, in both these cases, just look at privacyrights.org and virusbtn.com for your answers – too many breaches and too much new malware beating the AV vendors.

My predictions for 2016 are that we will continue to see exponential growth in zero-day malware, RATs and breaches. Don't let your organization be the next victim – stand up for what's right – better INTRANET DEFENSES, stronger ENCRYPTION, smarter AV tools, NEXT GEN security solutions and more consistent EMPLOYEE TRAINING. Do these and your 2016 will be a productive and profitable year!

To our faithful readers, Enjoy

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief, Pierluigi.Paganini@cyberdefensemagazine.com

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

25th ANNIVERSARY

Save $400 on your Full Conference Pass during the Discount period

Discount deadline January 29, 2016

#RSAC

Connect to Protect

Register now for RSA® Conference 2016

Celebrating its 25th anniversary, RSA Conference continues to drive the information security agenda forward. Connect with industry leaders and gain timely insights that will empower you to stay ahead of cyber threats. Join us to experience 28 tracks, 400+ sessions and workshops and over 500 exhibitors.

New to RSA Conference 2016:

- Extended Expo hours and content running all day
- More Learning Labs
- Expanded Crowdsourced Sessions
- Focus-On Sessions
- Birds of a Feather morning gatherings

Featured Keynotes:

Nick Bostrom
Director of the Future of Humanity Institute

Dave Isay
Producer of StoryCorps, heard on NPR's *Morning Edition*

Amit Yoran
President, RSA

Go to **www.rsaconference.com/cdm** to register today!

DIAMOND SPONSORS

intel Security · Microsoft · RSA

PLATINUM SPONSORS

cisco · Hewlett Packard Enterprise · paloalto NETWORKS · QUALYS Continuous Security · Symantec. · vmware

MEDIA SPONSOR

CDM CYBER DEFENSE MAGAZINE

How the Data Privacy Rights Movement Puts Businesses at Risk

By Ron Hovsepian

National governments are enacting new, more stringent data privacy laws in an effort to protect citizen data from unauthorized access and guard national security interests. This is a necessary initiative for all countries. However, in the rush to pass new legislation that improves protection of sensitive and personally identifiable information (PII), these nations are also forcing global businesses to restructure current strategies, practices, and processes. This is going to be a costly endeavor for businesses that have long relied on easy, consequence-free exchange of data across borders.

For example, the European Union (EU) just announced agreement on a final text of the General Data Protection Regulation (GDPR), which will replace the EC Data Protection Directive (Directive 95/46/EC) across 28 countries. Essentially, the aim of this regulation is to ensure the secure and adequate handling of personal data through its entire lifecycle.

These are all positive goals. But when you consider that global organizations rely on SaaS and cloud-based storage to streamline efficiencies and collaborate easily across borders, compliance becomes extremely challenging. The price for non-compliance is steep, with fines up to 4 percent of annual global turnover.

In order to measure awareness of and opinions on the global data privacy movement, Ovum Research conducted a comprehensive survey of more than 300 global IT decision makers. This research unveils a sobering account of how confused and unprepared these stakeholders are for the coming data privacy regulations. Here are a few key takeaways:

- **U.S.-based multi-nationals are particularly vulnerable.** The Ovum research shows that the global sea change on data privacy is harming U.S. businesses that operate overseas. The U.S. was ranked the "least trusted" country among 20 industrialized economies, including China and Russia. Of the leaders surveyed, 63% of respondents believe that the proposed GDPR will make it more difficult for U.S. companies to compete globally, and 70% said they expect the new legislation, which is likely to pass before the end of the year, will favor European-based businesses.

- **Businesses are bracing for fines.** Two-thirds of IT decision-makers surveyed said the new regulations will force them to make changes in their European business strategy. When asked about the pending GDPR, 52% of respondents said they think it will result in business fines for their company. More than 70% of respondents admitted that they expect an increase in spending due to data privacy regulations, and 30% expect budgets to rise by more than 10% over the next two years.

- **Businesses have no control systems in place to keep data private.** While some organizations are aware of data privacy as an issue, most are lacking reliable policies and

tools to ensure compliance with pending regulations. Even with daily news about data breaches and hackers attacking businesses, almost half (47%) indicated that their organizations have no policies or controls limiting employee access to consumer-grade cloud storage and file-sharing systems.

Only 44% of survey respondents said that they currently monitor user activities and provide alerts to data policy violations, and only 53% classify sensitive information to align better with access control technologies.

Nations are taking necessary steps to protect the data of private citizens with legislation like the GDPR. But the side effect to this reform is that businesses are struggling to understand and properly prepare for their responsibilities.

In this new world, business leaders will need to be aware of different jurisdictions imposing inconsistent and often incompatible mandates in various nations. The GDPR will come into force in two years, and many more nations are likely to follow suit with their own regulations.

With all of these regulatory changes, organizations need technology options and subject matter experts, such as a Chief Privacy Officers or international legal counsel teams, to help them properly prepare for a whole new world where they are directly responsible for compromised data, no matter where it rests or travels.

About the Author

Ronald W. Hovsepian is president, CEO and director of Intralinks, a global supplier of secure collaboration solutions for highly regulated industries. Previously, Ron served as president and chief executive officer of Novell, Inc. Before that, he held management and executive positions at IBM Corporation. Ron currently serves as a member of the board of directors of ANSYS, Inc.

He was formerly a non-executive chairman of the board of directors of the Ann Taylor Corporation. In addition, he served as managing director with Bear Stearns Asset Management, a technology venture capital fund, and managing director of Internet Capital Group, a venture capital firm, during his 28-year career. Follow Ron on Twitter: @RonHovsepian.

Why Companies Need To Encrypt And Throw Away The Key

by Dr. Leo A. Guthart

Should the government be allowed to access encrypted messages? This is a national security and privacy rights tradeoff debate that we need to be having. What CANNOT be debated is the very different, and important, issue of the need for commercial enterprises to do a much better job of protecting their own data from hackers with evil intentions.

No privacy rights tradeoffs or governmental "back doors" are involved here.

Only a few weeks ago, VTech Holdings, the maker of e-learning toys for toddlers, admitted that hackers stole information, including names, birth dates, head shots and chat message logs for more than six million children and nearly five million adults. Not even children are safe when it comes to these types of breaches.

That is still relatively minor by comparison when you consider the 110 million customers who may have had their credit card or other personal data stolen in the 2013 breach of Target Corp., or the more than 80 million customer accounts at JP Morgan Chase that hackers were able to access in the largest bank breach ever just last year.

One common, and very dangerous, misconception many executives still have when it comes to cybersecurity is that they believe they can protect their systems with firewalls and related software in the first place.

Here is a reality check – not only can we not stop the hackers from breaching this "perimeter protection", but if it hasn't already happened, the chances are good that you, too, will fall victim to a breach.

According to IBM, there were one billion records breached in 2014 alone. Cybercrime now costs businesses in the U.S. up to $100 billion each year and that number promises to climb as hackers grow more sophisticated in their efforts.

Before you jump off the ledge, understand that just because you are vulnerable to being hacked doesn't mean your information needs to be at risk. New methods of data encryption can now solve this problem readily, with technology that allows for data, down to the smallest of levels, to be split and physically dispersed, making it completely unreadable to any prying eyes.

The fact that a relatively select few are employing this new technology when it is so readily available is worrisome.

The fatal flaw leaving companies exposed to security breaches is that many are protecting their networks and firewalls, **but not the data within**. This can be compared to a bank locking its doors at night, but leaving the door to its vault wide open.

At one time, that type of protection may have been adequate, but today, it will not prevent a breach from occurring. Once that happens, it is crucial to make sure that the data itself is encrypted and unreadable, not only to hackers from the outside, but to any insider threats that may exist. This type of "data-centric" solution should be the staple of every organization's cybersecurity plan.

Encryption cannot stop someone from accessing your information, but it does render that data unusable. This is important, also, when it comes to the very real threat of data manipulation, which continues to be a weakness of existing cybersecurity.

The results of such an act could have unintended and catastrophic consequences for utility grid uses of data right on down to cases of identity theft.

Of course, there are other types of critical infrastructure that is highly dependent on computers to function, and in the very terror-conscious world in which we now live, the thought of that control falling into the wrong hands is alarming.

Data encryption can, and will, help prevent billions of dollars in damage while also stopping hackers from destroying reputations and ruining lives.

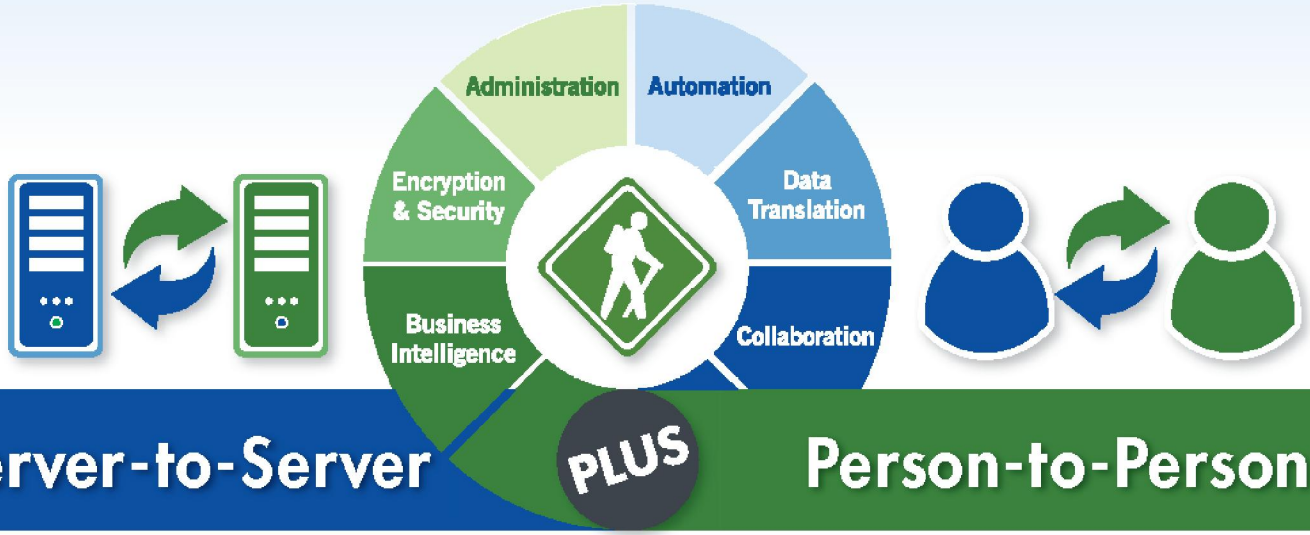
Each one of us is only a single unencrypted file away from disaster.

About the Author

Dr. Leo A. Guthart is a security industry veteran who served as Chairman of Honeywell's Security Group. He also served as Chairman of Cylink Corporation, a leading U.S. supplier of encryption equipment that was later sold to SafeNet, Inc.

He is currently Managing Partner at Topspin Partners Group.

Secure File Transfer



Simplify File Transfers with GoAnywhere MFT™

GoAnywhere Managed File Transfer automates and secures file transfers with your customers, vendors and enterprise servers.

Through a browser interface, GoAnywhere MFT allows your organization to connect to almost any system (internal or external) and securely exchange data using a wide variety of standard protocols.

GoAnywhere MFT can parse XML, CSV and XLS files to/from databases, and includes the ability to encrypt file transfers using Open PGP, SFTP, FTPS, AS2, HTTPS and AES.

Visit GoAnywhere.com for a FREE trial.

"GoAnywhere MFT monitors queues and automates encrypted file transfers (SFTP, FTPS, HTTPS).

We currently have 45,000 scheduled and 'triggered' transfers running daily."

One of the Largest North American Railroads

GO ANYWHERE™ → a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

"Best Overall Value" and "Leader" awards -- Info-Tech Research Group, Managed File Transfer Vendor Landscape Review 2015

How Hackers Find You and Do Their Hacking!

Many times companies will tell us that they will not get hacked because they are not big enough.

Your Size Doesn't Matter

This is an urban legend. What hackers do is look for a weak IP. This is an IP that has vulnerabilities and they do not care who owns the IP address. All they care about is that they can get into the network.

Many times, these hackers are like miners. Once they find a gold nugget (a weak IP address), they sell these IP addresses to big time hackers who use this information to obtain as much information from your computers as quietly as possible.

It is important to note that they do not alert you because then they can come back over and over again to obtain more and more information. Once they get in the sky's the limit!!

You last question is probably "Well, how DO they get IP addresses?"

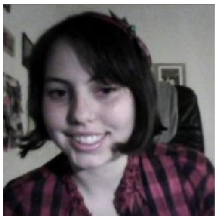
The answer is simple. They start out numerically from 0.0.0.1 and continue up until they find a weak IP address. It is true that many IP addresses are not "public addresses", but the hackers already know that. They just program their computers to begin at the first IP address and continue on until 255.255.255.255.

At this time, mathematically, there are only about 4.2 billion combinations for the entire world.

So the hackers just let their many computers do all the work while they just wait for their computers to spit out lists of weak IP addresses.

So you see, the hackers only care about weak IP addresses -- they don't particularly care who you are.

About the Author



Michelle Mocalis is the Social Media Marketing Coordinator for Oasis Technology and follows the latest trends within technology and cyber-security. She has a Bachelor's Degree in Business Administration with an emphasis in both Marketing & International Business. She can be reached at michellem@oasistechnology.com. Oasis Technology can be reached at 805-445-4833.

Decrypting the 4 Most Common Enterprise IT Security Myths

By Zoran Adamovic, CEO, HOB GmbH & Co. KG

According to SAP, there are more mobile devices than people on earth. Pew Research Center finds that 90 percent of people always have a mobile device within reach. A Gartner survey revealed that by 2017, half of the world's employers will not supply employees with computing devices; employees will provide their own devices as the workplace becomes more BYOD-oriented. Although technology seems to infiltrate every aspect of life, oscillating between personal and professional use, enterprise IT security is still a concept many are unaware of and, more importantly, are unsure how to handle.

As cybersecurity risks continue to grow in prevalence and severity, many myths arise about the best strategies for optimizing an organization's enterprise security. As such, businesses should take the steps to understand IT security risks, instead of wrongly heeding many of the enterprise security myths. Doing so will keep them from misusing resources and implementing ineffective enterprise security solutions for their specific needs. To help with this, outlined below are four common security myths, debunked:

MYTH 1: Hacking and malware cause the most data breaches

Although data breaches often have significant impacts and detrimental ramifications, hackers and malware are not always the cause. In fact, according to Trend Micro and PRC data analyzing cybersecurity in the last decade, hacking and malware caused only 25 percent of all breaches. The biggest cause of data breaches, accounting for 41 percent, was device loss or theft.

It's easy to forget that negligent activity can lead to data breaches. Something as simple as encouraging employees to use passcodes on their mobile devices, or remotely wiping a device's memory if it has been misplaced are easy solutions that can deter corporate data loss, malware and possible infiltration.

In BYOD workplaces, employees constantly communicate with corporate networks via personal devices. Because these devices alternate between professional and personal use, and since they are not tethered to a desk, they have a greater chance of being lost or stolen.

This is why businesses with BYOD policies should implement SSL or IPSec-encrypted secure remote access solutions. Solutions that facilitate access to corporate networks via a sandboxed mobile app prevent data from being lost or stolen, as data remain stored in the corporate network rather than on the device.

MYTH 2: All hackers are computer geniuses

One would like to believe that only geniuses can get past the security systems a company or individual has implemented, but this is not always the case. Hackers can take many forms. Yes,

they could be masterminds maliciously wreaking havoc on a system or stealing sensitive corporate information, but they could also be employees with legitimate access credentials.

Often careless employee practices leave sensitive information exposed and, although it sounds extreme, in some cases disgruntled employees may steal corporate data in an effort to sabotage the organization.

Businesses must be aware of all types of hackers in order to implement the most effective solutions possible. Employee IT security education and promotion is crucial, as well as ensuring that company software supports roles and right that can be granularly modified by a central administrator.

Software solutions that can ebb and flow with the size of a company's staff are an ideal way to prevent unfavorable situations with former employees.

IT specialists can easily add and remove software licenses as employees join and leave the company in these software-based environments and also restrict who can access certain silos of information.

This protects critical data by ensuring that the data remains in the right hands. With this system companies can make sure that someone in the marketing department doesn't have access to the construction plans or the medical information of other employees.

MYTH 3: Achieving 100 percent security is possible

While this notion is ideal, it's not realistic. According to CSO, the average business would have to increase its security budget ninefold to address only 95 percent of security threats.

Bombproof security measures might seem like a desirable solution, but they inevitably decrease the adaptability and ease of the system they are protecting, therefore becoming more cumbersome than valuable.

Business leaders need to find equilibrium between security and flexibility, thus addressing top security concerns while allowing for a changing and productive work environment.

While finding the balance between security and flexibility is difficult, it is not impossible. Remote access solutions can achieve this balance by:

- Ensuring highly secure data transfer with complex encryption methods.
- Meeting a broad range of transmission, saving and access requirements for various data locations such as an enterprise headquarters, branch office locations, home office locations and remote locations.
- Enabling seamless applicability and compatibility to facilitate program availability and platform independence.

MYTH 4: It's the number of attacks that matter

A common misconception is that if something occurs more times, it poses a bigger threat. However, more is not always better – or in this case, worse. A recent article in Wired noted, "Counting individual attack probes… is like counting bacteria – you get big numbers very quickly, but all you really care about is the impact and the source."

According to the Identity Theft Resource Center, from 2005 to 2015 almost six thousand data breaches occurred, exposing more than 820 million personal records – a large and intimidating figure. However, when analyzing cybersecurity, raw data is not enough.

Even though 820 million of anything is a striking number, these records encompass everything from obtained usernames and passwords to medical records and Social Security numbers. Thus, the vast variations of information that can be gathered make it futile to talk about the sheer number of data breaches.

Instead, a more useful approach is to analyze the severity of the breach and, more importantly, where and with whom the information ends up.

For Enterprise Leaders

In dealing with cybersecurity and keeping your data safe, it's crucial to be thorough and remain cautious. Implement strategies to ward off attackers and malware, but also be aware of "smaller" incidents that could lead to a data breach.

Understand that breaches are not always the results of malicious hardware and could actually be caused by something internal, or that could have been 100 percent avoided.

Enterprise IT security itself can be difficult to decode and is encrypted with myth. It's imperative to be aware of this when choosing a security solution for your enterprise.

About the Author

Zoran Adamovic, CEO, HOB GmbH & Co. KG

THE NO.1 INTERNATIONAL EXHIBITION FOR NATIONAL SECURITY AND RESILIENCE IN THE MENA REGION

ISNR

INTERNATIONAL EXHIBITION FOR NATIONAL SECURITY & RESILIENCE

15-17 MARCH 2016

ADNEC, ABU DHABI, U.A.E

www.isnrabudhabi.com

CROWD MANAGEMENT

THE FUTURE OF POLICING

BRINGING GOVERNMENTS, BUSINESS AND INNOVATION **TOGETHER FOR A SAFER WORLD.**

DISASTER PREVENTION

INFOSECURITY

JOIN 20,000 VISITORS AND 500 EXHIBITORS FROM 90 COUNTRIES AT ISNR ABU DHABI 2016

The MENA region's number one event in national security and resilience. In an ever more unpredictable world, ISNR Abu Dhabi is your gateway to five leading international events in one location, from emergency response to information security and beyond. All together in an awe-inspiring venue in the heart of Abu Dhabi.

HIGHLIGHTS FOR 2016

Impactful new events, content and connections	State-of-the-art innovation and breakthrough thinking	Future of policing and crowd management in action

REGISTER TODAY

DON'T MISS OUT. MAKE ISNR YOUR MUST-SEE SHOW. www.isnrabudhabi.com

Organised by: United Arab Emirates Ministry of Interior; Reed Exhibitions

Platinum sponsor: TRA Telecommunications Regulatory Authority

Featuring: Infosecurity Middle East; EMDI

Co-located events: FFME Fire Fighting Middle East; OSHME

@MOIUAE
www.moi.gov.ae

The Real Cost of This Year's Hot Holiday Tech

By Chris Rouland, Bastille Founder and CTO

The holiday season is here again and hot tech is once again poised to dominate wish lists everywhere. But unlike previous years when technology must-haves were reserved for gadget junkies, Internet connections seem to be creeping into everything from the crockpot for mom to the Barbie doll for your daughter. The Internet of Things and sensor technology has ushered in a new wave of connected devices, but the question that should be asked is, *are the devices actually gifts that keep on giving...to the bad guys?*

Be Wary of Wearables

Wearables, like fitness trackers and smartwatches, have seen steady adoption by consumers. This holiday season, fueled by the Apple Watch, consumer wearables might finally make the mainstream. In fact, IDC predicts that the wearable market will grow by 223% this year alone. Driven by shrinking prices and aging Millennials, 1 in 6 U.S. adults now own a wearable and that number will only continue to rise. Another boost to the wearable market has come from the Enterprise. Large organizations looking to encourage employee health and perhaps save a few bucks on insurance are now offering fitness trackers as part of their wellness programs. When was the last time you read the Apple update policy agreement? Consumers are largely unaware and unconcerned about the privacy policies that come with applications, products, and online activity. However, as we move towards integrating the Internet of Things into our lives, it's more important than ever to consider what we're sharing and how it will be used.

Quite simply – consumers are becoming the product.

While we may understand that giving up our email address is going to mean that we get more coupons and notifications from manufacturers, the average consumer doesn't understand that agreeing to the terms and conditions of most Internet of Things devices means that they open themselves up to a lot more than increased SPAM. Wearables, for instance, keep track of your daily activity. From location to steps taken to vital signs, these devices track the most mundane facets of your life. This may seem innocent enough until you begin to get offers from diet companies because your activity has decreased or coupons for new shoes because you have gone over one million steps. Perhaps even riskier is that many wearables have agreements in place with insurance companies as many large organizations are now using wearables as part of their wellness programs. What if your fitness band manufacturer decides to share this information and your premiums are affected?

This type of thing is usually spelled out in the product's privacy policy, but it can be fairly broad based and always favors the manufacturer. Generally speaking, they will reserve the right to share data in aggregate, for any reason that improves the product or service. This protects personally identifiable information – or should – but again, it's imperative to understand what data you're giving

away and how it could be used. In many cases, an individual's data, when sold to a third party, can be as lucrative as selling the device itself.

Be Mindful of your Network

The NEST thermostat is a virtual dream for travelers that have no idea when they will get home and want to be able to turn on the heat en route from the airport. Likewise, two of the hottest toys this year happen to connect to the Internet. In fact, many consumer devices from crock pots to wine refrigerators can be managed remotely from a smartphone. While none of these products have been the cause of catastrophe to date, the potential is there. We've seen baby monitors hacked, so it's no surprise that there should be some reservations around Mattel's Hello Barbie. After all, this Barbie remembers conversations and learns your child's behavior in order to enhance the interaction between toy and child. As these devices all make their connections to the Internet - and your home network - not only is the data at risk, but it opens up your home network to new mechanisms for a breach. If your family is looking at these toys in hopes of gifting Johnny and Jane with the hottest gadget to date, remember that the risks are there and no one wants to become the 'plaything' of hackers.

And it's not just fitness trackers that might be spying on you. Earlier this year news broke that Samsung's Smart TV is recording conversations and uploading the data to third parties to be transcribed. But the encroachment on your privacy doesn't end there. The TV's bizarre facial recognition capabilities allow the conversations to be associated with an individual. It is still unclear what Samsung plans to do with this information, but you'd better believe it will be sent out to third parties for marketing and sales purposes. What is even more concerning is the potential threat of this information getting into the hands of an adversary. Consumers need to worry, but these TVs are showing up in boardrooms too, making them attractive for advanced hackers targeting particular companies.

Prevention is Key

To prevent a home or an enterprise from becoming a hacker's wonderland, individuals and organizations alike must begin to take IoT security seriously. The threat is real and consumers need to understand the potential risks that IoT devices pose and decide whether they are worth those risks. For enterprises, policies and procedures must be put in place, as it is only a matter of time before they start to find compromises that are entering their networks through IoT devices.

About the Author

Chris Rouland is Co-Founder and Chief Technology Officer of Bastille a security solutions company focused exclusively on providing intrusion detection and vulnerability assessment for the Internet of Things (IoT). With more than 50 billion connected devices expected by 2020, Bastille is pioneering security for enterprise IoT with a committed focus on detecting and mitigating airborne threats.

Georgia hands out PII for 6 million voters in 'PeachBreach'

By Anna Wehberg, Sr. Marketing Director, Hexis Cyber Solutions

Proving that there are myriad ways to expose sensitive data, the state of Georgia botched its regular release of voter information data to include personally identifiable information like Social Security numbers and birth dates for 6.2 million residents of the Peach State.

A dozen CDs loaded with voter information

Dubbed "PeachBreach" by some commentators, this data breach happened in an oddly old-fashioned way. Employees at the Georgia Secretary of State's office manually sent compact disks of the information to 12 organizations that were signed up as yearly recipients. The CD of voter information went to a wide variety of groups. They included ones you'd expect to regularly ask for voter registration data, such as media outlets The Atlanta Journal-Constitution and Savannah Morning News. Atlanta's largest newspaper published photos of the CD that it received, on which was scribbled "Ga. statewide file, 10/15/2015."

Both major parties at the state level, plus niche political groups like the Southern Party of Georgia and Independence Party of Georgia also received copies. Even Georgia Gun Owner Magazine received the data.

These files, when released properly, include fields such as name, address, birth year, gender and which political party's primary the person most recently participated in. This year the records included data prohibited by state law from release, including driver's license numbers plus the above-mentioned Social Security numbers and birthdays.

Class-action lawsuit makes breach public

The breach only became public after the filing of a class-action suit against the state government became known.

The lawsuit said the wrongdoing by the Secretary of State's office wasn't limited to the breach itself, but that Georgia law states that victims of a data breach be notified. At the time the suit was filed, the plaintiffs allege "not a single Georgia citizen" had been told that their PII had been compromised.

Secretary of State Brian Kemp has already fired an IT staffer he blamed for the snafu, stating that the person did not follow internal rules.

"I have put in place additional safeguards to ensure this situation does not happen again," Kemp said after the breach became public.

It isn't clear when government officials realized the problem. The CDs went out on Oct. 13, but the Secretary of State's office might not have known about the illegally-compromised fields until the class action lawsuit was filed.

Will state spring for credit monitoring?

The dozen CDs containing illegally-disclosed data have been returned to the Secretary of State's office. While all 12 recipients have assured the government they made no copies of the data nor did they pass it along, Georgia voters are not happy.

"It's very, very scary," plaintiffs' lawyer Jennifer Jordan told the Journal-Constitution. "My information was compromised, and I was kind of dumbfounded."

It's commonplace in the aftermath of breaches for the organization responsible to pay for credit monitoring of its victims, however it isn't clear whether the state of Georgia will pony up in this case.

The episode shows that organizations must go beyond investing in trained IT personnel and buying up-to-date technologies. Having visibility of the evolving threat matrix and machine-speed notification of and response to hacking threats can be defeated by insider threats - even when that insider may have simply made an honest mistake.

About the Author

Hexis Cyber Solutions is a wholly-owned subsidiary of The KEYW Holding Corporation (NASDAQ: KEYW), and a provider of advanced cybersecurity solutions for commercial companies and government agencies.

Anna Wehberg, Sr. Marketing Director, joined Hexis Cyber Solutions in April 2014.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

Migrating to a Hybrid IaaS Environment: Look Before You Leap

How should organisations approach moving key business applications to the public clouds, while maintaining security and connectivity?

Nimmy Reichenberg, VP of marketing for AlgoSec shares his checklist of essentials

"The difficult, we do immediately; the impossible takes a little longer" is a phrase familiar to many IT teams. That's because they're used to senior executives making challenging demands, such as "Our competitors are making big savings by moving to the cloud, and we want to do that too.

So can we move our core business applications to the public cloud by the end of this year? It won't affect security, will it?"

If only it was that simple. Managing network security across a hybrid cloud environment is still an emerging area with many challenges, as highlighted in a recent AlgoSec survey that looked at the issues IT teams face in trying to unify security policy management across on-premise and public cloud environments.

Of the 360-plus senior IT professionals surveyed, 66% agreed that it's difficult for them to extend the corporate network security policy to the public cloud. Worryingly, a third of companies planning to deploy business applications in the cloud did not know which tools they will use to manage their network security policies after deployment.

So moving to a hybrid IAAS environment isn't something that can be done overnight – it needs preparation and careful management to ensure security is maintained. To help with preparation, here are 5 tips to help in devising a strategy for a migration.

Choosing the right security controls

There are three basic methods to secure network access on public clouds. Commercial-grade firewalls for the public cloud are available, but the level of support and functionality varies greatly between vendors.

Their benefits include unified management with their respective on-premise firewalls as well as familiarity with how policies are defined and enforced. Cons include cost (although some vendors are now offering pay-as-you-go or bring-your-own-licenses pricing models), scalability and a limited feature-set for some vendors.

Alternatively, some cloud providers will provide their own security controls (e.g. Amazon Security Groups). These controls are generally free – which is always attractive – and provide a good level of functionality.

However, they may lack enterprise-grade management and do not work across different cloud providers since every provider's controls are different.

Then there are host-based firewalls, which can offer an effective cross-cloud solution, but can involve additional security management overhead and a limited feature set.

Network security controls in the cloud are still fragmented, and there is no single correct answer when it comes to selecting the best option, so make sure you carefully evaluate the options and choose the controls that best suit your business needs.

Visibility across the cloud

Without visibility across hybrid cloud environments, you can't see what's going on, let alone secure it effectively.

Regardless of which security controls you choose, visibility is key to a successful migration and deployment.

Make sure you implement controls that provide visibility across the entire hybrid environment.

Automate to improve security processes

Security automation goes hand-in-hand with visibility, and is the key to effectively migrating to and managing a hybrid environment – especially given the flexibility offered by cloud environments as, when you're trying to manage hundreds or even thousands of policy rules, automation is the only way.

Manual processes for security change management would simply be unable to keep up with the constant updates needed across a large, hybrid infrastructure.

Automation helps to reduce unexpected business outages caused by changes, speeds up application deployments in the cloud, and also eases inter-team working.

Segmentation, segmentation, segmentation

The cloud creates a much wider attack surface for your organization. So as network segmentation is critical to security in the on-premise data centre, to stop infections and attacks spreading, it's doubly critical for hybrid environments.

Make sure you lock down access to your internal corporate networks from the IaaS platform as much as possible.

This will not only cut your exposure to risk, but will also improve incident response by enabling you to quickly identify and focus on any emerging issues – helping to reduce the scope, time and effort involved in security audits, which your IaaS-based applications will now be subject to.

Owning security

While enabling the different teams to work together using automation tools is critical to an easy migration and successful deployment of a hybrid cloud environment, it's also important to ensure the right team is leading security efforts.

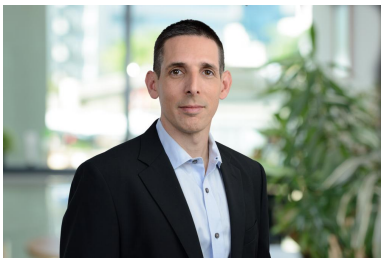
Our survey found that large and small companies were uncertain about where responsibility for security in hybrid cloud environments should lie: with the Information Security team, IT operations, or with platform providers?

It depends what best suits your organisation, but make sure that someone takes responsibility.

These points can help you keep security front-of-mind as you evaluate IaaS platforms and plan your move to a hybrid cloud environment – in turn making the move easier, while ensuring you can maintain a strong security posture.

www.algosec.com

About the Author



Nimmy Reichenberg - *VP Marketing and Strategy*

Nimmy Reichenberg has over 10 years' executive marketing and business development experience in enterprise technology. Prior to joining AlgoSec, Mr. Reichenberg served as the VP of Worldwide Marketing and Business Development at NextNine. Previously Mr. Reichenberg held various product management and marketing roles at M-Systems (acquired by SanDisk) and founded the marketing department for the company's enterprise security solutions.

Mr. Reichenberg is a frequent speaker at information security events and a regular contributor to industry publications. Mr. Reichenberg has a B.Sc. in Computer Science and an MBA.

The Highlights & Takeaways of CyberMaryland 2015

By Todd Weller, VP, Corporate Development, Hexis Cyber Solutions

The CyberMaryland 2015 Conference took place at the end of October in Baltimore this year during its an annual two-day event presented jointly by The National Cyber Security Hall of Fame and Federal Business Council (FBC) in conjunction with academia, government and private industry organizations.

Those attending were able to network, attend seminars and hear speeches from top cyber security professionals discussing the latest news and industry trends.

My experience from the event this year validates that next generation endpoint is heating up, focus is shifting to detect and respond from prevent, and integration and automation are becoming more critical.

Below are my takeaways from the opening keynote and the sessions I attended.

Opening Keynote Discussed Nation State Adversaries, Active Cyber Defense and Cyber Resilience

The opening keynote speaker was Philip D. Quade, Special Assistant to the Director for Cyber and Chief of the Cyber Task Force, National Security Agency. Key points included:

- The first wave of nation state attacks represented unsophisticated activity. Phase two is coming and will be marked by more sophisticated, coordinated attacks. Low and slow advanced persistent threats (APTs).
- China is interested in gaining economic advantage by stealing IP, as well as looking to gain control of critical infrastructures. Russia is very good at doing intelligence and motivated to impact critical infrastructure.
- Sharing threat information is becoming more critical as there is no individual company capable of taking on China on their own.
- The NSA's Active Cyber Defense effort was highlighted. This is referred to as SHORTSTOP. This represents a reference architecture consisting of multiple, best-of-breed advanced threat solutions.

The current architecture includes Palo Alto Networks' Next Generation Firewall, FireEye's network sandbox, Hexis' HawkEye G solution for next generation endpoint detection and response, and Splunk as the command and control layer.

- Mr. Quade also highlighted the importance of auto resiliency and auto regeneration. In a recent interview, Mr. Quade defined resilience as "the ability of a system to recover and resume operations, or to continue to operate, in the face of adversity."
- In the same interview, Mr. Quade indicates "Automation - specifically, real-time orchestration and integration of a variety of security products - is an approach starting to be leveraged in cybersecurity efforts to auto-harden and auto-defend our networks.

  Even with that in place, it is inevitable that our networks will be attacked. So, auto-resilience is the next logical step to enabling speed in systems recovery and maintenance of functionality."

Reduce Your Risk of Compromise Through Integrated & Automated Active Cyber Defense

This panel focused on the aforementioned SHORTSTOP reference architecture and was moderated by Patrick Arvidson, Director for Defending DOD Networks and Mission Assurance OSD, Office of the Principal Cyber Advisor and Russell Glenn, Director Cybersecurity, KEYW Corporation.

The panel included representatives from FireEye, Hexis Cyber Solutions, Palo Alto Networks, and Splunk.

- The future of cybersecurity lies in leveraging automation and integration.
- A fog of alerts makes it challenging to detect and respond to APT attacks.
- A government agency that is adopting the Active Cyber Defense architecture has experienced an 80% efficiency improvement on day to day routines. They were able to take 12 front line defenders down to 3 with the other 9 now focused on doing hunt operations.
- The most vulnerable part of environments is users and endpoints.

The Evolution of Security Innovation and What is Next? — Panel

- Prevention is not working well because it's based on having prior knowledge of what attacks look like.
- Prevention is more than taking foreknowledge or intelligence and configuring tools it's about containing a breach.
- John Pescatore of SANs hits the nail on the head indicating that there's a difference between containing a breach and containing malware. It's about removing the threat before it does damage. Prevention is preventing damage not APTs getting in.

The State of M&A in the Cyber Market – Maria Lewis Kussmaul, AGC Partners

- There's a heavy focus in the market on reducing the time to detect and respond before damage is done.
- Buyer focus is shifting to detection and response from prevention.
- Next generation endpoint security is hot.
- A recent PwC survey indicated that security budgets are up 24% in 2015 driven by a 38% increase in security incidents.
- Security industry leadership is now up for grabs as next generation players battle incumbents.
- Demand for effective countermeasures is strong.
- Cyber investments and M&A pace will continue at a more discriminating pace and with more disparate outcomes.

This event provided a lot of great insight on the industry and I highly recommend that anyone interested in the future of cybersecurity check out CyberMaryland 2016 next fall.

About the Author

Hexis Cyber Solutions is a wholly-owned subsidiary of The KEYW Holding Corporation (NASDAQ: KEYW) , and a provider of advanced cybersecurity solutions for commercial companies and government agencies.

Todd Weller, VP, Corporate Development, joined Hexis Cyber Solutions in March 2014. His responsibilities include analyst relations, competitive and market intelligence, corporate visibility, M&A, and strategic partnership development.

Todd draws on his 17+ years of experience as an equity research analyst where he covered the security industry for much of that time. In his equity research career Todd provided research coverage of over 60 companies across several technology sectors, including security, infrastructure software, data center/cloud hosting, and healthcare IT.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

ufi Approved Event

e.oman

Be a part of Oman's only ICT show

.comex

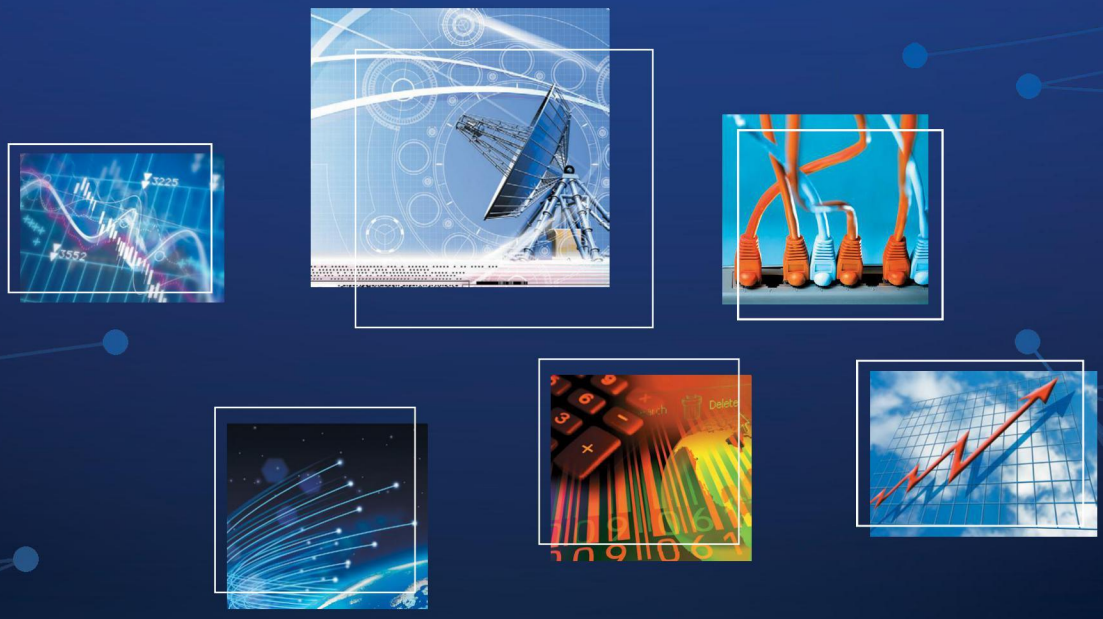
IT, TELECOM & TECHNOLOGY SHOW

26-28 April, 2016

Oman Convention & Exhibition Centre

Muscat - Sultanate of Oman

www.comex.om



For more information on COMEX 2016 Contact

Ashit Barnes
Exhibition Director
+968 9934 1687
barnes@oite.com

Ahmed Farag
Sales Manager
+968 9912 7806
a.farag@oite.com

Research Partners

OXFORD BUSINESS GROUP

Official Magazine

PC

Media Partners

TCM Tech Channel MEA

Telecom Era

Global Security Mag

SECURITY MIDDLE EAST

SSN

Central Asian Cellular Forum

CDM Cyber Defense Magazine

Cyber Security Review

Tedge news.com

Education Technology

DIGITAL FORENSICS / MAGAZINE

Developing Telecoms

Mobilk

Eye Of Dubai

Eye Of Riyadh

Communications Today

Organiser

OITE TRADE FAIRS

www.oite.com

Apoc@lypse: when the anti-malware is sick.

By Rogerio Winter, lieutenant colonel at Brazilian Army and Rodrigo Ruiz, researcher at CTI Renato Archer.

Are you sure that your systems are protected?

Several countries recognize that cyber threats can reach a national threat threshold leading to a state that prevents prosperity, security and stability. Notably, the anti-malware and antivirus systems have played a key role, just over 30 years in the defense of several companies' information systems, government and military. However, the anti-virus systems has suffered a large number of critical due to the efficiency of these. In 1987, Fred Cohen demonstrated that no algorithm could detect perfectly all the possible viruses. This was a very discouraging observation when we thinking about antivirus. Other people recently declared, "Antivirus is dead".

The antivirus concept was changed to the anti-malware concept, however antivirus is the most widely known. Inside the anti-malware is embedded a threat detection system which the signature-based technology is one of the most popular technologies against virus and malware.

The different anti-malware software makers announce new and efficient technologies that claim to offer better performance and cheaper answers us with malware security incidents within organizations. Clearly, there can be a technology that is faster, better and more efficient than all others. Our research went back to the basic beginnings, to the DNA of the antivirus. We questioned the paradigms now consolidated in the software through four decades, revised the history of the development of this software, and started to carefully study the common nucleus. Making an analogy to the human body, the fault is in the DNA of the ancestors of the modern antivirus software.

The use of terms like infection, incubation, and disease in the context of information security suggests a similarity between computers and biological virus, a logical parallel. The similarity between the virtual world and the reality is notable. Solutions to fatal computer problems were inspired by the observation of nature itself. In this way, we can establish a metaphor between human body and cyber body, particularly of the system protect. An autoimmune disease occurs when the human immune system has a fault, and it attack cells and tissues of the organism itself in the same way as a virus or a bacterium tries to infect a human body.

All the antivirus software on the market have the same algorithms in common. In other words, the methodology that compares signatures of the virus was created almost three decades ago. The virus classification is made by signature without considering the behavior of the virus.

What is not Apoc@lypse Technique?

The Apoc@lypse Technique is not a malware. Malware is malicious software that infect computers; however, they have a more limited range in terms of operating system, anti-malware vendor and time.

What is Apoc@lypse Technique?

We call the first autoimmune cyber disease, because the Apoc@lypse technique is a trigger for start the autoimmune disease in computer. Autoimmune disease in human is a disease in which a person's immune system wrongly attacks its own healthy tissues. The Apoc@lypse technique is a generic and extremely efficient way to bypass the protection of the anti-malware system. The technique explore a vulnerability that exist in the signature-based technology of the anti-malware and it allows infecting in the furtive form a machine target. We injected tens and hundreds of malware pieces of DNA known benign files in the system itself without any action of anti-malware. All file types are susceptible to action infection the Apoc@lypse technique, such as file system, user system or software. We can use any part of the malicious DNA and some antivirus will be affected and others not. However, a special DNA affects all antivirus. This is EICAR Anti-Malware Testfile, because all antivirus recognize it as a virus or malware but this is not a virus. The test file simply displays a text message and returns the control to the operating system. After infection, the anti-malware system started autoimmune cyber disease and all files infected was deleted from system.

The signature and hash identify and distinguishes the appearance, and not the attitude, of software. Even the heuristic concept carries with it the detection of several indicators of a signature or stereotype of a threat. The Apoc@lypse Technique is implemented in software and it allows choosing between several existent forms of infection.

Apoc@lypse Technical Potential

Anti-malware system are inefficient when we use Apoc@lypse Technique against system. The Apoc@lypse Technique undoubtedly will contribute to bring the system into more disrepute and discouraged users from using it. According to, The Global State of Information Security® Survey 2014 of PWC , the companies have invested in cyber security, but they are not accompanying the evolution of his current adversaries. Nowadays, we are trusting in model security created in the past to struggle present threats.

Proof of concept

We demonstrated that is possible to take control of anti-malware system and to command operating system destruction. The Apoc@lypse Technique proof of concept is more effective in Windows Operational System, but for the other operational systems (Linux, Android, UNIX e Mac) the effects can be less catastrophic. The Apoc@lypse technique explore undisclosed vulnerability in the anti-malware systems. Technical efficiency of Apoc@lypse were successfully tested in 157 anti-malware system existing in the international market. In figure 1, we present the geographical distribution of anti-malware companies in the world used in Apoc@lypse test bed. The technique Apoc@lypse is efficient in various versions of Operational System Windows 32 and 64 bits.

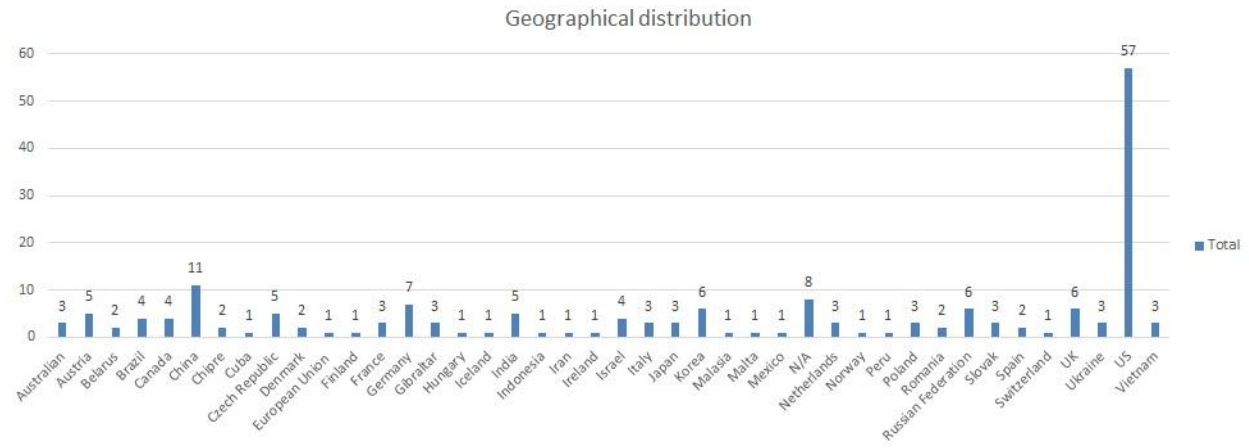


Figure 1 Geographical distribution anti-malware companies in the world. Source: authors.

Apoc@alypse technique corresponds to the end of the systems of signatures and hashes to identify threats against the security of information, since the system distinguishes and identifies the appearance, and not the attitude, of software. Even the current heuristic concept carries with it the detection of several indicators of a signature or stereotype of a threat.

How will Apoc@lypse influence the defense of military systems, bank systems, and controllers of infrastructure? As common systems are weakened, too many systems use computers with antivirus and anti-malware protection, and it may cause an avalanche and compromise the functioning of too many systems.

About the Authors

Rogerio Winter is a signals officer in the Brazilian Army who occupied multiple positions in network administration, command and control, electronic warfare, and cybersecurity. He received his master degree in Electronic Engineering and Computer Science from the Institute of Aeronautical Technology (ITA), Brazil. Currently, he is an Army Liaison Officer at the Center for Information Technology Renato Archer, Government Advisory Committee in IT-SA Brazil, and book´s coauthor “Apoc@lypse: the end of antivirus”.

Rodrigo Ruiz has discovered the vulnerability Apoc@lypse and carried out a digital bacterium to transport and inoculate the DNA of viruses in computational systems. He was the first one to draw the parallel between autoimmune cybernetics and disease, which is the basis of this book, and he created the proofs of concept. Rodrigo is book´s coauthors “Apoc@lypse: the end of antivirus” on.

EXHIBIT IN 2016

SSS
Saudi Safety & Security
2016

Saudi Arabia's leading security, fire and safety exhibition

16 - 18 May 2016
Dhahran International Exhibitions Center,
Dammam,
Kingdom of Saudi Arabia



The SSS 2016 international exhibition will play host to innovative and pioneering technologies and products aimed at overcoming security, safety and fire issues. Saudi Arabia is now one of the world's fastest growing markets for security and safety solutions, making the SSS 2016 exhibition an ample opportunity for companies to network with private companies offering solutions in the fire, safety and security space.

> "A great launchpad for getting collaborators/prospects/potential clients in the Middle East region together. The perfect event for safety professionals."
>
> Neclilae Edcuard,
> Marketing Manager, Invictus (Adina SRL)

2015 PARTICIPANTS

Want to exhibit?

Please contact Mostapha Khalil E: mostapha@bme-global.com T: +44 203 463 1097

Previous Supporters

2015 Sponsors

Official CPD Member

Organised by

Official Production House

Official Housing Agent

2016 Media Partners

www.sss-arabia.com

Follow us on Twitter: @bmeevents
For all the latest news: @SSS_Arabia #SAUDISECURITY2016

Three Lessons We Can All Learn from the Securus Technology Hack

Chris Pogue, Senior Vice President, Cyber Threat Analysis, Nuix

The recent news that telephone service provider Securus Technologies was hacked, just another in a long line of companies to make this dubious claim, got me thinking more than usual about the lessons that everyone should be learning from stories like it. Admittedly, part of my job is to pay close attention to breaches and hacks in every industry, but this one crossed some very interesting lines that I think will have some interesting repercussions to legal service providers.

As background, Securus Technologies provides a service it calls "Secure Call Platform" to prisons in the United States. This service allows for monitoring and recording of calls to and by inmates in these institutions, something I think most people wouldn't have any issue with. After all, these are convicted criminals—their privacy rights are forfeit upon criminal conviction and incarceration. Even the people they are talking to are given notice that the phone calls are being monitored and recorded, so there is no expectation of privacy.

What I believe to be the major issue is that a company that touts a "secure" service has all of a sudden found itself looking at the compromise of more than 70 million records of phone calls. Reportedly, those records include: the inmate's name, the numbers they called, the date, time and duration of the calls, and other metadata. It doesn't stop there, however; the compromised records, which were leaked by an unnamed hacker, contain links to recordings of the calls.

While it doesn't sound any different from other breaches or data leaks that have been in the news, there are some important legal concerns that surface we look more closely at the Securus breach.

Lesson 1: Unfair or Deceptive Practices

I hinted at it above—companies have an obligation to be honest with their potential customers about the services they provide. When a breach occurs, organizations are increasingly being scrutinized for their defensive countermeasures, but also to see if they engaged in unfair or deceptive business practices. The FTC, in particular, has recently become much more aggressive in its probing of organizations that have suffered a data breach.

We don't know how the Securus breach happened yet—it's much too early to know that kind of detail and they have not made any public announcements with the specifics of the attack. That being said, there has been an alarming trend among breached organizations to overstate the complexity of their incident, while understating the impact. If this breach follows suit, things are going to get a whole lot worse.

Based on authority given to the FTC under the Federal Trade Commission Act, we can logically assume that Securus will be held accountable for advertising its "Secure Call Platform" in some manner as untrue. The sad reality is that even a secure system can be compromised if even an

employee makes one mistake. There are many low-tech ways to hack a system, including tricking an employee into giving up a password through a fake email (phishing) or by phone (social engineering).

Another recent breach sheds light on a true case of deceptive business practices. When online dating service Ashley Madison ended up in the spotlight just a few months ago, the company's "paid delete" service suddenly came under intense scrutiny. By opting for this service, users paid Ashley Madison $19 to fully delete all of their account information.

However, when user information made it into the public domain due to the breach, it suddenly became very clear that not all of the user records were deleted. For a company that brokers in intimately private matters like Ashley Madison, this is a very big deal indeed.

The lesson: Organizations must pay close attention to their marketing and business practices *as well as* their defensive posture. A breach and subsequent press coverage will cost a company millions of dollars but not just in the areas we typically attribute to cyber-attacks. It will open doors that the company may have preferred to keep shut, shining a glaring light into the darkest corners of every closet and potentially revealing some very damaging skeletons hidden within.

Lesson 2: The Uncertain Nature of "Reasonableness"

Reasonableness is a difficult concept to quantify, mainly because it is so open to interpretation. When they are breached and ultimately end up in litigation, organizations need to prove that they took reasonable measures to protect themselves and their customers' information. I could go on for pages on this topic alone, and that's part of the problem—while an organization can argue that it took what it believed to be reasonable measures to defend against an attack, an opposing counsel can just as easily bring up all manner of other "reasonable" practices that the organization could have followed. At that point, it becomes a battle of the experts.

The lesson: Many organizations prefer to handle all their security in-house. Ultimately, this puts them behind the curve when it inevitably comes time to defend their actions after a breach. Partnering with industry-recognized security experts can help organizations build a defensible position upon which they can argue reasonableness when the time comes.

Lesson 3: Privileged Communications

I saved this point for last, because it raises two distinct points of concern. The Securus breach includes a subset of telephone conversations between the inmates and their attorneys—conservatively estimated at about 14,000 conversations—some of which are more than likely confidential and privileged legal communications. These conversations should never have been recorded and, in fact, Securus claimed that privileged calls were exempt from the recording and monitoring service that they provided.

We've already covered the point about unfair or deceptive business practices, and from my perspective this has every appearance of a deceptive practice. When a company says that it won't record calls that would violate constitutional protections, but records them anyway, the term "deceptive business practices" is an understatement.

By extension, I started to think about the legal realm and something that is kind of an ill-kept secret in the security profession. Law firms have become vast repositories for very sensitive information and, as a result, are incredibly likely targets for attack by hackers. However, the big news about information breaches and compromises centers on well-known, big-name corporations. If law firms are such likely targets, doesn't it stand to reason that they are being attacked?

The answer, not surprisingly, is yes. Earlier this year, the New York Times cited a Citigroup report which claimed "The unwillingness of most big United States law firms to discuss or even acknowledge breaches has frustrated law enforcement and corporate clients for several years." This reluctance to talk about breaches makes it near impossible to gauge whether these kinds of attacks are on the rise, the report acknowledged. However, the message is clear that it's an issue firms should take seriously.

The lesson: While breach notification laws currently vary by state, it's only a matter of time before an overarching regulation is adopted on a federal scale. The days of law firms hiding breaches from the public are bound to come to an end, especially if a large firm is discovered to be a breach victim.

For some reason, lawyers and their firms either won't admit or don't believe that they are vulnerable to an attack. The time has come for them to understand that the data they retain is of tremendous value on the black market. Logically, that means somebody, somewhere will try to steal it. Law firms must take seriously the protection of their clients' data. Just like the corporations they work with, they need to seek the services of security experts to help defend against attack.

Every breach in the news has some lesson that other organizations can learn, if they are willing to listen and admit they have a problem. By the time the truth of the breadth and the depth of the incident eventually comes out, the poignancy of the lesson has often passed us by, but it's still there and should be heeded. After all, the best mistakes to learn from are those other people have made. It's less painful that way, but still just as effective.

About the Author

Chris Pogue has more than 15 years' experience and 2,000 breach investigations under his belt. Over his career, Chris has led multiple professional security services organizations and corporate security initiatives to investigate thousands of security breaches worldwide. His extensive experience is drawn from careers as a cybercrimes investigator, ethical hacker, military officer, and law enforcement and military instructor. In 2010, Chris was named a SANS Thought Leader.

2ND ANNUAL
CYBER SECURITY
FOR OIL AND GAS
CANADA

January 25-27, 2016 – Calgary, AB

THE RULE OF FOUR

The 4 main reasons why cyber attacks are growing in popularity

Inexpensive – Many attack tools can be purchased for a modest price or downloaded free from the Internet;
Easy – Attackers with only basic skills can cause significant damage;
Effective – Even minor attacks can cause extensive damage; and
Low risk – Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes.

Top 4 strategies to stop targeted cyber intrusions

Application whitelisting. Allow only specified programs to run and block all others, including malicious software.
Patch applications. Reduce the number of exploitable entry points by patching with the latest updates to applications such as; Java, PDF viewers, Flash, web browsers and Microsoft Office.
Patch operating system. Update regularly and when prompted in order to reduce the number of exploitable entry points.
Restrict administrative privileges. Restricting users' administrative use prevents the spread of malware in the network.

Are you under threat?

Signs of an Advanced Persistent Threat (APT)

Unexpected encrypted traffic leaving your organization or large, outbound data transfers via http/https
Unauthorized logins to critical network devices
Unexplained remote access activity
Unusual web communications, DNS resolution and user agent strings

Be aware. Prevent the risk of APTs

Education and awareness - Only open emails from known users, beware of attachments or hyperlinks or correspondence from non-professional, personal Gmail, Yahoo and Hotmail addresses.
Configure systems securely -Minimize administrative privileges, whitelist applications, encrypt data and disable unnecessary services.
Maintain the network perimeter -Deploy an e-mail gateway and web content filter and actively monitor perimeter devices.

What's next? **Speaking Session By**: Jim Love, CIO/Chief Digital Officer, IT World Canada
January 26th, 3:00 PM
Creating A Security Culture
From social engineering to simple carelessness, employees and executives create gaping holes in an organization's security protection. How can organizations deal with this? What strategies work and don't work?

Approaches to mitigate risk and threats

1. Industry awareness on critical infrastructure protection
2. Incident response: proactive vs reactive approaches to examining the latest threats in 2016.
3. SWOT analysis on the rise of cyber insurance policies.
4. Tracking and trending what we know about ICS regulations in 2016.

How can we help? **Speaking Session By**: Matthew Harper, Director, Info. Security, Devon Energy Corp.
January 27th, 10:00 AM
Fostering the relationship between ICS and IT
Processes and procedures behind the increasing need for security

Source: www.publicsafety.gc.ca

Cyber Predictions

Amir Orad

If there's one thing that stays consistently top of mind for CIOs and business leaders, it's security. As enterprise technology evolves and new technologies, such as wearables, hit the market, there are new security threats and vulnerabilities for cyber criminals to target – but also new ways that organizations can protect against attacks.

Every organization needs to consider how they can leverage the latest technologies and security analytics to protect their business. From retail and finance to healthcare and media – no industry is safe from the potential risk of security breaches and data theft.

Cyber security risks will be a core focus for IT and business leaders in 2016. As a result, we'll see more organizations implementing technology and analytical solutions to monitor, identify and mitigate these risks.

Managing security analytics is a challenge many IT organizations face, but in 2016, many organizations will improve with technology tools to overcome these challenges and maintain secure, compliant organizations.

More organizations will rely on data analytics to increase overall umbrella monitoring.

For companies that have large, complex data sets coming from many different security monitoring sources, data analytics can be a useful tool to see the overall picture.

To gain a better understanding of what is happening across an entire network, in 2016 more companies will implement tools that allow for easy data mash-up, supporting analysis across the entire network and across all security related applications.

"False Positive" threats will distract from real ones.

Many existing security systems have binary outcomes, generating too many false positives that either waste resources or cause the companies to ignore real threats because of the volume of items flagged.

In 2016, companies will consider learning algorithms that look at multiple variables, like user role, time of day, etc., to help differentiate between legitimate and suspicious behavior. These algorithms will help weed out the false positive scenarios that overwhelm and distract from real threats.

More organizations will use pseudo environments to distract cyber criminals.

In 2016, more organizations will take advantage of creating pseudo environments to lure in hackers and trap them in a fake network. By mimicking a real network, businesses can confuse the attacker and spend time tracking culprits without threat of real loss.

Industrial Systems will see tremendous growth in cyber security solutions.

These systems have their origins in cyber security for power plants and utilities – systems that had national security implications. Today these threats are more ubiquitous and impact all Industrial systems. As a result, there will continue to be growth for cyber security solutions in this area.

As more and more companies rush to market with IoT solutions, there is a ripe opportunity for hackers to exploit new vulnerabilities in connected devices.

We will see more examples of threats targeted specifically at IoT as proof points, such as hacking into thermostats and refrigerators. To be secure, buyers should inquire about the different protocols IoT vendors are putting in place to monitor and prevent cyber attacks.

In 2016 we expect to see even more sophisticated hacker technologies and strategies, resulting in more enterprise vulnerabilities and compliance concerns. However, we're also seeing advances in the technologies to help protect against these vulnerabilities, keeping organizations safe from breaches and attacks.

In 2016, in order to keep sensitive corporate data safe, there will be more and more demand to invest in analytic and visualization tools that can help end users process the huge data sets related to these cyber threats, giving organizations the visibility to track, mitigate and protect against cyber criminals.

About the Author

Amir Orad is a successful CEO, entrepreneur and a big data technology thought leader. He brings proven success in leading and scaling businesses by orders of magnitude in both start-up and public company settings as well as multiple exits and M&As. Prior to Sisense, Orad was the CEO of NICE Actimize the financial crime and analytics software leader monitoring billions of transactions at the world's top institutions. Orad led the company's business functions since it was a $30M business, first as EVP and later as President and CEO. Under his leadership the business grew over six fold with Wall Street reported revenue nearing a $200M run rate. Prior to Actimize, he was Co-founder and CMO of Cyota Inc, a cyber analytics-powered company that was acquired by RSA Security in 2005. Following the acquisition, he was VP Marketing at RSA.

Mr. Orad holds an MBA from Columbia University's executive program (Beta Gamma Sigma) and a BS in Computer Science and Management from Tel Aviv University. Amir is a founding board member at BillGuard, the personal finance analytics mobile app company. He is a thought leader in the application of big data and analytics, and as a frequent lecturer and author he is often quoted in WSJ, The Guardian, CNBC, and BBC.

Consumer tracking by advertisers: an emerging threat to corporate data networks?

Are you annoyed by ads that keep following you on the internet? You are not alone. Like millions of other consumers, you have allowed websites and their advertising providers to track and share your online activity.

When you unwittingly accept a website's terms and conditions by clicking on the "I Agree" button, you grant the site permission to place trackers and cookies in your browser. Just visit a news site, and you will discover that the site and its advertising partners place upwards of 45 cookies and trackers on your device to start tracking your activities from then onwards…

Simply put, websites, even trusted ones, share your online profile, likes, dislikes, browsing behavior and buying history with their "marketing partners" including ad platforms and data brokers everyday. Most data brokers and ad platforms are companies you haven't heard of and certainly don't implicitly trust.

The Federal Trade Commission in its recent consumer online privacy report states data brokers may have aggregated up to 3000 items of online and offline information on each of us, including our name, address, mortgage and financial information and even the items of grocery we bought recently to create profiles. These profiles are sold to advertising platforms and websites to generate targeted ads and contents tailored to your profile.

What does this mean to you as a consumer? When businesses share your personal data, you see only what the website wants you to see, including targeted content, pre-selected products, demand pricing, etc.

We are inclined to think targeting is good, since we are shown products that we are interested in, but that's is not necessarily how it works.

Imagine if all the products that you are shown are the most expensive ones just because you bought a sports car for $100,000. Imagine people with health or disabilities- they need to worry about their profiles that includes their health and buying history being shared with unauthorized parties and possibly prospective employers.

Meaningful and pertinent ads don't bother most people. They know that ads keep bloggers/publishers/ merchants in business. It is the tracking/profiling/targeting by untrusted sites that bothers them. At some point targeting and customizing, crosses over into a form of surveillance.

A recent Pew Research survey indicates 9 out 10 Americans feel they have lost control over how companies collect and use their data. The same survey indicates that 93% of the respondents want to take control of their online privacy including who views and collects their data and guarding against "e-stalking" by untrusted sites or data brokers.

Fortunately, some websites are unlocking their platforms to allow consumers to delete their profiles. Also, anti tracking solutions from companies like PrivatizeMe, keep user's browsing and search history from being tracked by e-stalkers is now available.

How does advertising related tracking affect corporate information security?

With the risk of cyber-theft and data loss on the rise, corporate security personnel have focused on securing their applications and networks, firewalls and intrusion detection, without much attention to browser related trackers.

With employees bringing their own devices to work and using corporate laptops, increasing a larger share of the corporate employees browse and search using public networks at cafes and airports as well as home networks that lack sophisticated firewalls.

As they surf the Internet, visit sites and see ads, they are tracked by thousands of sites, including third parties. A device used "in the wild" brings all of this and more when connected to the corporate network.

This is where the trouble begins: some bad actors may partner with unwitting websites or may introduce trackers embedded in ads into user devices. These bad actors could include competitors, sovereign governmental spies, identity hijackers and even intellectual property thieves.

Imagine if some bad actor placed trackers in ads on popular websites. These ads are usually served by third party ad platforms. They can introduce these trackers onto user machines as users go about surfing popular websites and view or click on these ads.

Over time bad actors can track tens of thousands of users. Assume for a moment your company employs a few of these users and the bad actor wants to infiltrate your company.

They can use the trackers and the company IP address to target specific users and set up honeypots or info sites to lure these targets. These honeypots may be informational sites with work related topics, such as white papers, that may be of interest to the targeted users.

The white papers could introduce sleeper malware into the user's devices designed activate behind the corporate firewall to infiltrate your network.

Another technique is to craft targeted malicious advertisements. These maladvertisements may be directed at specifically targeted users using standard ad targeting or techniques described above. Published reports show well-known sites such as Drudge Report, Yahoo and Google's DoubleClick have served maladvertisements in 2015.

This sleeper malware may activate itself once the user is inside the corporate network to case it. Over time this may result in data loss resulting in identity theft or even intellectual property theft.

We recommend corporate network administrators deploy products or trusted services that thwarts e-stalking by untrusted sites yet enables meaningful ads on all employee devices. Corporate

network administrators could justify such privacy protection tools since they benefit both employees and corporations.

Solutions may include browser software and services from ad blocking companies, which block all ads, or installing internet security software on the user's devices.

But, blocking all ads may lead to unsatisfactory user experience and impair the site's operation, as some websites refuse to operate with ad blocking software turned on.

From the user perspective browsing and search still work, while ads still remain relevant and the user information leakage is controlled.

From a corporation perspective PrivatizeMe limits user tracking and targeting by outside entities.

PrivatizeMe provides free tools and search service that stops e-stalking by untrusted websites/bad actors, while users are browsing at work, home or on unsecured public networks.

About the Author

Ajit Pendse is the CEO of PrivatizeMe, LLC. He is a seasoned entrepreneur and innovator who has turned internet/computing/communication technology concepts into viable products and companies.

His experience includes leading startups with successful exits, restructuring companies, and business development with Fortune Global 100 companies.

A prolific inventor, he has over twelve patents in data security, IoT, Health technology, VoIP and communications areas.

PrivatizeMe provides safe browsing technology that enable users to Browse and search free from trackers, cookies, and cyber stalkers. For more information visit https://privatizeme.com


infosecurity
MIDDLE EAST
15-17 MARCH 2016
ADNEC, ABU DHABI, U.A.E
www.infosecurityme.com
SECURE YOUR
DIGITAL WORLD.
SECURE YOUR WORLD AGAINST CYBER THREATS AT INFOSECURITY MIDDLE EAST.
In 2016, Infosecurity Europe brings its pioneering cyber security event to the Middle East for the first time – and you can be part of it at ISNR Abu Dhabi. From leading-edge innovations and best practice solutions to world-class technologies, Infosecurity Middle East brings it all together, with specialist suppliers, workshops and dedicated technology showcases to help you protect your vital data and infrastructure.
HIGHLIGHTS FOR 2016
International Conference on Cyber Crime
Three day workshop in partnership with (ISC)2
Expert insights on the challenges facing your business
REGISTER NOW
DON'T MISS OUT. MAKE INFOSECURITY MIDDLE EAST YOUR MUST-SEE SHOW.
www.infosecurityme.com
Organised by
UNITED ARAB EMIRATES MINISTRY OF INTERIOR
Reed Exhibitions
Platinum sponsor
TRA
هيئة تنظيم الاتصالات
TELECOMMUNICATIONS REGULATORY AUTHORITY
@MOIUAE
www.moi.gov.ae

Opsec shop talk with Edward Snowden

By Anna Wehberg, Sr. Marketing Director, Hexis Cyber Solutions

Whatever one's opinion on the National Security Agency's most well-known former contractor, cybersecurity pros will likely be interested to hear what Edward Snowden has to say about operational security.

Opsec tips from one of the world's most wanted

The whistleblower recently sat down in Moscow for yet another media interview. But this one was different because the reporter on the case, Micah Lee of The Intercept, chose to focus on the geeky details of personal cybersecurity.

"In most of Snowden's interviews he speaks broadly about the importance of privacy, surveillance reform, and encryption," wrote Lee. "But he rarely has the opportunity to delve into the details and help people of all technical backgrounds understand opsec and begin to strengthen their own security and privacy. He and I mutually agreed that our interview would focus more on nerdy computer talk and less on politics."

It's important to note that Lee and The Intercept do not aim at neutrally presenting arguments for and against privacy. The publication takes a marked pro-privacy stance, one at odds with those at many governmental or business organizations. That said, it is enlightening to hear Snowden's practical advice, even down to which apps to use.

Snowden remains one of the most wanted men on the planet. He faces espionage charges in the U.S. after disclosing an enormous cache of classified data that exposed government surveillance programs.

Snowden recommends Signal, Tor

His first recommendation for someone wishing to leave no trace of their communications and activities? Encrypt your phone and text messages. Specifically, Snowden touted the smartphone app Signal.

"It's free, and you can just download it immediately," Snowden told Lee. "And anybody you're talking to now, their communications, if it's intercepted, can't be read by adversaries."

As far as Internet browsing and instant messaging, Snowden recommends Tor, a free application that aims to allow its users to prevent "network surveillance and traffic analysis" of their activities.

Paranoia-free living?
Snowden makes an argument that ironclad privacy should be easy.

"We should armor ourselves using systems we can rely on every day," Snowden told technologist Lee. "This doesn't need to be an extraordinary lifestyle change. It doesn't have to be something that is disruptive.

It should be invisible, it should be atmospheric, it should be something that happens painlessly, effortlessly."

Snowden advocated a practical approach to opsec in which persons evaluate what threats they face, what parts of their lives they would like to keep private and not to worry about cloaking everything.

"You don't need to live a paranoid life, off the grid, in hiding, in the woods in Montana," said Snowden during the interview, which was held in a hotel near Red Square.

Use a password manager
There are some basic steps Snowden advocates everyone take. In addition to the phone and message encryption mentioned above, he also recommends people encrypt their hard drives in case the physical object is stolen. He also says to use a password manager.

"Your credentials may be revealed because some service you stopped using in 2007 gets hacked, and your password that you were using for that one site also works for your Gmail account," Snowden said.

Ad blockers as security tools
There's been a lot written recently about ad blockers. Web publishers are seeing them decimate their display ad revenue.

Not surprisingly, Lee and Snowden have less concern for failing online ad business models than the privacy protections that come with ad blockers.

Snowden said any sites that use Javascript or Flash to automatically launch content can be vectors for attacks on one's machine. To him, that absolves any implied contract to look at the ads that support the site.

"If the service provider is not working to protect the sanctity of the relationship between reader and publisher," Snowden said, "you have not just a right but a duty to take every effort to protect yourself in response."

Interestingly, The Intercept attempts to back up its pro-privacy stance by collecting almost no information about its readers. Journalism researchers at the Poynter Institute say The Intercept hasn't completely figured out a business model along these lines, but give it credit for putting its analytics where its mouth is.

Is privacy versus security a false choice?

Maybe it goes without saying that Snowden represents one extreme in the debate between privacy and security. One former special counsel for President Bill Clinton wrote in The Daily Caller that abalance of the two remains possible.

"We should not allow Edward Snowden," wrote Lanny Davis, "who preaches privacy rights to us from Russia (not exactly a safe haven for privacy rights), or anyone else persuade us to accept the fallacy of the false choice:

We need and can have protection of privacy rights and personal and national security."

Cybersecurity pros should consider giving the full interview between Snowden and Lee a read. If nothing else, it provides a fascinating window into the nerdy details of the online and offline lives envisioned by one of the world's most polarizing figures.

About the Author

Hexis Cyber Solutions is a wholly-owned subsidiary of The KEYW Holding Corporation (NASDAQ: KEYW), and a provider of advanced cybersecurity solutions for commercial companies and government agencies.

Anna Wehberg, Sr. Marketing Director, joined Hexis Cyber Solutions in April 2014.

Connect with Hexis online: http://www.hexiscyber.com/

Hexis Blog: http://www.hexiscyber.com/blog

Twitter: @hexis_cyber

LinkedIn: https://www.linkedin.com/company/hexis-cyber-solutions

NSA Spying Concerns? Learn Counterveillance

Free Online Course Replay at www.snoopwall.com/free

"NSA Spying Concerns? Learn Counterveillance" is a 60-minute recorded online instructor-led course for beginners who will learn how easily we are all being spied upon - not just by the NSA but by cyber criminals, malicious insiders and even online predators who watch our children; then you will learn the basics in the art of Counterveillance and how you can use new tools and techniques to defend against this next generation threat of data theft and data leakage.

The course has been developed for IT and IT security professionals including Network Administrators, Data Security Analysts, System and Network Security Administrators, Network Security Engineers and Security Professionals.

After you take the class, you'll have newfound knowledge and understanding of:

1. How you are being Spied upon.
2. Why Counterveillance is so important.
3. What You can do to protect private information.

Course Overview:

How long has the NSA been spying on you?
What tools and techniques have they been using?
Who else has been spying on you?
What tools and techniques they have been using?
What is Counterveillance?
Why is Counterveillance the most important missing piece of your security posture?
How hard is Counterveillance?
What are the best tools and techniques for Counterveillance?

Your Enrollment includes :

1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement for passing the Concise-Courses Counterveillance 101 course.

Visit this course online, sponsored by Concise-Courses.com and SnoopWall.com at http://www.snoopwall.com/free

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

You have built a great app with an amazing team.

Let us help you secure it.

SnoopWall's patents-pending AppShield™ SDK can secure any mobile app on all major platforms. Our AppShield SDK makes your app invisible to any other app on the mobile device which might otherwise eavesdrop on it, just like the B2 Bomber employs stealth technology to evade radar detection. With 24/7/365 active monitoring, regular updates and a dedicated team of cybersecurity experts, you can be assured that your app's security and customer data are safe, all the while providing a non-intrustive customer experience.

KEY FEATURES

- Cloaking Technology (patents-pending)
- Dynamic Port Management (patents-pending)
- No Need for Code Obfuscation
- No Malware Scanning Required
- No Backend Database Required
- Root & Jailbreak Detection
- Secure Storage for Data Hiding
- Application Hardening Technology
- No Known Way to Exploit
- Detects & Blocks Tomorrow's Threats
- Apple iOS, Google Android, Microsoft Windows
- No Sysadmin, no Reboot, no special Privileges
- Tiny Deployment Size & Rapid Integration
- Most Cost Effective Per Deployment Pricing

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

Does your mobile app have built-in next generation firewall technology to safeguard customer data?

Mobile apps are critical and vulnerable touchpoints in most companies networks. Just like the firewall which protects your IT network, an app firewall is needed to protect your mobile app. However, most app development teams do not have this expertise, nor are they dedicated to this mission.

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

- HIGH RISK OF PATENT INFRINGEMENT $$$$$
- MAJOR DISTRACTION FROM CORE DEVELOPMENT FOCUS
- HIGH REPUTATIONAL RISKS
- POSSIBLY NOT SECURE
- UPDATED WHEN YOU CAN FIND THE TIME
- FULL BLOWN SOLUTION WILL TAKE YOU 20,000 CODER HOURS (10 CODERS FOR 12 MONTHS)
- LIGHTWEIGHT RISKY SOLUTION WILL TAKE YOU 10,000 CODER HOURS (10 CODERS FOR 6 MONTHS)
- MAINTENANCE AND SUPPORT WILL TAKE YOU 5200 HOURS PER YEAR (2 CODERS FOR 12 MONTHS)
- HIGH RISK TO BREAK YOUR AWESOME APP AND USER EXPERIENCE
- HIGH RISK TO CAUSE USER CONFUSION AND LOSS OF CUSTOMERS
- MAY LOSE SOME OR ALL CUSTOMER RECORDS
- MAYBE SSL PINNING IS THE MOST YOU CAN DELIVER
- MAY PROTECT SOME OF THE PORTS SOME OF THE TIME
- TIME TO DEVELOP AND DEPLOY: 6-12 MONTHS
- **COST TO DO IT YOURSELF: $1.2M**
- **ANNUAL COSTS TO KEEP IT UP TO DATE: $650k**
- **COSTS TO AVOID PATENT INFRINGEMENT: $500k-1.5M**

VS.

LICENSE OUR AppSHIELD SDK

- ✓ PROTECTED ACCESS TO PATENTED AND PATENT PENDING SOLUTIONS
- ✓ LEVERAGE YEARS OF MOBILE SECURITY EXPERTISE
- ✓ LOW REPUTATIONAL RISKS
- ✓ EXTREMELY SECURE AND PROVEN SOLUTION
- ✓ 7x24x365 CYBERSECURITY PROTECTION
- ✓ THE SOLUTION IS DONE
- ✓ THE SOLUTION HAS BEEN PROTECTING MILLIONS OF TRANSACTIONS SINCE 2014
- ✓ MAINTENANCE AND SUPPORT IS INCLUDED
- ✓ INCLUDED IN THIS SYSTEM:
  - → ZERO DAY MALWARE PROTECTION
  - → ADVANCED PERSISTENT THREAT PROTECTION
  - → FEATURES INVISIBLE TO CONSUMER EXPERIENCE
  - → ALL MOBILE APP CUSTOMER PII PROTECTED
  - → MILITARY GRADE ENCRYPTION
  - → REAL-TIME DATA LEAKAGE PROTECTION
- ✓ **TIME TO INTEGRATE AND DEPLOY: 3-5 BUSINESS DAYS**
- ✓ **NO INFRINGEMENT RISKS ONCE LICENSED: FIRST OF ITS KIND IP**
- ✓ **ANNUAL UPDATE COSTS A FRACTION OF DO IT YOURSELF**
- ✓ **PRICING IS A NO-BRAINER (MUCH MUCH LOWER)**

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

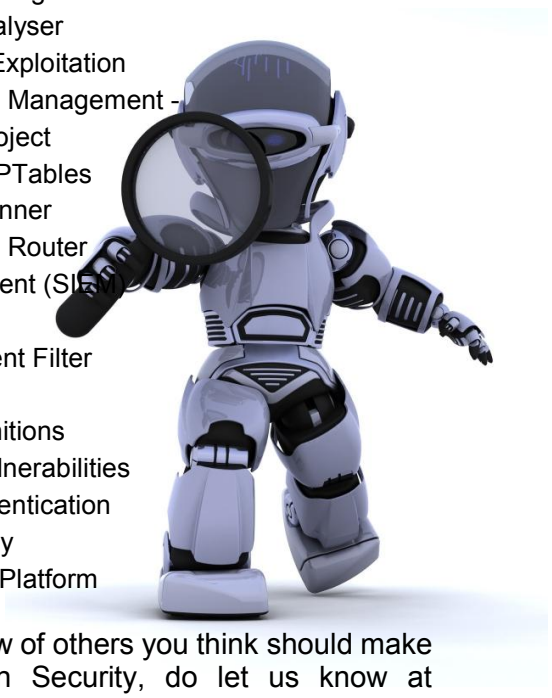
Top Twenty INFOSEC Open Sources

Our Editor Picks His Favorite Open Sources You Can Put to Work Today

There are so many projects at sourceforge it's hard to keep up with them. However, that's not where we are going to find our growing list of the top twenty infosec open sources. Some of them have been around for a long time and continue to evolve, others are fairly new. These are the Editor favorites that you can use at work and some at home to increase your security posture, reduce your risk and harden your systems. While there are many great free tools out there, these are open sources which means they comply with a GPL license of some sort that you should read and feel comfortable with before deploying. For example, typically, if you improve the code in any of these open sources, you are required to share your tweaks with the entire community – nothing proprietary here.

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available (Version 6 & earlier)
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network Protocol Analyser
6. Metasploit.org – The Best Suite for Penetration Testing and Exploitation
7. OpenCA.org – The Leading Open Source Certificate and PKI Management -
8. Stunnel.org – The First Open Source SSL VPN Tunneling Project
9. NetFilter.org – The First Open Source Firewall Based Upon IPTables
10. ClamAV – The Industry Standard Open Source Antivirus Scanner
11. PFSense.org – The Very Powerful Open Source Firewall and Router
12. OSSIM – Open Source Security Information Event Management (SIEM)
13. OpenSwan.org – The Open Source IPSEC VPN for Linux
14. DansGuardian.org – The Award Winning Open Source Content Filter
15. OSSTMM.org – Open Source Security Test Methodology
16. CVE.MITRE.org – The World's Most Open Vulnerability Definitions
17. OVAL.MITRE.org – The World's Standard for Host-based Vulnerabilities
18. WiKiD Community Edition – The Best Open Two Factor Authentication
19. Suricata – Next Generation Open Source IDS/IPS Technology
20. CryptoCat – The Open Source Encrypted Instant Messaging Platform



Please do enjoy and share your comments with us – if you know of others you think should make our list of the Top Twenty Open Sources for Information Security, do let us know at marketing@cyberdefensemagazine.com.

(Source: CDM)

National Information Security Group Offers FREE Techtips

Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

The best service of NAISG are their free Techtips. It works like this, you join the Techtips mailing list.

Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting your question to the Techtips newsgroup.

Next thing you know, a discussion ensues and you'll have more than one great answer.

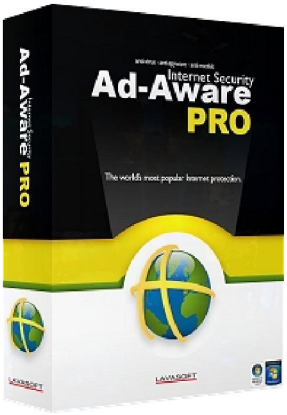
So use it by going here:

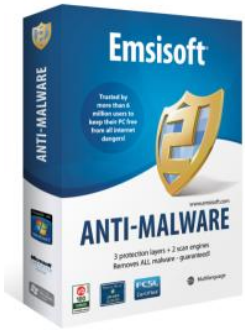
http://www.naisg.org/techtips.asp

SOURCES: CDM and NAISG.ORG

SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com





where they (like you) will be entered into a monthly drawing for the Award winning Lavasoft Ad-Aware Pro, Emsisoft Anti-malware and our new favorite system 'cleaner' from East-Tec called Eraser 2013.

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

Free Monthly Cyber Warnings 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 Warnings 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 signup 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.

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine December 2015

Sample Sponsors:

To learn more about us, visit us online at http://www.cyberdefensemagazine.com/

Cyber Warnings Newsflash for December 2015

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Here is a summary of this month's cyber security news. Get ready to read on and click the links below the titles to read the full stories. So find those of interest to you and read on through your favorite web browser…

Java plug-in malware alert to be issued by Oracle

http://www.bbc.com/news/technology-35159851

Apple-targeted malware to rise in 2016, warns Symantec

http://tech.firstpost.com/news-analysis/apple-targeted-malware-to-rise-in-2016-warns-symantec-292006.html

Macro Malware Reappears

http://www.spamfighter.com/News-20009-Macro-Malware-Reappears.htm

Panda Security: New Malware Hit 230,000 Per Day in 2015

http://www.infosecurity-magazine.com/news/panda-new-malware-230000-per-day/

Fileless Memory Infection, Macro Malware on the Rise: McAfee Labs

http://www.eweek.com/security/slideshows/fileless-memory-infection-macro-malware-on-the-rise-mcafee-labs.html

Santa Claus Malware In Christmas Apps Targeting Android, iOS, PC Users

https://www.hackread.com/santa-claus-christmas-app-malware-targeting-pc-ios-android-users/

Pro POS Malware: Not Quite Professional-Grade?

https://securityintelligence.com/news/pro-pos-malware-not-quite-professional-grade/

The security review: Nemucod malware, Star Wars and China on cyber sovereignty

http://www.welivesecurity.com/2015/12/21/security-review-nemucod-malware-star-wars-china-cyber-sovereignty/

AFRICAN COUNTRIES TOP LIST FOR MOBILE MALWARE ATTACKS

http://www.htxt.co.za/2015/12/22/mobile-is-the-weak-link-in-business-network-security/

Building malware defenses: Control email, web browsers, and ports

http://www.networkworld.com/article/3016674/security/building-malware-defenses-control-email-web-browsers-and-ports.html

Microsoft now taking on Man in the Middle ad injection and browser hijacking

http://winsupersite.com/microsoft/microsoft-now-taking-man-middle-ad-injection-and-browser-hijacking

POS Malware Tool Emerges to Exploit Retailers

http://www.eweek.com/security/pos-malware-tool-emerges-to-exploit-retailers.html

UK Bombarded with 1,200 Types of Malware in November

http://www.infosecurity-magazine.com/news/uk-bombarded-1200-types-malware/

Ghostware and Two-Faced Malware Coming in 2016

https://www.hackread.com/ghostware-two-faced-malware-coming-in-2016/

New, improved Macro malware hitting Microsoft Office

http://www.scmagazine.com/macro-malware-hitting-microsoft-office-16-years-later/article/460250/

A third of pirated movie sites spread malicious software, report says

http://www.cbsnews.com/news/pirated-movie-video-download-sites-spread-malicious-malware/

Ho ho hosed: Asian biz malware pwns air-gaps, thousands of Androids

http://www.theregister.co.uk/2015/12/16/ho_ho_hosed_asian_biz_malware_pwns_airgaps_thousands_of_androids/

Websites to Search Torrent Links Delivering Malware to 12m Visitors Every Month

http://www.spamfighter.com/News-20006-Websites-to-Search-Torrent-Links-Delivering-Malware-to-12m-Visitors-Every-Month.htm

ZBOT: ANDROID BANKING MALWARE TARGETS RUSSIAN USERS

https://securityintelligence.com/news/zbot-android-banking-malware-targets-russian-users/

Retailers Scrambling Against Latest Credit Card-Stealing Malware

http://fortune.com/2015/11/24/retailers-modpos-malware/

VA sees jump in malware, intrusion attempts

http://www.fiercegovernmentit.com/story/va-sees-jump-malware-intrusion-attempts/2015-12-18

Bitcoin Stealing Malware Attacks Gamers

http://cointelegraph.com/news/115875/bitcoin-stealing-malware-attacks-gamers

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

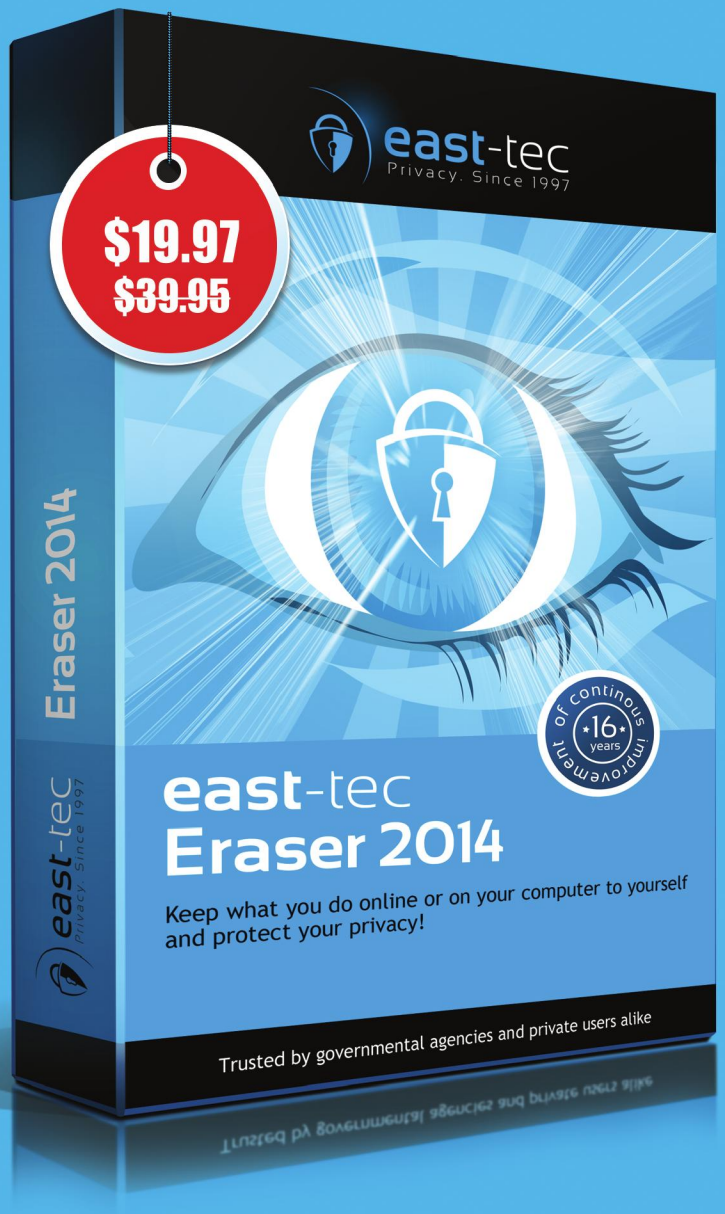
Cyber Defense Magazine - Cyber Warnings rev. date: 12/29/2015

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

Protect your data and privacy by removing all evidence of your online and offline activity with **East**-Tec **Eraser 2014**.
Securely erase your Internet and computer activities and traces, improve your PC performance, keep it clean and secure!



Exclusive offer for Cyber Defense magazine readers

Save 50%

on ALL East-Tec products
www.east-tec.com

Coupon Code:

CYBERMAG2014