CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

IN THIS EDITION:

- Ransomware Defence
- Threat Intelligence
- Compliance Essentials
- Defending DDoS Attacks

November 2016

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 Miliefsky
stevinv@cyberdefensemagazine.com

EDITOR

Pierluigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Laurel Stewart
Andrei Barysevich
Michael Shalyt
Sunil Madhu
Jatin Sethi
Vatsal Jain
Josh Lefkowitz
Megan Ray Nichols
Josh Gomez
Stewart Kantor
Scott Millis
Anamika Kumari
Abrar Ahmed
Milica D. Djekic
Destiny Bertucci
Dennis Turpitka
Ryan Orsi
Cricket Liu
Fortunato Guarino
Yana Yelina
Raj Samani
Jon Leer
John Galda
Rodrigo Ruiz
Phillip Adcock
Dr. Daniel Osafo
Gregg Petersen
Corey Wilburn

Interested in writing for us:
writers@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

Copyright (C) 2016, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide. sales@cyberdefensemagazine.com

Executive Producer:
Gary S. Miliefsky, CISSP®

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Before You Know It, We'll Be Seeing You at RSA Conference 2017

Friends,

This coming RSA Conference 2017 has moved up another month and will take place in San Francisco between February 13th and 17th at the Moscone Center – the "Big Top" of information security. Each year, we've seen the conference grow in size – with an anticipated 30,000 attendees this year. Now is the time to make all of your travel arrangements. We've found that AirBnB, Expedia, Travelocity, Orbitz, Trivago, Kayak and Priceline are very helpful to get there and then when you arrive, make sure you have Lyft or Uber app installed so you can easily get to and from the event.

I like the theme this year: "Power of Opportunity". RSA Conference staff wants you to take advantage of this upcoming opportunity to learn about new approaches to info security, discover the latest technology and interact with top security leaders and pioneers. The hands-on sessions, keynotes and informal gatherings allow you to tap into a smart, forward-thinking global community that will inspire and empower you.

With attacks like the one against Dyn, a botnet sending out 700mb to nearly 1GB of DDoS traffic, you know we have much innovation to do in cyber security. There should be new and better ways to ensure the Internet of Things becomes a Secure Internet of Things (SIoT) and until then, we remain highly susceptible to 'Internet' blackouts and outages like your local power company during a heavy thunder and lightning storm.

To stay one step ahead of the next threat, we continue to look for more innovative cyber security companies and will have more awards to share during RSA Conference 2017. Meanwhile, we have found some gems that we'd like you to keep an eye on or consider for your needs, of the top twenty Cyber Security Leaders of 2016 here: http://www.cyberdefensemagazine.com/cyber-security-leaders-2016/

Here at CDM, we continue to focus on the important areas of INFOSEC to help you be more proactive and avoid having vulnerabilities exploited, having seen so many breaches lately. So, we hope you like what you'll find in this month's edition of Cyber Warnings. As they say in USA during this month, it's "Thanks Giving" and we're thanking our best and brightest thinkers for contributing to our knowledge base with some wonderful articles. Please enjoy. Cheers!

To our faithful readers, Enjoy

Pierluigi Paganini

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

Copyright © Cyber Defense Magazine, All rights reserved worldwide

WHERE CYBERSECURITY HARNESSES THE POWER OF OPPORTUNITY.

RSA Conference is the world's foremost gathering of infosecurity professionals. Each year, thousands of the industry's best and brightest come together to exchange ideas, discuss their latest challenges and find the cutting-edge solutions that will help them better protect our digital world.

Attend RSA Conference to expand your knowledge through sessions, tutorials and keynotes. Meet with innovative companies. And network with peers and thought leaders. Experience diverse perspectives and discover the power of opportunity.

Join us:

RSA Conference 2017
February 13–17 | San Francisco

RSA Conference 2017 Asia Pacific & Japan
July 20–22 | Singapore

RSA Conference 2017 Abu Dhabi
November 2017 | Abu Dhabi

Connect with RSA Conference today. Stay on top of the latest trends and be the first to hear about Conference news and special offers.

www.rsaconference.com

RSA Conference 2017

San Francisco | February 13–17 | Moscone Center

Follow us on: #RSAC

What is Taint Checking?

by Laurel Stewart, Director of Marketing, GrammaTech

Introduction:
Taint checking? This isn't a trap, I promise. It sounds vulgar, but its etymology is perfectly reasonable, stemming from the notion that data that has been "tainted" by a malicious user (and could be used to breach your system) is a dangerous vulnerability in code and needs to be found and eliminated.

Wikipedia actually has a pretty clear definition of taint checking:

> "Taint checks highlight specific security risks primarily associated with web sites which are attacked using techniques such as SQL injection or buffer overflow attack approaches."

I'm assuming that those in the security auditing world of the 2016 cyber-security landscape have likely moved past and become immune to the chuckles of this unfortunately-named technical term. But for the rest of us, I thought I might provide a clear overview, so you can start addressing this extremely-important concept with confidence in the boardroom. Ready?

Taint Sources and a Program's Attack Surface
So let's go back to that definition from wikipedia. It's not bad, although its focus on websites is a little misleading, given that most embedded devices are now connected to the internet, so the security risks are much broader in scope.

When security analysts determine the safety of a given system, they look at a program's attack surface, which is defined by the places in the program that are exposed to an attacker. When we look at tainted data, this is essentially what we're talking about — sources of taint correspond closely to the program's attack surface. Taint sources are locations in the program where data is being read from a potentially risky source, and include things like environment variables, data, files, file metadata (such as a file's permissions or data stamps), the network or information bus, the system clock, or network services (such as the results of a DNS query).

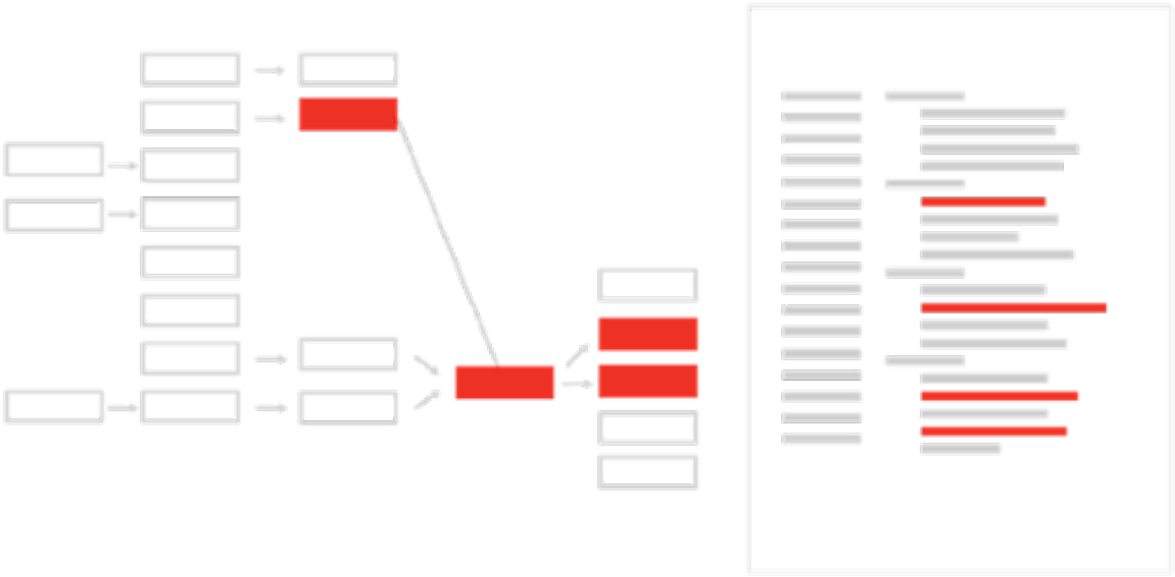
An attacker can use these unverified channels to trigger security vulnerabilities or cause programs to crash. Many different types of issues can be triggered by tainted data. In addition to the few that Wikipedia mentioned above, these issues include command injections, cross-site scripting, arithmetic overflow, or path traversal. (For a technical deep-dive into a buffer overrun vulnerability, I highly recommend the whitepaper Protecting Against Tainted Data in Embedded Apps with Static Analysis, written by our VP of Engineering, Paul Anderson.)

So how does this relate back to static analysis?

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Taint Analysis in CodeSonar

It comes back to taint analysis, which is an extremely useful technique to help anyone performing a security audit better understand a program's attack surface(s). Taint analysis is performed automatically by CodeSonar as part of its regular set of analyses, and presented visually within the CodeSonar interface to demonstrate how risky data can flow from one part of a program to another.



Since taint can flow through the program in unexpected ways, it's important to understand these channels fully. In CodeSonar, the flow of tainted data can be visualized and program elements involved in flows can be overlaid on top of the regular code view. This visualization helps developers understand the risks of their code and aids them in deciding how best to change the code to shut down the vulnerability. It helps security auditors understand at a high level how taint is flowing through the code, in order to understand the attack surface.

Reducing Risk

The bottom line is that taint analysis is an effective method to reduce risk, by helping you eliminate exploitable attack surfaces. So it's imperative that we get comfortable talking about it, even if it has a less-than-ideal name.

About The Author

Laurel Stewart is the Director of Marketing at GrammaTech, where she has followed the IoT trend from prediction to reality. With a technical background and years of experience in marketing, she is committed to providing software manufacturers with a clearer understanding of what is required in this new cyber-security landscape.

Laurel can be reached online at https://www.grammatech.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The anniversary of EMV roll-out: criminals are anxious to beat the system

Introduced by the financial industry in the early 2000s, EMV smart payment cards have largely supplanted magnetic stripe technology, and for good reason. Due to concerns surrounding insufficient security measures, usage of the once-ubiquitous “magstripe” payment cards has since sharply declined in most countries. The United States, however, continues to remain dependent on the outdated technology.

Despite proven advantages shown to significantly lower — and in many cases, reverse — established levels of card-present fraud, the United States continues to lag behind on the implementation of EMV. This delay is largely attributed to the inherent costs and minimal incentives for banks to migrate from the outdated magnetic stripe infrastructure.

Payment fraud declining

As long as magstripe cards remain in use, their inherent security flaws will continue to render cardholders more susceptible to fraud. The problem is that magnetic strip technology stores payment information in plain text on the card's magnetic stripe, which makes the cardholder’s financial information vulnerable to a variety of skimming techniques used to commit fraud. EMV technology, however, provides significantly stronger protection by encoding and storing the cardholder’s payment information on an integrated circuit embedded within the card.

Indeed, ever since the rollout of EMV smart cards, card-present fraud has been decreasing for the first time ever. Criminals are struggling to find workable solutions to bypass the implemented security controls, providing a needed reprieve for exhausted consumers and financial organizations. Despite the obvious advantages, however, many business owners remain hesitant to accept EMV smart payment cards. This is largely due to the complexity of the technology. Many are concerned that EMV’s significantly longer card processing time may inadvertently put customers’ at an increased risk of information theft and criminal targeting.

Cybercriminals adapt to EMV

Despite EMV’s implementation challenges, recent observations suggest a decline in the supply of stolen payment information being sold on the cybercriminal underground. Consequently, both demand and prices for such stolen information have significantly increased.

Alone, the destabilization of established supply and demand levels on the cybercriminal underground is a cause for concern. This disturbance will inevitably create a lucrative environment for attracting criminal syndicates with unlimited financial and technical resources to develop the technology to bypass EMV controls.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

In fact, we recently discovered a next-generation EMV skimmer that is both small enough to fit inside a standard point of sale (PoS) terminal and able to store up to 5,000 records at one time. This device uses the terminal's internal power supply and can be left inside indefinitely. To retrieve the skimmed information, criminals insert a special memory card that resembles a standard credit card into the PoS terminal.

Most notably, this skimmer comes equipped with decryption software. This enables criminals to de-obfuscate the encrypted payment information, which can later be copied and recorded onto a plain magstripe card. Though likely developed in one of the Baltic countries, the device was advertised in the Spanish underground and sold for the hefty price of $3,000.

Not all EMV technologies are created equal

Many people don't realize that there are in fact two different generations of EMV technology. Indeed, many financial organizations in South America are reliant on the first generation, which is known as Static Data Authentication (SDA). Unfortunately, SDA renders cardholders substantially more susceptible to skimming and cloning attacks. In many cases, due to significant issuance costs, banks have decided to postpone the deployment of more sophisticated and improved smart cards based on Dynamic Data Authentication (DDA) protocol, which can cost up to five times more than SDA.

It is important to highlight, however, that criminals have yet to develop a reliable solution for cloning compromised EMV smart cards utilizing DDA technology. Despite the recently discovered skimmers, criminals are still left with a single option for decoding the stored data and attempting to clone the information onto magstripe blanks. However, the latest antifraud systems can quickly identify unauthorized swiped transactions for EMV-supported payment cards, subsequently lowering the chances of a successful fraudulent purchase. As North American financial institutions continue to phase out previously-issued magstripe cards, the overall exposure to card-present fraud will inevitably decrease.

Threats on the horizon

We foresee that in the coming years, the most significant threats will not be related to the EMV technology itself, but rather to the false sense of security it fosters in the minds of business owners and the financial industry. Having blind faith in the supposed invulnerability of technology can yield disastrous results. What we see time and time again is that once the level of potential payoff reaches a tipping point of "too big not to steal," criminals always find a way to rig the system.

As with any man-made technology, all it takes is an equally-intelligent person to find a solution. Whoever finds the way to bypass smart card security could easily become a multi-millionaire overnight. When the day comes that malicious actors find a loophole, organizations will likely be completely unprepared to mitigate the threat.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Based on Flashpoint's in-depth knowledge of the criminal underground, we have noticed a surprising level of consensus amongst cybercriminals that the latest generation of payment platforms, such as Apple Pay and Google Pay, have thus far proved to be highly robust and secure — far superior to EMV.

Recommendations

As much as we want to rely solely on banks to protect us from criminals, all of us can follow these simple recommendations to significantly lower the chances of compromise:

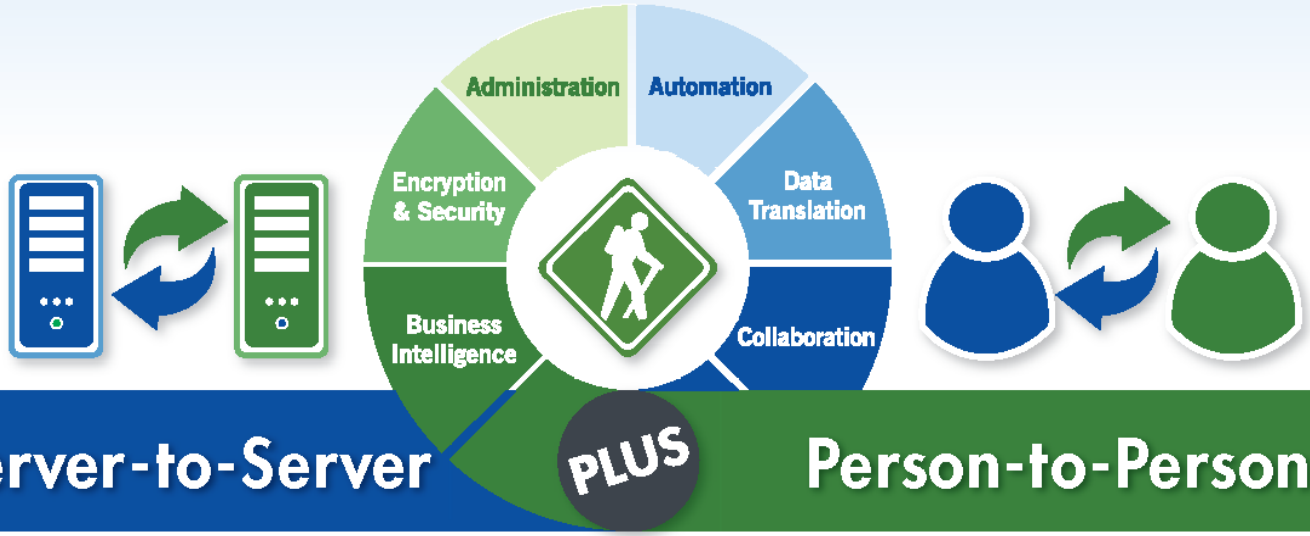
1) Always utilize robust alerting systems built within banking applications.
2) Activate pre-authorization and purchase notifications for amounts as small as $1. Criminals will often test stolen records on a cup of coffee before attempting to use it at the nearest Apple store. If you only receive alerts for large amounts, by the time you spot a fraudulent purchase and contact your bank, the criminals will be long gone and may have successfully spent hundreds, if not thousands, of your money.
3) Never use your debit card for any online or in-store purchases. If the card is compromised, it will be a painfully long process to get the money reimbursed by a bank. In some cases, if funds are stolen using a PIN number, some banks may not reimburse you at all. Considering monthly mortgage and loan payments among others, many people don't have the luxury of losing access to their funds.
4) If possible, use a separate credit card for all commercial purchases. The compromise of a credit card will not affect you financially while the bank investigates the theft. If you are absolutely against credit cards and adhere to strict financial practices, open up a separate bank account and only maintain a balance sufficient to cover your average monthly expenses, thus limiting the exposure to your main bank account.

About the Author

Andrei Barysevich is the Director of Advanced Collection at Recorded Future. He specializes in threat intelligence on highly restrictive criminal communities and he oversees proactive intelligence operations. A native Russian speaker, Andrei was previously an independent e-commerce fraud researcher, and a private consultant for the FBI's New York Cybercrime field office. Andrei's work and commentary has been featured in The Wall Street Journal, Motherboard, The Atlantic, and numerous other publications. For the past 13 years, he has been involved in multiple high-profile international cases resulting in successful convictions of members of crime syndicates operating global reshipping, money laundering, and bank fraud schemes.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

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

Are your critical systems lying to you? Protecting SCADA Systems from Data Forgery

by Michael Shalyt, VP Product Aperio Systems (www.aperio-systems.com)

Like many things in life, the greatest cyber threat to critical infrastructure is in the things we cannot see.

Both security analysts and the general public spend a lot of time and energy discussing big-name hackers — "Anonymous" and its cohorts or secret government agencies that sneak past perimeter defenses and wreak havoc on or expose sensitive data from IT systems after making their way in.

But attacks on critical infrastructure, though less discussed, can cause catastrophic damage. Lloyd's of London estimates a successful attack on the U.S. power grid could result in $1 trillion worth of damage, not to mention loss of life.

And as the head of the UN's nuclear watchdog agency put it, after revealing that nuclear facilities in Germany and South Korea suffered disruptive cyber attacks, the stakes are no longer theoretical (see this Reuters article for more details).

Serious cyber attacks against critical systems can come from all directions and at all levels of sophistication.

Successful breaches by nation states and political actors have dominated headlines but, in today's world, attackers range from mere hobbyists, hacktivists and cybercriminals to sophisticated state-sponsored attackers.

An Iranian national hacked the control systems of a NY dam, attackers left a quarter million Ukrainians in the dark, and hacktivists with fairly limited skills were able to penetrate a water treatment plant in the US. And these are just the examples we know about.

We can safely assume there are numerous breaches that are as yet undetected or undisclosed.

Unfortunately, it is clear that persistent attackers can penetrate critical control systems – and when critical infrastructure is concerned, even a single destructive attack is one too many.

Therefore we must assume the worse – that the attacker already has control over the sensitive network.

Once attackers are inside, in order to inflict severe and long-lasting damage to critical

Copyright © Cyber Defense Magazine, All rights reserved worldwide

infrastructure, they need to forge reported operational data -- this is how they can blind operators and protection mechanisms and execute their attacks undetected.

What is Data Forgery?

Nearly every good spy thriller depicts a nail-biting break-in where a security camera system is reconfigured to play a continuous loop of an empty corridor. The hapless guard has no idea that the intruders are actually sneaking down the corridor at that precise moment.

When attacking SCADA systems, malicious intrusion is twofold. It's about putting systems into potentially damaging states and – like in a good spy thriller – hiding all evidence of intrusion.

After all, industrial control systems were designed to be as resilient as possible to malfunctions and physical disasters. Industrial control operations teams are well trained and highly experienced in managing faults, downtime, and even weather conditions.

When failures occur, operators are capable of reacting quickly and proficiently to stop the damage, minimize downtime and to isolate the source of the problem to, ultimately, protect the critical infrastructure.

Bottom line: Control systems and operators are able to prevent severe damage, as long as they know the **true state** of the plant. True state awareness is, in essence, the last line of defense.

How to protect against data forgery

Every physical device and process has a unique fingerprint, due to its particular history and features. This fingerprint is extremely sensitive to external manipulations. For this reason, physics is the key to detecting and reacting to data forgery.

For example, if a cooling system reports figures outside of normally acceptable parameters, sensors will alert operators to this abnormality.

But if attackers configure the cooling system to report acceptable performance levels, hackers can slowly shut down the system and threaten potentially dangerous and very expensive equipment – while the operators remain oblivious.

Physical sensor data can be compromised at every step, so we must validate the integrity and authenticity of the physical signals, revealing the true state of the system’s physical components.

This can be done either by rigorous encryption of the digitalized physical data (from the sensor all the way to the operator screen) or detection of data tampering attempts via comparison to a

Copyright © Cyber Defense Magazine, All rights reserved worldwide

learned physical model of the specific equipment (using the laws of physics governing the dynamic system as a form of “natural encryption”).

But it’s not enough to know there’s a dissonance between physical reality and digital data. You must know first and foremost, whether it’s due to an attack (as opposed to, say, sensor malfunction). Next, you must be able to pinpoint the exact target of the attack.

Operators must know the specific valve, pipe, turbine or drill that's directly affected. Non-specific alerts are of little use to operators since industrial plants and factories cannot afford to be taken offline due to ambiguous threats or false alarms.

Conclusion

True state awareness is critical to maintaining operational resilience and preventing physical damage. That is why data forgery, when used by malicious actors to rob operators of visibility into their own plants and equipment, is a growing threat and should be proactively addressed in order to prevent severe damage.

About the Author

Michael Shalyt, VP Product, Aperio Systems (www.aperio-systems.com)

Michael Shalyt leads the APERIO Systems research and product development team. Prior to joining APERIO, Michael led the malware research team at the renowned cybersecurity firm Check Point, following four years as a leading researcher and team leader in an elite IDF intelligence unit.

Michael is a graduate of the elite “Psagot” IDF academic program and holds a dual Bachelor’s degree in Physics and Electrical Engineering from the Technion, in addition to a Master’s degree in quantum control and quantum information, also from the Technion.

He has been recognized with numerous awards, including several Technion Presidential Excellence Awards, and a bronze medal for the Israeli team in the 36th International Physics Olympiad in Salamanca, Spain.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Adapting to the Size and Speed of CyberFraud

500 million hacked.

At first, it was the magnitude of the Yahoo! breach that made headlines. That at least half-billion users had their personal information stolen sent a chill down the spines of both customers and the brand-name institutions they rely on. In the following days, insiders explained how Yahoo! was slow to make cybersecurity a top priority after it was hacked six years ago by the Chinese military. The company allocated resources for improving appearance and user convenience at the expense of basic security measures. When accounts were breached, it sometimes wouldn't even demand a password reset, for fear of turning off users.

Overview

For financial institutions (FIs), security has always been a top priority. Where that once meant steel vaults and armored trucks, now it means digital solutions. In March, the Consumers and Mobile Financial Services report from the Federal Reserve found that people use online banking almost as much as they head to the ATM (71 percent vs. 75 percent). Mobile banking is on the rise too, now used by 53 percent of people with smartphones.

Aware of digital exposure, FIs are acting fast. Last year, J.P. Morgan doubled its cybersecurity budget from $250 million to $500 million, and Bank of America CEO Brian Moynihan said his company's cybersecurity budget was essentially unlimited. Cybersecurity is a worry across all industries – in 2014, cybercrime had a market capitalization of $445 billion, meaning that if it were a company it would be second-biggest in the US, behind only Apple – but for FIs it is extremely important, as they deal with cash, credit, mortgages, securities, pensions, and payments. To survive in this increasingly turbulent cyber world, it is imperative for them to understand not just how large cyberfraud has become, but how it happens – and how it can be prevented.

How Hackers Monetize CyberFraud

According to the Verizon Data Breach Investigations Report (DBIR), 95 percent of web app attacks are motivated by money. Hackers rarely fit Hollywood stereotypes about revenge and altruism. They are looking to steal high volumes of sensitive user data to sell on the Dark Web. They often use an e-commerce platform as the means of entry, or gain a stronghold through a phishing campaign. The DBIR found 20,000 incidents where compromised websites were used in distributed denial of service (DDoS) attacks or repurposed as phishing sites.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Once in possession of stolen profile data, hackers will package it for sale on the Dark Web. They will advertise aspects of the data like credit card numbers, Social Security Numbers (SSN), phone numbers, and emails. Sometimes they even offer volume discounts. The nefarious characters that acquire this data – which they often do incognito, via Bitcoin payments – will usually age it, meaning let it sit for a period of time, as the unsuspecting true persons associated with the data go about their daily lives. This improves the quality of the stolen data and increases its potency, which was what happened in the Yahoo! breach.

The most common way to effectively use the stolen data is to create synthetic IDs. This means using part of a real identity associated with a valid credit card or SSN while changing other parts of the data, usually the email address and sensitive phone information. The reason a cyber thief changes these components is to intercept "out-of-band" (OOB) communications, the text messages and emails confirming that a change has been made. This renders two-factor authentication (2FA), for years a trusted cybersecurity measure, increasingly patchy. In fact, in July the National Institute of Standards and Technology (NIST) updated to its Digital Authentication Guidelines (DAG) to state that 2FA over SMS is no longer secure. If FIs want to ensure customer security, they will have to be on the front lines of evolving cybersecurity standards.

Understanding Exposures

The recent transition to EMV chip-card technology in the US has made it difficult for hackers to clone credit cards, so instead hackers have been initiating fraud via account takeover and account creation. One study saw account takeover fraud increase by 112 percent from August 2014 to August 2015. To stay ahead of the criminals, smart organizations have started taking steps to improve their chances of catching this type of activity through the use Social Biometrics, device fingerprinting, and geodesic IP location tracking.

Social Biometrics is the process of leveraging social media data alongside trusted online and offline information to correlate data in the application process. This allows for vastly improved fraud prediction and authenticity validation, as new email, phone or address information introduced by fraudsters will have a low correlation and therefore high fraud indication. This method is particularly useful for fraud mitigation. Replicating a human-like network for a fraudulent (or synthetic) identity would be incredibly difficult, and would show low social proof of authenticity.

Device fingerprinting seeks to understand known good or bad devices – e.g. devices that have been used to commit fraud in the past – and determine if they are connected to the identity presented at the time of application. These systems have been around for years, and the quality of their fraud mitigation is reliant upon the expanse of their network. Of course, when individuals regularly change the devices that they use to connect to the internet and apply for new accounts, like phones and laptops, device fingerprinting becomes difficult.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Geodesic coding relies on understanding the distance between the address or locality associated with an identity, and the location from which the application or change is initiated. For example, if an identity that "lives" in New York applies for a new credit card with a phone number from California, via a computer in Europe, the fraud score could be tipped off and trigger an organization to deny the account creation, or it could subject the account to review by a human analyst, who would likely pick up the discrepancy.

What these solutions provide is speed. Today's hacks happen very quickly. The DBIR found that in 93 percent of breaches, systems were compromised within minutes, and 28 percent of the time, data was exfiltrated within minutes. More troubling, once the data was stolen, only 3 percent of breaches were discovered within minutes, 5 percent were discovered within hours, and 9 percent within days. This means that 83 percent of victims didn't learn of the breach for weeks or more.

Conclusion

When cyberfraud occurs, FIs can lose a lot more than time and money. They can lose customers, not just in the moment, but for life. Millennials just passed Baby Boomers to assume the mantle of "largest living U.S. generation." If FIs are going to capture the trust of this massive demographic of technology-savvy young people, they must start by showing them that they can do business safely, securely, and seamlessly. Nobody wants to be the next Yahoo!.

About the Author

Sunil Madhu, CEO and Founder, Socure

Sunil has spent over 20 years innovating identity and access management, addressing hard problems in network and application authentication and authorization. A security architect by profession, he is also the founder and CEO of Socure, a growth company dedicated to innovating Digital Identity Verification, by using advanced artificial intelligence and machine learning to deliver analytics from trusted online, offline and social media data. A serial entrepreneur, Socure has led several successful transitions through IPO and acquisition. Sunil holds a MS degree in MIS from Glasgow Caledonian University and a BS with Honors in Computer Science from Strathclyde University in the UK.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Cyber Tension in South Asian Countries

By Jatin Sethi (Assistant Professor, Department of Cyber Platform, UPES Dehradun, India) & Vatsal Jain (Student, UPES Dehradun, India)

Introduction

The tension between India and Pakistan across the Line of Control (LoC) has crossed the geographical boundaries and is now reflecting in the cyber space. After the recent terrorist attack in India and the military actions between these two countries in September 2016, all other countries around the globe were worried about the critical situation. But most of us were not expecting that this will reflect in cyber space. From a long time we have started talking about Cyber War, now and then it is being said that World War 3 will be majorly a cyber war. Richard A. Clarke and Robert Kane have defined "cyberwarfare" as ***"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"*** in their book titled as Cyber War - The Next Threat to National Security and What to Do About It. So it could be stated that present condition is not cyber war but yes it could be called as **cyber tension** definitely**.**

Many reputed newspapers (offline and e-newspapers) have mentioned that various cyber-attacks have been performed by both the countries in past one month. One major point which has been missed is that there is also a chance that lots of other disturbing attributes may have participated in between which may not be from India or Pakistan but will make this situation more vulnerable and misguiding. But let's clear the objective of this article; it will not be focusing on the political tension between these countries, neither to prove the existence of these attacks, because ***it is not about these two countries only but also every nation should understand the common cyber threats, their impacts and how to prevent from them*.** Hence this article will be focusing on:

- Targeted Sectors
- Types of attacks which have been observed in past few days
- Impact of these attacks
- Preventive measures to be taken

As per very reputed news agencies it has been mentioned that in total in past one month approximately there were more than 20000 victims. The major attacks were observed on the assets of educational organizations, government organizations and IT firms.

The types of attack that have surfaced up till now are mainly **website defacement** and system locking using popular **ransomware** techniques. The snapshots of the websites during these attacks are available all over the internet which includes flags of the countries, some abusive messages, threatening messages etc., hence could not be included here.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Website Defacement

Website Defacement is an attack where attacker identifies vulnerabilities on a website or web server and then changes the visual appearance of that website by changing the data available on that website. The figure 1 and figure 2 shown below is sequence diagram which describes a common procedure of website defacement. Website Defacement is one of the very common and the oldest attacks which are still very popular. And the irony is still that very reputed websites get exploited till today by this attack. Vulnerabilities such as misconfiguration of web pages, weak passwords etc. leads to website defacement. Website defacement could usually be text defacement or image defacement.

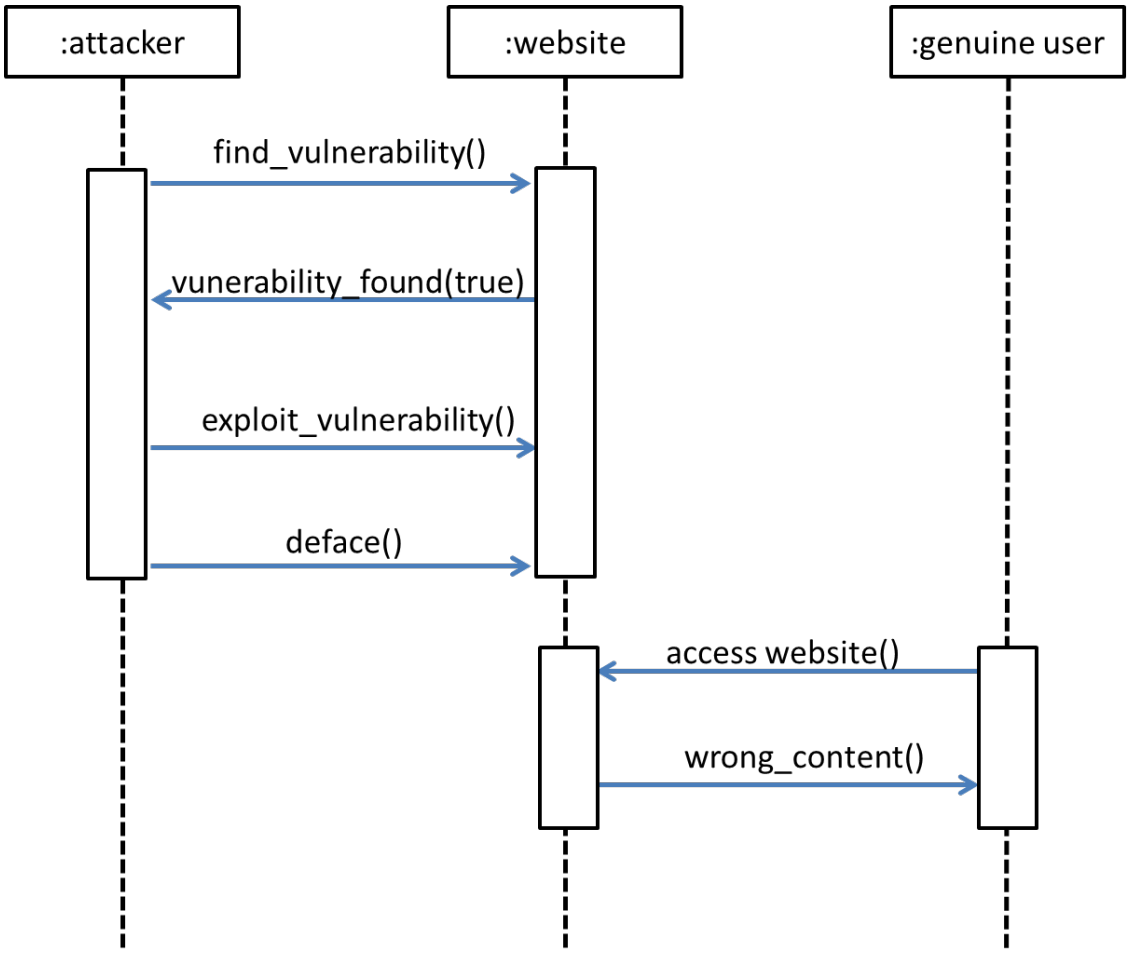


Figure 1

In Figure 1, as mentioned that attacker will try to find out vulnerabilities on the website like SQL injection, cross site scripting etc. Once vulnerability found, the attacker will try to exploit these vulnerabilities and once vulnerabilities exploited the attacker will deface the website i.e. either by changing the text or image. Similarly as shown below in figure 2, it may be possible that the attacker will try to gain access to the web server or website management systems, once access gained, the attacker will have access to the source files hosted on these servers. To deface,

Copyright © Cyber Defense Magazine, All rights reserved worldwide

attacker will replace the original files with fake files. Then in both the cases when a genuine user will try to access the website, instead of seeing the original and relevant content the user will access the false content.

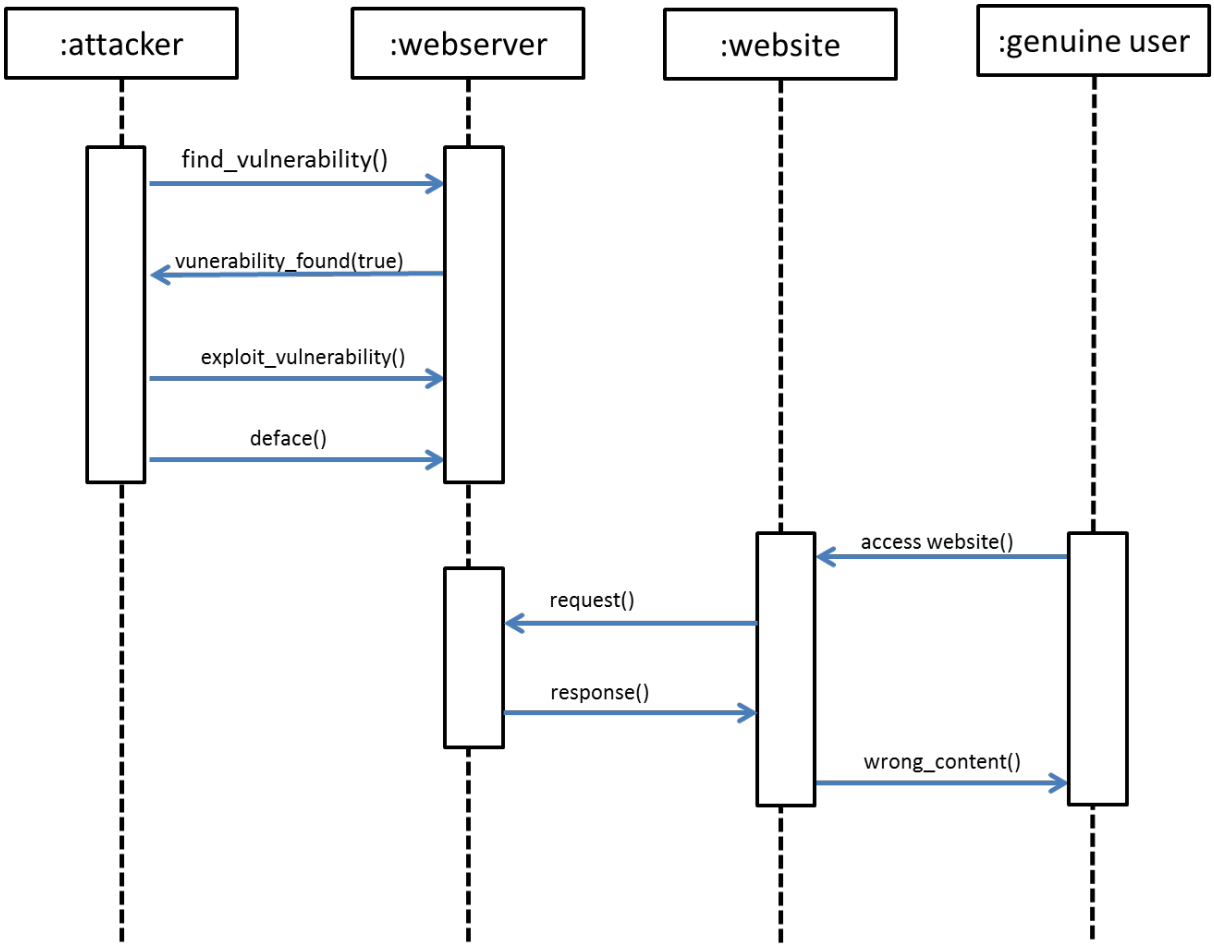


Figure 2

Website defacement will not cause any major disruption, but still it may have potential impacts, some of which are listed below:

1. **Data Breach**: Website defacement may not cause direct data breach but attackers may use it as trap, because website defacement is definitely noticeable. Hence when everyone is focused on defacement and performing corrective action, the attacker may take the advantage and try to steal potential data, install malwares or perform privilege actions.

2. **Reputation Damage**: The direct impact is reputation loss and creditability loss. A defaced website can be seen by anyone and this can be big influence on how users judge your ability for security.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

3. **Downtime and non-availability**: To reduce reputation damage, the website could be made not available for some time but this could be a major disruption, because root cause analysis and remediating vulnerabilities may take long time.

4. **Losing Customers and business**: It's very much understood that any of the above three impacts will give rise to customer loss which further will give rise to financial loss.

Preventive measures for website defacement may include:

1. **Safe API**: Be careful with the APIs and always use safe API because API may introduce SQL injection and in case parametrized API is not available make sure to escape special characters.

2. **Input Validation**: White list input validation is always recommended because it will help against SQL Injection, cross site scripting etc.

3. **Escape**: Always escape all untrusted data and special characters when taking input through the website.

4. **No misconfiguration**: Use strong passwords, never use default passwords and employ account management to prevent unauthorized intrusions. Never leave ftp services on anonymous access mode, always use strong password for the same.

5. **Penetration Testing**: Periodic penetration testing will help in identifying the vulnerabilities and will assure the strength against the exploits. Web application audits other than penetration testing will help in improving the security.

6. **Backup**: Having a backup of the site will help in reducing downtime and non-availability and will help in reverting to normal state. This will also ensure users about security capabilities and will build trust.

7. **Monitoring**: Monitoring is a continuous process i.e. it is not yearly or monthly while it is near to real time. Monitoring of unauthorized access, unauthorized changes to web servers, unexpected traffic, access to control servers etc. will help in preventing website defacement before it occurs. Also it will help in performing forensics and root cause analysis.

Ransomware

Ransomware, a word which is very much popular now days and many of us thinks that ransomware is one of the latest attacks while the truth is that the first known ransomware was identified in 1989 and its name was AIDS Trojan. But yes since 2011 and 2015 it has become very famous due to attacks on Windows and Mac OS respectively. And now ransomware is

Copyright © Cyber Defense Magazine, All rights reserved worldwide

available in various flavors mainly encrypting files so that victim can't use them, stopping important applications like web browsers and preventing victim from accessing the computer. Top ransomwares are tescrypt, crowti, brolo, fakebsod etc. There are certain stages in the ransomware attack and figure 3 shows the ransomware workflow. This shows how victim downloads malware unknowingly and that malware encrypts victims machine and files and the attacker asks for payment. Also it may be possible that victim downloads the malware from a received mail rather than visiting infected website.

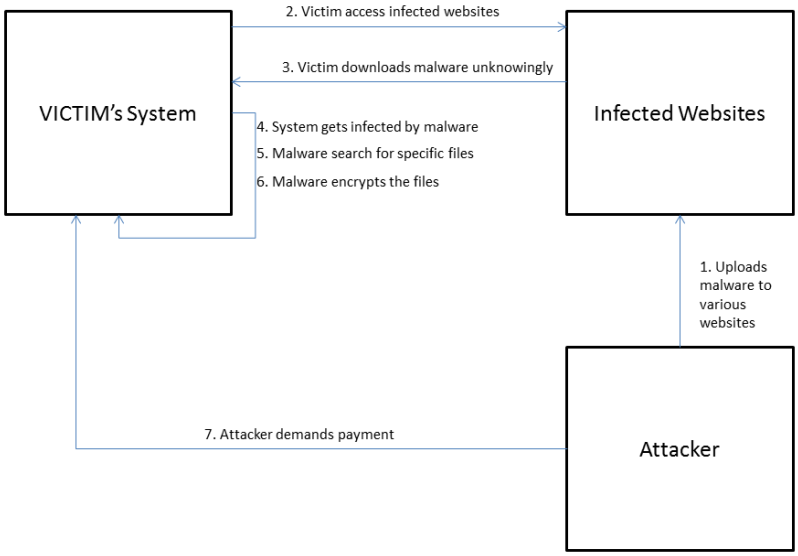


Figure 3

Major issue that arises due to a ransomware attack is of availability. The files may be physically present with the user, but the user may not be able to access it, simply because it is encrypted. After this attack, the attacker generally contacts the victim and asks for some amount of ransom, preferably in cryptocurrency (eg. BitCoin). Hence definitely financial loss is quite large in this scenario because it will be sum of business loss due to unavailability and money paid to the attacker.

Preventive measures for ransomware attack may include:

1. **Email Security**: Effective and up-to-date mail filtering protocols must be applied so that mails from unauthentic sources are blocked or reviewed by security officers. Avoid accessing unverified emails; avoid clicking links in the mails. The attachments should be scanned by the antivirus; then only it should be downloaded.

2. **Detect & Block**: Using effective firewalls to block the unwanted traffic so that malicious attacks/requests from known as well as unknown hosts could be blocked.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Not only firewall but IDS as well should be implemented to detect and block malicious traffic.

3. **Web Browser Security:** Use web browser protection solutions to monitor and analyze browser's state and block websites from delivering exploits.

4. **Update and Patch Management:** Regularly update software, applications etc. to protect against latest vulnerabilities.

5. **Back Up:** Always keep secure backup copies of important and sensitive files.

Conclusion

Website Defacement and Ransomware attacks are found to be the most common attack during this cyber tension between the countries. These attacks may lead to direct loss as well as there is large number of indirect impacts. But the common issue was non availability of the assets. Hence this is an alert for the organizations irrespective of the country to implement preventive measures which will definitely not ensure 100% security, but surely will reduce the likelihood and impact of the attacks which may occur in future.

About the Authors

Jatin Sethi is currently working as an Assistant Professor at Centre for Information Technology, University of Petroleum and Energy Studies (UPES) Dehradun, India. At UPES he teaches cyber security specialized subjects as well as core computer science subjects. He has completed his MS in Cyber Law and Information Security from Indian Institute of Information Technology, Allahabad, India in 2014. His area of interest includes Information Security Management System, Data Privacy, IT Governance etc.

Vatsal Jain is a student at University of Petroleum and Energy Studies currently pursuing a Bachelor's of Technology in Computer Science Engineering with specialization in Cybersecurity and Forensics by IBM. Currently he is Joint Secretary for the ISSA Dehradun Chapter. He may be reached at vatsal1511@gmail.com.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBER SECURITY EXCHANGE

DECEMBER 4-6, 2016

PGA NATIONAL RESORT AND SPA - PALM BEACH GARDENS, FLORIDA

www.cyber-securityexchange.com

#CYBEREXCHANGE

MEET THE SPEAKERS:

The Cyber Security Exchange speaker faculty is an exclusive community of innovators, **influencers, and leaders.** Embrace the **opportunity to enhance the power and reach** of your professional network by sharing three **days with the most respected cyber security executives in the industry, including:**

BOBBY SINGH
CISO
Toronto Stock Exchange

JOSH JAFFE
Director: Information Security Risk and Governance
Emerson

HARRIS SCHWARTZ
Global Head of Security
Levi Strauss

ALEX KOEHLER
Executive Director/CISO
Amgen

KATHERINE FITHEN
Chief Privacy Officer
The Coca-Cola Company

DENNIS DICKSTEIN
COO, Americas
UBS

PATRICIA COLLINS WEEDON
SVP & Global CISO
Discovery Communications

EDWIN MARTINEZ
CISO
CEC Enterprises

Empowering the Human Element of Cyber Security Across the Organization while Addressing Security Gaps and Vulnerabilities in the Ever-Changing Threat Landscape

- Strengthening third party and vendor relationships while reducing the risk privacy, security and compliance
- Evolution of Security Incident Response for more holistic enterprise management
- Effective business communications across the C-Suite to better secure the enterprise
- Inventive and productive ways to engage employees on cyber security awareness

BROUGHT TO YOU BY: IQPC Exchange

REQUEST AN INVITATION AT:
www.cyber-securityexchange.com | spexchange@iqpc.com | 813-658-2553 | Mention code: CYBERAD

Business Risk Intelligence: A Necessity Across the Enterprise

Josh Lefkowitz, CEO at Flashpoint

While the Deep & Dark Web has yielded important security considerations for some time, it's really been in the last 18 months that the industry has begun to understand how critical the intelligence gleaned from the underbelly of the Internet can support business functions across the enterprise.

As more companies have started proactively working to understand these opaque regions of the Internet more effectively, many decision-makers and stakeholders have recognized that intelligence derived from the Deep & Dark Web can help inform decisions, protect their organizations, and ultimately mitigate risks.

The primary challenges that exist are, one, that while the Deep & Dark Web isn't all malicious, there are risks for companies that try to explore it without proper expertise. And two, intelligence and data from the Deep & Dark Web have in the past only been used for specific security and intelligence teams, even though there are many groups within an organization that can benefit from Deep & Dark Web intelligence to shore up their understanding and awareness of risk.

The desire to overcome these challenges explains why Business Risk Intelligence (BRI) has been rapidly adopted by some of the world's largest organizations over the last year. BRI broadens the scope of cyber intelligence beyond threat detection to provide relevant context to business units not traditionally afforded the benefits of intelligence derived from the Deep & Dark Web.

While the integration of cyber intelligence into an organization's security posture has long been considered fundamental, traditional applications tend to serve solely cybersecurity teams and are therefore insufficient for fully-addressing security needs across other business functions.

As the overlap between today's cyber and physical threat landscapes continues to expand and create unprecedented challenges, many organizations are recognizing the critical need to inform key stakeholders far beyond what has been possible with the cyber intelligence status quo.

BRI surpasses the myopic, long-held industry standards for cyber intelligence applications to inform decision-making, improve preparation, and mitigate risk throughout an entire organization.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

BRI derived from the Deep & Dark Web was developed to better serve organizations' diverse needs by addressing a gap in the cyber intelligence market. This gap emerged years ago after cyber intelligence's role as a fundamental necessity was initially established within corporate America under the recognized label of Cyber Threat Intelligence (CTI). The CTI function facilitates a highly-reactive approach to security, as it is largely anchored across industry verticals by way of Indicators of Compromise (IoCs).

It's important to note that since CTI was developed solely to serve cybersecurity teams, it does little to support other business functions — many of which would otherwise benefit from Deep & Dark Web intelligence. Consequently, cybersecurity teams have typically been the only function to reap the benefits afforded by Deep & Dark Web intelligence — up until the adoption of BRI, that is.

BRI's widespread versatility enables organizations to not only bolster cybersecurity but also confront fraud, detect insider threats, enhance physical security, assess M&A opportunities, and address vendor risk and supply chain integrity. BRI provides the agile intelligence necessary to foster interdepartmental risk evaluations, help protect digital infrastructure, map threats to critical assets, reveal threats to supply chain management and identify physical security and business travel risks.

Organizations with robust BRI programs have successfully gained an increased understanding of the impact, relevancy and corresponding business risks from malicious insiders, hacktivist groups, nation state and cyber threat actors, and radical jihadists.

Given the mounting difficulties many organizations face in navigating a volatile threat landscape, BRI's cross-functional, comprehensive approach to intelligence has now become a requirement. As current economic, political, cultural, and technological externalities continue to create challenges across the enterprise, these same externalities have fostered an environment where threat actors thrive and their exploits become more sophisticated — thereby posing greater risks to organizations.

Such risks stem from our growing susceptibility to damages from attacks against critical infrastructure, global financial networks, and other elaborate exploits that undermine society's safety and confidence in trusted large-scale systems and establishments. Since such attacks can threaten all business functions across an organization, effective mitigation strategies should evidently involve collaboration from all business functions, which BRI facilitates.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

BRI is especially crucial given that traditional cyber intelligence applications — such as those rooted in CTI — are simply insufficient for proactively preventing or mitigating these emerging risks. As CTI fosters a reactive, indicator-based approach to security, it often does not enable decision makers to preemptively detect and mitigate attacks before they occur.

Given the multifaceted and often threatening nature of many emerging risks, prevention — when possible — is absolutely crucial. BRI's holistic approach addresses the high damage potential of many emerging exploits to help decision makers better reduce their organizations' risk.

Indeed, ransomware is one of many such emerging risks that has recently caused many organizations to shift away from CTI. Large-scale ransomware exploits have grown more common because financially-motivated threat actors have recognized just how profitable these attacks can be. Often used to target healthcare institutions, this type of malware can halt operations across all business functions and deprive organizations of access to critical systems.

Ransomware attacks can ultimately cause sizable financial losses, damaged brand reputation, or worse — so prevention is key. As ransomware continues to take center stage as a salient topic of discussion and concern within corporate board rooms, public-sector evaluations, and executive security conversations alike, more decision makers across the enterprise are recognizing that BRI's cross-functional, holistic approach to cyber intelligence is necessary for proactively mitigating these complex, dangerous risks.

Whether an organization has an entire department of seasoned intelligence analysts or a smaller team that needs more daily support, BRI can deliver relevant intelligence to help them make informed decisions and mitigate risk. However BRI is achieved, the mix of the right people, data, and technology is critical.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Cyber Attack Preparation Tips & Tricks

The World Wide Web is the new frontier, but unlike unexplored territory on the ocean floor or distant moons, there's already a massive crowd of people exposing themselves to its unknown risks.

This October a massive distributed denial-of-service (DDoS) attack on backbone service provider Dyn affected nearly every American with internet access in some way. The strain on backbone internet providers crippled websites as well equipped as Twitter and Netflix, and we can only expect to see more of this behavior in the future.

Large-scale attacks like this — while frightening — are infrequent occurrences, but the people behind them don't just take time off when they're not exploiting major network entities. Over half of small businesses reported being affected by a cyber attack in 2015, and that only includes the ones who noticed it.

So if you're a business owner, how can you defend against what seems to be an unavoidable evil?

Get Prepared

There are steps you can take to reduce your exposure. Cyber threats are primarily effective because many businesses don't understand how to prepare for them. Here are some suggestions:

- **Know Your Network.** Make sure you understand how all the machines in your network communicate. Identify bottlenecks and single points of failure.

- **Have a Disaster Response Plan.** Create regular backups of your data and store them offsite on a machine that does not communicate with your primary network. Understand how to restore your system from these backups quickly in the case of an emergency.

- **Educate Your Team.** Human ignorance is the vulnerability that most cyber threats take advantage. Make sure your team knows how to spot phishing attacks and avoid suspicious emails and attachments.

- **Have Security Software.** Proactive threat detection that uses heuristics allows modern security vendors to identify threats even when they are brand new. Many security suites offer a number of additional features to help protect your network's integrity or report a detected threat.

Keep your team informed about how to identify possible threats, and keep your system under tight surveillance — the combination of these actions is an effective way to protect your company's data. But what if you are attacked anyway?

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Act Quickly

If your security software or your personnel have reported an attack on your network, here's what to do:

- **Isolate the Threat.** Locate the machine where the threat was detected and remove its access to your network. Leaving it connected could allow the threat to move to other machines, which can quickly drive up the work involved to mitigate the scenario.

- **Harden Your Network.** Make sure that all devices on your network are using up-to-date software. If a security solution is in place, make sure it's allowed to receive the latest updates on new threats.

- **Have a Response Plan.** Your PR team should have a communications plan ready, particularly if your organization handles sensitive information. You should also have a security firm on hand with forensics experts who can trace the origin of the threat, analyze the extent of the damage to your system and advise you on how to clean your system and avoid similar threats moving forward.

- **Contact Authorities.** The FBI is responsible for handling cyber crime in the United States. Know how to contact your closest office and begin an investigation. Collect log files and other diagnostic information from your network if possible, for submission. Doing so might keep this from happening to others.

Communication is key. There are a number of commercially available technologies that let you monitor network resources for signs of an event. Once you notice something, engage the right people inside and outside of your organization quickly to achieve the fastest resolution.

Done right, you can avoid the shame many high-profile companies have had to endure.

About the Author

Megan Ray Nichols is a freelance science writer and the editor of Schooled By Science. She writes weekly on scientific news stories. Megan is a regular contributor to Datafloq, Big Data Made Simple and The Energy Collective. You can subscribe to her blog here and follow her on Twitter.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The Future of Cybersecurity

Augmented Reality

By Anouk Papillon, Senior SEO Manager, Userp.biz

As technology keeps developing, companies need to keep protecting themselves. We need solutions for physical security and, increasingly, for cybersecurity too.

The answer to protection measures of all kinds seems more and more likely to be Augmented Reality.

While it was regarded as something of a gimmick for many years, it has been influencing the areas of gaming, travel and retail for some time and is now also moving into other spheres.

Augmented Reality vs. Virtual Reality

Augmented Reality and Virtual Reality both try to create enhanced and immersive experiences for the user. Where Augmented Reality seeks to add to real-world perceptions, however, Virtual Reality seeks to add all-new ones.

Augmented Reality builds another layer onto whatever is happening in the physical world, via a headset or device screen, while Virtual Reality isolates users as much as possible from sensations in the physical world. Headsets and other wearables are used to create worlds with new visual, graphic and other stimulations.

A realtor might, for example, show prospective buyers a new house and take them on a Virtual Reality tour where they can explore the property from a remote location.

By contrast, Augmented Reality could be used to show how improvements or changes could be made on existing structures within a house.

Showing people the possibilities for where they could travel, how they could change physical structures or objects and what items they buy could look like, are all possible with Augmented Reality.

Both Augmented and Virtual Reality have also been used in different training and education exercises, and are now even likely to be used by governments to demonstrate changes and speak with constituents.

Their powers of immersion, interactivity and demonstration are great, and people are exploring and applying them on an increasing basis.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Augmented Reality as a Cybersecurity Measure

Legal security measures and illegal ways to circumvent them are both becoming more sophisticated all the time, and Augmented Reality could give companies the edge they need to keep their information secure.

Different projects are currently being developed, with the main idea being to reduce the mental demands on cybersecurity officers and deliver important information to them so that they can stay focused on whatever task they are performing.

It's similar to the technology that has been used by aeroplane pilots for years, and is another example of how humans and technology can work together in the modern world.

On the flip side, it should also be remembered that what is used or trusted can also be detrimental.

Wearables used for Augmented Reality could be hacked into and used for surveillance, and a reseller could leak some of your tools online, as was recently seen with Cellebrite and McSira Professional Solutions.

In the end, cybersecurity is always going to be, by its very nature, a proactive endeavour. Constant vigilance and updates, including Augmented Reality, are the best way of moving forward.

About The Author

Anouk Papillon is a Senior SEO Manager at Userp.biz, focusing on Outreach & Content Creation. SEO Specialist by day and freelance writer by night.

She is passionate about new technologies, innovative ideas and future trends, especially in the entertainment and online industry.

When not working, or writing, you can find Anouk strolling along Cape Town's beaches, hiking mountains or reading.

You can email her at anouk@userp.biz.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Mitigating Detection Gaps

Corporate Security teams are often governed by strict business processes and controls that can impede rapid adoption of new security solutions or changes to existing ones. The result of stringent change controls can sometimes mean organizations are forced to put maximum reliance on their security solutions and vendors. This is especially the case with inline security solutions (solutions that provide the ability to block certain traffic), companies are often extra cautious with updating these appliances in order to minimize risk of blocking business applications or communications. This severely reduces the value of the investment in these solutions.

Detection Gaps – An Inconvenient Truth

False Negatives can happen from time to time and they can occasionally be the precursor to an intrusion or widespread infection. Companies that rely on signature based security solutions should consider the risk of situations where new threats (or yet to be discovered ones) are active in the wild without detection via existing signatures. It is therefore possible for the environment could be exposed to malicious activity and not generate security alerts until adequate security updates have been published perhaps days or weeks later.

When a new threat in the wild is discovered, that initial research is often proprietary information that will be used by security companies to protect their customers *before* publicly sharing analysis (usually via a blog post), this is especially the case with high profile Zero Days, malware campaigns and web site compromises.

Once information on a new threat is made public, security vendors that have not yet discovered the threat or lack detection will typically respond by scrambling to update their own detection libraries, this can take anywhere from hours to days depending on the complexity and scope of coverage needed. In cases where there is evasion of the core detection technology, the time to an update could be even longer. During these temporary detection gaps, companies can be exposed to threats.

Through the use of encrypted delivery techniques as well as the flourishment of underground crypting services, it's common for malware payloads to go initially undetected by AV products, especially if advanced features like heuristic, behavioral and cloud analysis are not enabled.
Your next line of defense might be network based detection if the malware is beaconing out to command & control infrastructure. If callback detections are also missed, the malware can embed itself in your environment and communicate without causing any alerts for a sustained period.

This has been the case with many of the POS intrusions we've seen in recent years.
Whether due to outdated Security Infrastructure or False Negative situations, this has had a devastating impact on businesses

Copyright © Cyber Defense Magazine, All rights reserved worldwide

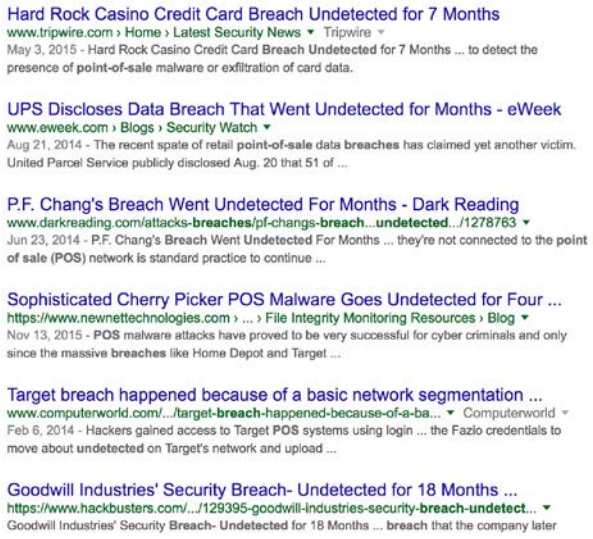


Figure 1 – Some recent POS intrusions

POS threats are a good example of how Threat Intelligence can be leveraged as POS malware is typically not as widespread as much as commodity malware. Reserved for specific environments and using infrastructure that can often hide in plain sight, these threats may need to be sought out by teams using specialized tools and techniques as opposed to waiting for alerts.

Commodity malware (also referred to as Crimeware) is the most common type of malware and includes threats like Ransomware, Banking Trojans, Downloaders and AdFraud bots to name a few. In many cases, the delivery channels for these infections are phishing emails, malvertising campaigns and compromised websites, these are all also subject to False Negative scenarios where detection is not available until the threat is discovered or published.

Figure 2 – Ransomware infection after being exploited by a Exploit Kit.

Many web based infections involve multi-stage attacks (i.e. Exploit Kits) that change hosting infrastructure, URL patterns, exploitation techniques and payloads at a high frequency, all in an effort to stay one step ahead of detections.

Higher end security solutions may be able to detect anomalous network traffic or exploit code, however Exploit Kits have proven time and time again that the professional cybercriminal's ability to adapt to modern detection technologies and evade them is constantly evolving.

Staying abreast of indicators like the patterns, domains and delivery channels associated with these threats can help organizations avoid them and reduce the impact of detection gaps.

Minimizing The Detection Gaps With Threat Intelligence

Armed with threat intelligence, security teams can pro-actively investigate and hunt for evidence of suspicious or malicious activity associated with the threats mentioned. Not every company

Copyright © Cyber Defense Magazine, All rights reserved worldwide

has malware analysts and threat researchers on staff to track and develop mitigations for newly discovered threats. Having threat intelligence available to your security team enables them to be proactive and hunt out threats that current security solutions may be blind to.

Some examples of leveraging Threat Intelligence can include but are not limited to:

- Checking for compromised email accounts belonging to your org or business partners
- Blocking web and email access for phishing and typo-squat domains
- Searching logs for malicious domains or URLs that are *not* being blocked
- Consuming feeds for compromised websites and blocking or limiting access
- Monitoring suspicious domain registrations and pre-emptively blocking
- Tracing web based malware infections back to the source network or website
- Generating custom intrusion detection signatures
- Checking for evidence of TTPs within your environment
- Looking for Lateral Movement activity

These are just a few ways security operations teams can leverage threat intelligence and mitigate the impact of detection gaps when they arise.

Another use of threat intelligence would be to replay packet captures that test the effectiveness of signature based security appliances with known malicious traffic samples. This can be done using open source tools like tcpreplay and publicly available pcaps.

Some sources for malicious pcap samples include:
http://www.malware-traffic-analsyis.net
http://threatglass.com/
http://www.pcapr.net/
http://contagiodump.blogspot.com/2013/04/collection-of-pcap-files-from-malware.html

By establishing a threat intelligence program, organizations can join the hunt and enable their security operations teams to proactively find and mitigate threats before detection gaps are exploited.

About the Author

Josh Gomez

Senior Security Researcher for Anomali, a provider of market leading threat intelligence platforms. He has more than15 years experience in the networking and information security industries. Prior to Anomali, Josh was a senior member of FireEye Labs where he specialized in the research and detection of exploit kits, malvertising and crimeware. He has also developed AV/IDS/IPS detections for Symantec and led security operations at a large Fortune 500 retailer.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CELEBRATING 25 YEARS OF SUCCESS

25TH ANNIVERSARY

"Digital India"

Convergence India 2017

International Exhibition & Conference

8 9 10 February 2017 | Pragati Maidan, New Delhi

South Asia's largest ICT expo

Show Highlights

500	30	150	20,000
Exhibitors	Countries	Speakers from World over	Visitors

Technology Showcase

• Telecom • Broadband • Cloud & Big Data • IoT • Digital Homes • Mobile Devices • Broadcast
• Cable & Satellite TV • Film & Radio • Content Creation, Management & Delivery

Co-located events and Add-ons

• Internet of Things India expo 2017 • 4th Telecom Summit • GSMA Open Day
• 2nd SCTE India Awards • Start-ups Showcase • Mobile Devices & Accessories Zone

Co-located Expo

Internet of Things India expo 2017

Convergence • Connecting • Convenience

Support

Ministry of Electronics & Information Technology
सत्यमेव जयते Government of India

Digital India Power To Empower

Media Partner

CDM CYBER DEFENSE MAGAZINE

Organiser

30 YEARS

Ei Exhibitions India Group

For Exhibition & Conference, please contact:
Mr. Yash Menghani, Senior Manager, yashm@eigroup.in
217-B, Okhla Industrial Estate, Phase III, New Delhi 110 020
Tel: +91 11 4279 5000 | Fax: +91 11 4279 5098
www.convergenceindia.org

Mission Critical Security and the Rise of the Private Internet of Things

by Stewart Kantor, CEO, Full Spectrum

We live in a world where constant data connectivity has become the standard, allowing us to access information from any number of devices operating over the public Internet. While ubiquitous connectivity poses enormous opportunities for critical infrastructure, data communications managers for our electric grids and natural gas, transportation and water systems, are conflicted by the ease of implementation offered by the public wired and wireless Internet. Even with strong firewalls in place, the public internet creates exposure to hacking or cyber-attacks, which could result in partial or complete loss of control of critical systems.

The DDoS attack launched on Dyn is the most recent example of a cyber-attack that crippled popular websites like Netflix and Twitter, and although the cost of this was mostly economic and general inconvenience, it highlighted the exposure to the nation's critical infrastructure as these industries contemplate leveraging the global Internet of Things (IoT).

As an example, smart grid applications being proposed by electric utilities across millions of square miles and millions of locations offer radical improvements in operational efficiencies while creating enormous exposure including the loss of control or access to portions of the electric grid. The good news is that new data communications technologies are emerging that allow a utility to leverage the efficiencies of internet protocol with isolation from the public internet.

The US electric grid is currently undergoing a revolution driven by the rapid adoption of millions of renewable energy resources at the grid's edge. In order to optimize the supply and demand of electricity in real time, utilities need precise monitoring and control of these new sources of generation.

Specifically, they need highly reliable and secure communications to the power inverters attached to solar installations and power storage units. The most readily available and obvious connections are available from public network providers either from your cell phone or cable provider.

These networks may be appropriate for billing type function, but they are not secure or reliable enough for a utility company for grid management.

Public Data Networks Not Available, Not Good Enough

Ensuring real-time data communications to all data control points along the grid is one of the increasing challenges faced with the adoption of a new IoT structure – particularly with increased network traffic over public networks and prominent threats from hackers looking to

Copyright © Cyber Defense Magazine, All rights reserved worldwide

interfere with communications. In addition to security and capacity concerns, network latency is of paramount importance in utility networks. Many advanced applications require almost an instantaneous and predictable response - below 100 ms.

Public network providers are unable to guarantee this type of response time for many structural reasons. And lastly, public networks are designed to provide connectivity where their customers live and work.

Utility infrastructure can be dispersed over wide areas and are not strictly confined to populated centers. And as many of us have experienced with public cellular data networks, ensuring coverage in densely populated, urban areas can be a challenge due to terrain, foliage and physical structures. In rural areas, connections can be non-existent.

Monitor & Control with a Private IoT

To ensure all control points and smart devices are connected securely, and communications are not hindered via latency challenges or hacker threats, utilities are starting to introduce private wireless data networks using licensed radio frequencies and software defined radio technology.

Unlike the public cellular data networks that are often saturated with consumer data traffic (e.g. video downloads, streaming, etc.), these private networks are owned, operated and deployed by the utility, allowing them to manage millions of assets and remote devices without ever connecting to the public internet.

Software defined radio communications over private wireless data networks offer utilities an IoT communications solution designed to meet their specific needs. Compared to public cellular data networks, including 4G LTE systems and proposed 5G systems, private wireless networks have been designed to cover the entirety of a utility's service territory, dedicating enough bandwidth for the appropriate functions.

Both public and private wireless systems feature downlink and uplink capabilities, however, public LTE systems allocate most of their bandwidth to downstream capacity as this is often required for consumer use.

Utility private networks, however, are designed for high capacity upstream traffic (or pulling data back) to their network operations center. In addition, there is a significant difference between public and private utility networks in how data traffic is prioritized based on location, application and device.

Public LTE networks, since they are often filled with consumer traffic, can be unpredictable in terms of latency, making it difficult to operate many time sensitive grid functions.

Private networks however, fall solely under the control of the utility, allowing them to keep the network clear for their own communications.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Securely Separating from Public Threats

Creating an added layer of security at all control points throughout the grid is one of the most critical benefits of a private wireless data network. The recent hijacking of the Ukrainian power grid and the DDoS attack on Dyn servers clearly illustrates the threat to operational reliability posed by public networks for grid management.

A private network provides complete separation from the public networks, both virtually and physically with a distinct air-gap, allowing for non-routable IP addressing with closed loop monitoring and control. In addition**, the utility is able to maintain control over system up-time, mean time to repair (MTR) and an awareness and control over who and what is allowed access to the network.**

Private wireless networks and software defined radio technologies have made grid automation a reality without compromising on security or network speed. Private networks are providing better control over the grid and better monitoring of the use of existing energy resources and new distributed energy resources, both of which are changing our grid structure significantly.

Forward looking utilities have already started to adopt these new and innovative communications technologies to proactively meet current and future security and latency demands resulting from the grid's shift to automation for renewables, and to bring our power-grid into a new era of energy control.

About The Author

Stewart Kantor is the CEO and a co-founder of Full Spectrum Inc, a wireless telecommunications company that designs, develops and manufactures FullMAX, its private broadband wireless internet technology for mission critical industries.

He has more than 20 years of experience in the wireless industry including senior level positions in marketing, finance and product development at AT&T Wireless, BellSouth International and Nokia Siemens Networks.

Since 2004, Mr. Kantor has focused exclusively on the development of private wireless data network technology for mission critical industries including electric utilities, oil & gas companies and the transportation industries. Stewart can be reached online at inquiries@fullspectrumnet.com, @Full_Spec_Net and at our company website www.fullspectrumnet.com.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Stay Vigilant, We're in for a Wild Ride

2017 Security Predictions

By: Scott Millis, CTO, Cyber adAPT

2016 brought about more cyberattacks than we thought possible, especially involving ransomware, and we definitely won't see that trend breaking stride in 2017. In February of this year, an IRS hack led to an estimated 700,000 stolen social security numbers and other sensitive information. This ruthless attack severely increased the risk of identity theft for all compromised victims.

By next year, we expect every single adult in the US will know a **blood relative that has had their identity stolen** – the Internal Revenue Service reported that 2.7 million people had their identities stolen in 2014 and according to TransUnion, 19 people fall victim to identity theft every minute.

Here's a quick tip: *When you elect to use credit cards, stick to the 'chip and pin' cards – no swiping. Online, use your credit card issuers 'one-time-numbers' for purchases. Get a shredder and use it. Think of it as 'safe recycling'.*

Now I'm no fortune teller, but there are a few predictions I can make for the coming year – that I think most of us in the security industry can agree on:

- **Ransomware** will spin out of control – Symantec's Security Response group has seen an average of more than 4,000 ransomware attacks per day since Jan 1, 2016, a 300-percent increase in the average 1,000 attacks per day in 2015 the company highlighted in its 2016 Internet Security Threat Report.
    - *TIP: The best current defense against loss from this attack is to make backups of all your data in a separate place. Regularly and often.*

- **Dwell time** for breached networks (up to 2 years in some extreme cases) will see zero significant improvement.
    - Ponemon Institute found that when a breach was identified within 100 days, average costs were $5.83 million per breach. However, if a breach went undetected for more than 100 days, costs rose nearly 40%.

- **Mobile will continue to rise** as a key point of entry – with at least one if not more major enterprise breaches will be attributed to mobile devices. A Ponemon Institute report found that for an enterprise, the economic risk of mobile data breaches can be as high as $26.4 million and 67% of the organizations surveyed reported having had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- Mobile payments will bring our 'what ifs' to reality – biometric and 'let me take a selfie' sensations will only become more common as people realize that passwords can quickly become a liability – MasterCard's 'selfie pay' and Intel's True Key are just the tip of the iceberg.
- *TIP: CAUTION – treat your biometric data like your other precious financial and personal data.*

- **IoT vulnerabilities** and attacks will be on the rise AND will increase the need for standardization for various security measures – hackers at this year's Def Con found 47 new vulnerabilities affecting 23 devices from 21 manufacturers.
  - October saw a massive distributed denial of service (DDOS) attack on major global websites including Twitter, Netflix, Reddit and the UK government's sites – reportedly powered by the Mirai botnet made up of insecure IoT devices.

For the sake of everyone's personal and professional security, I hope these issues will not be as grandiose as we predict – however, the realist in me says otherwise.

Dear 2017,

We will prepare for your cyber security warfare as best we know how – **monitor** inside the network, **protect** outside devices, and **stay hyper-aware** of all activity-in-motion in between.

Sincerely,

Scott Millis and the Cyber adAPT team

About The Author

Scott Millis is the Chief Technology Officer of Cyber adAPT. Scott is a senior IT executive and security industry pioneer with an exceptional talent for aligning security and business objectives.

Formerly the Chief IT strategy officer at McAfee, (now Intel Security), he brings a deep understanding of all aspects of IT across diverse sectors including manufacturing, distribution, large enterprises and professional services. Previous positions include CTO at Courtlink and SVP, Data Processing at Foundation Health Corp. Scott's role at Cyber adAPT® includes bringing his years of experience in IT to provide strategic market direction through interactions with the industry's top business leaders. Scott studied Computer Science at the University of California at Irvine and, more recently, has been certified as a wine sommelier by WSET, (the Wine and Spirits Education Trust). Scott can be reached online at smillis@cyberadapt.com or https://twitter.com/scottmillis and at our company website www.cyberadapt.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CNI PROTECTION | CYBER SECURITY | POLICING AND LAW ENFORCEMENT
MAJOR EVENT SECURITY | BORDER SECURITY | OFFENDER MANAGEMENT | SERVICES

SECURITY & COUNTER TERROR EXPO

PROTECT | PREVENT | PREPARE

3-4 MAY 2017 OLYMPIA LONDON

Supported by

Home Office

The UK's Leading National Security Event

Meet 10,000+ senior public and private sector security professionals

Book your stand today

T: +44 (0) 20 7384 7894
E: sophie.mckimm@clarionevents.com

www.sctx.co.uk/cyber

@CT_EXPO

www.sctx.co.uk/linkedin

Sponsored by

GEOQUIP WORLDWIDE

sodexo QUALITY OF LIFE SERVICES

PELCO by Schneider Electric

Organised by

CLARION EVENTS

It's the Industry Titans Against the Federal Deities

Ensuring zero intrusion with best practices in the encryption software industry

by Anamika Kumari, Content Writer, Allied Analytics LLP

Veracrypt tracked the success route of Truecrypt with great agility. The rise of the latter at the encryption software industry skyline was as rapid as was its decline. A recent audit highlighted its architecture to be infested with critical loopholes that made the system vulnerable to external threats. A series of security fixes followed the internal audit that began in August 2016. Two months later, the developers came up with Veracrypt1.19 a more secure version of the previous format. It does include some issues that could not be resolved due the intense complexity in their codes, yet can be handled by religiously adhering to the safe practices as outlined in the Veracrypt User Manual.

Empowerment of open source frameworks

How is it that a similar file-system level encryption (FLE) strategy failed earlier, while another encryption software tool developed from the same source code saw the daylight of success? A close observance to certain government strategies and their security policies might lend you some answer. Our focus here, is on the commendable support handed out by the Open Source Technology Improvement Fund (OSTIF) towards the safekeeping and improvement of similar projects. Among the others that were patronized by the OSTIF are OpenSSL, OpenVPN, GnuPG, and OTR messaging. These platforms target to protect the privacy concerns of public users over secure internet, private networks, email servers, and public chat networks.

Rising above the federal dilemma

The global encryption software industry got wound in an unexpected turn of events in 2013, when global surveillance revelations began trickling from NSA's debauched child Edward Snowden. The first world was already concerned about the data-in-transit and data-at-rest critical to their business and enterprise. With NSA's intrusion, the technology development programs were instantly accelerated. The result is evident; North America now represents the largest market for data-at-rest encryption software solutions for both FLE and FDE (Full Disk Encryption).

The role of non-profit organizations in the upraise of encryption software industry is under microscope of the federal governments. The battle will intensify with the recent change in political demographics of the U.S. The encryption debate in the region so far has caused ripples that have been felt across the globe. Amidst the tug of war between product developers and the government agencies continue, compliance to the security breach notification law is a rather imperative criterion of selection.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Technology reinforcements from vendors

The developer and vendors in the global encryption software market know the best practice guidelines by heart and soul. They have a defined agenda to guard the interests of their consumers and consequentially their own business. The foremost in feature in this list is to steer clear of any provision for backdoors. Virtual drive creation and encryption, whether on a system or on cloud, is another suggested approach. Some of the products out there also offer overwriting the original files at the storage location once a deletion attempt is made post the creation of an encrypted copy. Even in the presence of more intricate algorithms, Advanced Encryption System (AES) remains the standard (and approved by U.S. government) for regular users. The combination of public and private keys for transfer and reception of secured file sand folders is another practice that is a benchmark for evaluating the robustness of an algorithm.

User awareness and responsibilities

However, the above-mentioned practices collectively comprise one side to the complete story. On behalf of the enterprises and consumers that employ these products at the end of the supply chain, there are far-reaching and minute considerations that need to be realized before making any purchases. A user is expected to compulsorily realize possible vulnerable nodes in their system. Next, a distinct segregation of levels is required in which the encryption strategy will be employed. Safekeeping the guarding keys and passwords from being potential threat sources is an obvious requisite. A close monitoring of the employee-owned devices and encouraging them to use end-to-end for these is yet another precautionary move which strengthens their network security.

The global encryption software industry is motivated by these social, governing, and technical factors. Its impending growth and success lies in these best practices, which when adopted aptly by the manufacturers and end-users will overcome potential hindrances and achieve outstanding financial targets.

About The Author

Anamika Kumari is a Level II Content Writer at the Allied Analytics LLP.

Anamika Kumari has pursued her Bachelor's degree in Electrical Engineering, and is certified in industrial automation. She is deeply fascinated by the impact of modern technology on human life and the earth at large. Being a voracious reader, passionate writer, and a critical observer of market dynamics, she has a strong taste for the hidden science behind all arts.

Anamika can be reached online at anamika.kumari@alliedanalytics.com and at our company website http://www.alliedmarketresearch.com

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Six Reasons PIV-I Has Emerged as the Standard For High-Assurance Identity Management

By Abrar Ahmed, CIO and Senior Vice President, SureID, Inc.

In a world where breaking news about high-profile cyberattacks seems to be a daily occurrence (the Yahoo September 22, 2016 data breach is a recent example), the federal government has begun dramatically increasing the level of security surrounding its IT systems and processes.

According to Gartner Research, often the weakest links in a security paradigm are "privileged accounts" with access to sensitive information. Within the federal government landscape, this sensitive but frequently unclassified information known as CUI (controlled unclassified information) is coming under increased scrutiny both inside and *outside* the federal purview.

As a result, federal contractors with both privileged and non-privileged access – and that handle CUI – face significant new compliance obligations.

Last year, the National Institute of Standards and Technology (NIST) released a special publication called SP 800-171 that calls for "the protection of CUI while residing in non-federal information systems and organizations." This includes "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified," which was first introduced as a definition in the DFARS 252.204-7008/7012.

Federal government contractors that handle a type of CUI called "covered defense information" (CDI) for the Department of Defense (DoD), one of the first agencies to adopt new regulations that implement NIST SP 800-171, are facing a compliance deadline of December 31, 2017.

Failure to comply could put contractors at risk of losing covered contracts and becoming ineligible to bid on future ones until the requisite obligations are satisfied.

Multifactor Authentication & PIV-I

NIST SP 800-171 lists 14 "Security Requirement Families" that defense contractors handling CDI may need to satisfy to win and maintain covered DoD contracts. One Security Requirement Family in particular requires the most significant attention from such organizations: Identification and Authentication.

In short, a simple username and password no longer will be sufficient to authenticate an individual's identity; rather, an organization must implement a multifactor paradigm, such as a username and/or PIN (something you know); a biometric marker such as a fingerprint (something you are); plus a smart card (something you have).

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Implementing such a system will provide significantly improved security versus the traditional username-password construct.

Several basic multifactor authentication frameworks exist that will satisfy the multifactor authentication mandate. Examples are soft tokens and hard tokens (e.g., smart cards, key fobs, or dongles) designed to store user credentials, and one-time passwords (OTP) sent to a mobile device.

Nevertheless, these solutions do not provide both the high-assurance identity proofing and robust physical-logical access—all within one single smart credential—as the personal identity verification (PIV) used by federal agencies and the similar credential for non-federal entities: personal identity verification-interoperable (PIV-I).

The PIV-I framework leverages a photo, fingerprints (biometrics), cryptography and a PIN and provides a powerful and cost-effective way to deliver strong protection against security breaches from nefarious actors. It heightens the defenses against cyberattacks, in contrast to username and password combinations, which are particularly susceptible and can easily be compromised.

Exploring the Value of PIV-I

What makes the PIV-I security framework so effective? Here are six reasons to implement PIV-I to support a multifactor authentication strategy to satisfy NIST SP 800-171.

1) Door to Desktop. Typically in an enterprise environment a proximity badge is used for identification and physical access. In addition, for logical access, a username and password combination often represents the security token. In contrast, PIV-I provides for a single high-assurance identity credential that can be used to access everything from doors to desktops in a secure manner. The benefit of this is simpler access management that includes full lifecycle identity management and ongoing screening of existing credentials.

2) Platform Agnostic. PIV-I is readily adaptable across a diverse employee base to achieve the highest level of security. For example, the PIV-I credential can be trusted by any entity, either government or business, that accesses the Federal Bridge. By contrast, a construct like one-time passwords (OTPs) is often tied to a specific device. Although OTPs can be agnostic, the same level of assurance does not exist with this option.

3) Cryptographic Data Protection. The PIV-I framework facilitates a variety of important security features within each individual credential, providing increased confidence that sensitive data won't be intercepted, including the ability to:

- Digitally sign documents (non-repudiation)
- Authenticate to network resources
- Encrypt messages for communication

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- Authenticate with an access control system that utilizes the same tool within well-defined standards—ensuring the solution will work with a myriad of technologies, from mainstream workstation and server operating systems to door readers and management systems that leverage cryptographic standards

4) Highest Assurance Level. The federal government has established policy setting forth specific identity assurance standards for various levels of trust associated with different credential types referred to as "Assurance Level."

This federal policy identifies four levels of identity assurance with level one being the lowest and level four representing the highest. PIV-I credentials are considered Level of Assurance Four (LOA4) because they meet the requirements of in-person identity proofing, hardware-based digital certificate storage and secure issuance policy ensuring the appropriate person receives the correct credential.

No matter what role the individual may play within the federal-nonfederal CUI paradigm, using a PIV-I credential reinforces the security-aware mindset that is so important to ensure data and the access to it remain secure.

5) A Mobile Credential. PIV-I can be utilized as a "derived credential," which is carried on a mobile device instead of a card. This option provides a cost-effective alternative to adding smart card readers to mobile devices or replacing machines that don't support the form factor. A mobile device also improves productivity by accommodating employees who travel often and rely on smartphones and computers to accomplish work tasks.

6) Simplified Access Management. Through PIV-I, system administrators can check the status of any credential within their network, significantly reducing the lag time involved with identifying and refusing a compromised credential.

Is Your Organization Ready?

As witnessed by the fallout of the recent Yahoo hack, the price of a major breach can be immense. The clock is ticking toward the December 31, 2017 deadline for affected DoD contractors to come into compliance with NIST SP 800-171.

The time to act is now; no other identity authentication paradigm has the requisite strength in its credentialing process to match PIV-I for organizations contracting with the federal government.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

How to investigate a cybercrime scene?

By Milica D. Djekic

The crime may appear anywhere – even in a cyberspace. It's simply a social phenomenon which would include people to deal in an inappropriate manner. So, as it's well-known – the cyberspace got a place of the big folk's concentration. It's so logical that such a spot could get potentially threatening to someone's safety and security.

Basically, that's the fact! Through this article, we would try to discuss how cyberspace could become our new cybercrime scene as well as attempt to provide some insights how such a case could get investigated.

Step 1: The motives

Many people would believe that sitting at home in front of their computers with the internet connection would make them feel secure. Unluckily, that's not the fact.

The cyberspace is a place of many troubles and headaches. As we said, even sitting at home and surfing your favorite web pages cannot protect you from a crime.

Although it's about the cyber environment, we would call that crime a cybercrime. So easily, the bad guys could steal your confidential data, discover your work's IP address or get money from your bank's account.

Once someone has decided to hack you, there is a huge chance that you would become the next target. It's only a matter of time and effort how long it would take before you suffer your first breach.

The question here would be what drives those folks to attack someone's computer or the entire network. There is a vast variety of reasons and we would try to analyze some of them. First, many hackers would get led with the desire to do something spectacular, so they would join that business for their adventurism.

Also, we should get aware that some hacker's would be politically, religiously or ideologically motivated and some of them – even state-sponsored. Being government-sponsored means that

Copyright © Cyber Defense Magazine, All rights reserved worldwide

hacker would officially or unofficially work for some country and try to obtain the confidential information from the enemy country through cyber means.

Finally, the real cyber criminals could be some sort of adventurists – similarly as the guys who would plan the armed robbery of the bank – but their reasons are more or less the same – they want the MONEY! In other words, those folks would be so financially motivated and seek an opportunity to use their skills to get a good benefit.

Luckily to all of us, anyone doing anything in a cyberspace would leave a trace, so it's mainly possible to resolve such a case.

The area dealing with such a capacity is called cyber forensics and through this effort – we would analyze how cybercrime investigation goes on and how capable the Law Enforcement agencies of today are to conduct a skillful investigation and prepare a qualitative documentation for the court.

Step 2: The cybercrime got discovered

Once the bad guys got a condition to commit a cybercrime, they would do so. It's a matter of routine checkups when such a case would get discovered. It's recommended to periodically control your IT asset in order to confirm if everything got appropriate.

Once the IT Security Professionals have discovered a cybercrime, they would contact the authorities which would conduct a skillful investigation using digital forensics tools.

Those tools would offer to experts to capture some evidence and prepare them for the next step of the investigation which is an analysis.

Here, we would want to mention that some digital forensics tools could be downloaded from the web for free, but it's necessary to leave your personal details in any case.

This would suggest that such a marketplace got well-controlled, so IT Security Professionals would mainly use those resources.

Step 3: The investigation has happened

The next step with the investigation after collecting the evidence and not interfering with the cybercrime scene making the permanent changes would be to analyze such a gathered data.

It's necessary to pass through many trainings and educations as well as gain a plenty of practical experience before you become a Digital Forensics Professional.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The entire analytical process would provide the skillful reports as an outcome. Those reports would further be transferred to a court, so the case would get continued there. Many countries would not recognize cyber offences as a crime for a reason they would not deal with any legal regulations about so within their societies.

Also, even if the country is capable to conduct some investigation, it could be quite trickery to the court's members to deal with the digital forensics reports due to the lack of skills and expertise in that area. So, how to conclude the case – in a general way?

Step 4: The case got concluded

The case should lead to an arrest of the suspect and such a person should appear on the court. In a practice, many of these cases would get the international character for the reason the hackers or cyber criminals would belong to the international gangs.

In such a way, it's important to distinguish which country got a jurisdiction over whom and conduct the investigation and the entire court's process following the international legal regulations.

The final decision here should be a duration of the punishment or maybe a recommendation what to do with those individuals. This is a good example how the international collaboration may work in a practice and how it's significant to establish a reliable co-operation following the best practice in a field.

About The Author

Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

IoT ASIA | 29 – 30 March 2017 SINGAPORE EXPO

INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS
TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES

Establish your presence and meet new customers at **Asia's leading IoT event!**

www.internetofthingsasia.com | #iotasia

Industry Recognition

ufi Winner of the Marketing Award 2016

2015/16 #IoT Awards

Singapore Experience Awards 2015 Recipient

2014/15 Internet of Things Awards

Organised by

SiAA

SingEx Powering Your Business Events

Founding Partners

Institute for Infocomm Research A*STAR

HUTCAB SERVICES

LINKWISE TECHNOLOGY

日経BP社 Nikkei Business Publications, Inc.

TCAM Technology Pte Ltd

Top Systems Security & Compliance Essentials

By Destiny Bertucci, Head Geek, SolarWinds

As 2016 comes to a close and we look to the year ahead, one thing we can expect to remain a constant is cybersecurity threats. Despite greater awareness, in 2017 we expect there will be exponential increases in both the volume and visibility of data breaches, particularly for large corporations. The next data breach or corporate hack isn't a questions of *if* but *when.*

Just a few months ago, it was announced that in 2014, Yahoo! fell victim to the biggest data breach in history, losing nearly 500 million accounts' worth of personal user data to attackers. Security must become top of mind for today's businesses, especially given the fact that the overall landscape has become much more complex and difficult to manage.

To start – and this should come as no surprise – the growth of hybrid IT has exacerbated security vulnerabilities. While it's important to realize that infrastructure and/or data location matters much less than accessibility (in fact, anything that can be externally accessed is equally likely to be attacked), the expansion of IT beyond the traditional four walls of the data center and into the cloud has opened an entirely new can of worms for security policies and procedures.

In simpler times, IT professionals were comforted by the knowledge that their data was on servers securely locked away in the data center, able to be rendered inaccessible simply by cutting the power.

Now that data is hosted in the cloud, and although most public cloud providers have strong SLAs that are compliant with stringent policies, including HIPAA, PCI DSS, FEDRAMP, SOX, and many others, the shift to the cloud has added another layer of security and monitoring complexity.

There is also a significant skills gap to contend with, as the convergence of IT roles brought on by hybrid IT and trends like DevOps have resulted in a dearth of security experts.

More often than not, security, rather than being treated as its own data center discipline, is considered an afterthought. Not only do today's IT professionals increasingly need to know a little of everything across networks, systems, and the cloud, they are also being tasked with managing their organization's security measures.

Unfortunately, security is very fluid, ever-changing and demands constant attention. IT professionals who already wear several hats are often not adequately equipped to successfully defend their business from attacks.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Similarly, administrators who have traditionally worked in silos of expertise (SysAdmins, NetAdmins, VirtAdmins, DBAs) typically will not have enough knowledge about the interconnected nature of their infrastructure to proactively identify security holes and vulnerabilities.

This lack of available security experts, coupled with the rise in data hacks and ransomware attacks, has given rise to an alarming trend that will continue to proliferate in 2017: businesses now feel compelled to weigh the implications of potential data loss against the expense of hiring security experts.

In many cases, businesses in the next year will choose to take a calculated risk regarding what they can "afford to lose" rather than what it costs to prevent data loss entirely.

So, as the industry looks to prepare itself for the year ahead, I'd like to share a few systems security essentials that today's IT professionals can implement to further defend their data centers:

1. **Invest in compliance software.** This is the best way to maintain accountability. Integrating compliance software such as security information and event management (SIEM) into an environment allows IT professionals to ensure that vulnerabilities are being taken care of by leveraging an easy interface within which one can handle things like patches and log event management.

   This type of software acts as a safety net of sorts, proactively monitoring for security vulnerabilities and configuration problems and alerting when an issue needs to be addressed.

   It's especially useful for organizations without a formal security team or process, and that are particularly susceptible to low-hanging vulnerabilities like late patches, leaving things at default settings or not requiring regular username and password updates from their end-users.

2. **Create a security team.** Attackers have automated network searches in place to find things to breach and steal, and as a result, IT professionals must be more vigilant than ever when monitoring applications with the most sensitive, and therefore valuable, information.

   Even if a complete team of security experts isn't feasible, organizations should at least look to create a basic level security team that can work together to create a security framework and evaluate it on an ongoing basis to best prevent attacks.

   Remember: the security landscape is constantly changing. This should not be a "set it and forget it" plan. Rather, it should be reassessed every six to nine months to ensure

Copyright © Cyber Defense Magazine, All rights reserved worldwide

everything is up to date and as effective as possible. In many cases, I've evaluated a company's security process and found that policies were set up as much as two years prior without any thought to updating it.

Once a team is in place, originations should plan to leverage a comprehensive monitoring toolset that can outline a baseline of performance across systems, networks, and especially databases, which are particularly vulnerable to attacks.

Having a fundamental understanding of what typical performance looks like for these pieces of infrastructure will normalize the security expertise of a team by providing a reference point to check when something seems wrong.

The security team can then execute on a pre-determined response plan in order to quickly and effectively remediate.

3. **Look to free resources.** These days, there is no limit to the amount of free and readily available resources one can leverage. The National Vulnerability Database and the Common Vulnerabilities and Exposure (CVE) database, for example, provide real-time updates on current and potential future security threats, their corresponding level of seriousness and suggestions for remediation that IT professionals can use to inform the updates and patches they roll out.

   No one wants to be vulnerable due to Security 101 mistakes, such as allowing users to keep default settings and passwords, which leaves the door open to much more serious breaches.

   Ultimately, IT departments should take advantage of these resources to stay on top of security trends and leverage their alerting features to best maintain their organization's security and address any vulnerabilities immediately.

4. **Save end-users from themselves.** End-user education is a sorely underutilized method of further securing an organization's data.

   The numbers consistently show that a majority of attacks actually originate inside the organization, often stemming from things like an employee falling victim to a phishing scheme that introduces malware on the network, DDoS attacks, or accidental end-user errors that stem from an inadequate understanding of potential security threats.

   Of course, end-users don't want or mean to cause problems, they just don't always understand what they're doing and how one action today can cause trouble tomorrow, the next day, or even a month from now.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

At the end of the day, organizations are only as strong and secure as their weakest link.

As more and more end-user devices get added to the network through workplace trends like BYOD, BYOA, and IoT, it's in every company's best interest to properly educate their end-users about the impact new devices like wearables or personal devices (tablets, eReaders, etc.) connected to the corporate network can have on overall security.

The organization's IT department should be proactive and transparent about flagging security vulnerabilities that could be exacerbated by end-user activities, such as using company email on a smartphone OS that requires a security patch, or accessing a social media profile with a password that may have been part of a larger breach.

Without a doubt, security and compliance standards are becoming an even greater concern thanks to the rapid growth of hybrid IT, IoT, the integration of more personal devices in the workplace, and a general lack of security experts.

By implementing these four essential best practices (and leveraging all available resources), IT departments can do better at ensuring systems security is top of mind, and be well on their way to developing a reliable security process that will protect against the expected rise in ransomware and other cyberattacks in 2017.

About the Author

Destiny Bertucci is a Head Geek at SolarWinds®, and is a Cisco® Certified Network Associate (CCNA), CIW Masters, INFOSEC, MCITP SQL and SolarWinds Certified Professional. Her 15 years of network management experience spans healthcare and application engineering, including over nine years as SolarWinds Senior Application Engineer.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Practical Guide: How to Prevent Insider Threat

by Dennis Turpitka, Practical Guide How to Prevent Insider Threat, Ekransystem (https://www.ekransystem.com/en)

Nowadays, everybody is aware of the danger of internal threats to information security. Several times a year we hear news reports about a new high profile data breach caused by malicious insider. The most recent example that comes to mind is the Washington State Health Care Authority (HCA) breach from February 9, 2016, when the data of more than 90 000 patients was misused by an employee.

Most of these reports are coming from government institutions, however this does not mean that private companies are not susceptible to malicious threat coming from within. In fact, insider attacks are something that businesses all over the world experience every day, but many of them choose to not publicize such attacks if at all possible, since it can easily damage their reputation and lead to a loss of clients and investors.

Insider attack in itself is an umbrella term that covers many types of malicious actions, from a completely intentional data theft or fraud committed for profit, to sabotage for making a point or getting back at a company, to industrial espionage, to even honest inadvertent mistakes. The thing that all of these actions have in common is the fact that they all are committed by employees with legitimate access to inner workings of you company. Often said employees are managers, database operators, programmers or IT specialist, working with sensitive data, infrastructure or critical system settings.

Effectively dealing with such a variety of threats from within the organization is a complex and layered process that requires commitment on the part of the company. Using the right internal threat management software will lend you some results, but for truly preventing and detecting insider threats, your very approach to employee management should be designed in a specific manner.

Making sense of all the tips and recommendations for dealing with insider threats can be hard and time consuming. This is why we took all the best practices and distilled them to six large, yet necessary steps that we combined into this practical guide How to Detect Insider Threats. By following these six steps and incorporating them into your company IT security, you will be able to effectively prevent insider threats and will have all the necessary measures in place for an efficient detection and response to a potential insider attack.

Step 1. Understand insider threats

In order to make your security truly effective, you need to first understand the nature of insider threat and what different types of them exist. Internal threats to information security are coming from insiders that are usually defined as people, who have legitimate access to restricted information and critical infrastructure of your company.

There are three main groups that can be classified as insiders:

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- **Current employees –** first group that comes to mind, your current employees have legitimate immediate access to all your sensitive data. The biggest danger among them pose users with privileged accounts. Such users have the highest level of access and usually enjoy a high level of trust from the company, putting them in the best position to commit malicious actions and get away with it.
- **Third parties** – modern companies are usually affiliated with a wide range of different people and organizations. Subcontractors, service providers and business partners all have access to your corporate network and sensitive data that they can use to conduct malicious actions.
- **Former employees –** while technically they lose their legitimate access upon termination, not all companies bother to properly delete inactive credentials. If former employee finds that their credentials are still working, they can use them to conduct malicious actions. Another potential danger is a backdoor or a logic bomb (malicious software that fires off automatically after a set period of time) that former employee may leave behind in order to gain access to the system or sabotage normal business operations long after they leave.

It is also important to understand the common reasons for committing insider attacks. In some cases, changes to employee behavior can give your security personnel some hints as to what they are planning and will allow them to prevent insider attack before the damage was done.

- **Corporate espionage –** employees can be recruited by a competing company via blackmail or bribery in order to transfer your sensitive data to them. Instances of corporate espionage can be very hard to detect. If employee makes many unexpected trips or suddenly has an influx of money, it may be a time to worry.
- **Personal financial gain –** employee can steal client database to sell it on a black market or start a competing business. In this case, they will often brag to their colleagues about this, which can help prevent the attack.
- **Revenge for perceived injustice –** disgruntled employees can conduct malicious actions to get back at the company for perceived injustice toward them. Malicious actions out of revenge are often designed to bring as much damage to the company as possible and to interrupt regular business procedures.
- **Inadvertent mistakes –** in many cases, insider attack turns out to be a simple mistake on the part of an employee, whether it is to click on a link in a suspicious email opening your company to a hacker attack, tell their password to a colleague, or to send sensitive data to the wrong person. Possibility of such unintentional threats should be accounted for and their prevention should be included as a part of a general insider attack prevention strategy of your company.

Understanding the nature of insider attacks is an important step that will help you conduct a more thorough risk assessment and define main weaknesses of your security.

Step 2. Employ secure approach for managing employees and credentials

You should organize your work process and assign credentials in such a way as to limit the

Copyright © Cyber Defense Magazine, All rights reserved worldwide

number of privileged accounts, restrict access to sensitive information as much as possible and create an unfavorable working environment for malicious actions.

In order to achieve this, there are two major principles that you should follow:

- **Principle of least privilege** – each new account by default should be created with the lowest level of privileges possible. The level of privileges should only be raised if it is necessary. This way you limit the number of privileged accounts inside your organization and make sure that all of them have specific purpose and are constantly in use.
- **Principle of separation of duty** – duties inside the organization should be divided between individuals as much as possible, promoting collaboration whenever a complex task needs to be solved. Statistically, employees are much less likely to conduct malicious actions when they are collaborating with other employees. For example, actions, such as backup and restoration of data should be separated between different people if possible.

The two aforementioned principles work together to minimize opportunities for insider attacks and strengthen overall data security posture of your organization.

Step 3. Conduct thorough risk assessment

Risk assessment is the necessary process that allows to identify all the weak points in your current security and give you a clear understanding of what needs to be improved.

There are three major steps to risk assessment:

- Identifying a potential threat
- Identifying how vulnerable your organization is to this threat
- Identifying how much damage would be done in case of this type of an attack

Received information will give you a clear understanding of what security measures should be implemented and how their implementation should be prioritized.

Risk assessment should be conducted periodically as well as anytime when a major changes to security or network infrastructure are introduced. Insider threats should be examined as an integral part of your risk assessment process. As a result, you should get a clear understanding of the effectiveness of your insider threat prevention and protection measures and how to strengthen them accordingly.

Overall, results of a thorough risk assessment should be used to build and revise general company security strategy, including protection from both insider and outsider threats.

Step 4. Work on employee security awareness

In many cases, security breaches are directly caused by employees neglecting simplest security rules and practices. Such neglect more often than not comes from the fact that majority of employees are poorly educated in the matters of cyber security. Employees are often either completely unaware of certain security practices, or are willingly breaking them in favor of their

Copyright © Cyber Defense Magazine, All rights reserved worldwide

own convenience, without realizing the severity of consequences that can follow.

The only way to remedy this situation is to conduct security awareness training in order to familiarize your employees with the latest security trend and make them aware of how they affect the cyber security of your company. This will help to significantly reduce the number of mistakes made by employees (since if they are aware of the severe consequences of their actions, it will prompt them to be more careful) and protect them from social engineering. They will know to not only ignore the links in spam emails, but also to report a fellow co-worker, who asks for a password from their account, or brags that he plans to start a competing business.

Also by making your employees aware of the security measures you are taking against insider threats, you are enlisting them on your side, creating a healthy working environment based on trust and deterring some of them from conducting malicious actions.

Step 5. Employ secure password and account management procedures

Using shared or default accounts is a prevalent practice in many organizations. However, this may allow certain employees to obtain access to privileged accounts that they do not supposed to have. Prohibiting use of shared accounts is necessary for reliable security.

You should also make sure that your accounts are thoroughly secured by unique complex passwords that are changed on a regular basis. It is also necessary to immediately change any default passwords that your company may use for any software or hardware. Such passwords are usually public and will allow both hackers and malicious insiders to easily take control of the system. Another important thing to do is to prohibit password sharing between employees, as well as the use of a single password across multiple accounts. This way you are not only making it harder for malicious user to get their hands on credentials of other employees, but also are thoroughly protecting your data from cyber security attacks by outsiders.

Another way to strengthen your account security and make sure that account is used by a correct person is to implement a secondary authentication. Such system, implemented with either mobile devices or more sophisticated physical tokens can be used to reliably confirm the identity of the person trying to log in and serves as a safety net in case the password has been compromised.

Step 6. Conduct employee monitoring

Employee monitoring is a great prevention and detection tools that will help you effectively deter malicious insiders and ensure integrity of your sensitive data. Professional monitoring software will give you a full visibility into what users are doing, providing you with the ability to quickly detect insider attacks, establish a culprit and issue a timely response.

- **Monitor user actions.** Many companies limit themselves to access monitoring or built-in login capabilities of software and systems that they are using. However, in most cases this is not enough, as user will be able to easily disguise their malicious actions as a regular work and alter or disable most internal logs. It is best to conduct thorough user action monitoring using dedicated monitoring solutions. Such software will be thoroughly

Copyright © Cyber Defense Magazine, All rights reserved worldwide

protected from tampering and will be able to produce comprehensive record of user actions, allowing you to efficiently detect insider attacks.

- **Monitor privileged users.** Users with privileged accounts are usually directly working with sensitive data or critical system settings and have all the tools necessary to conduct malicious actions, while disabling any default monitoring. It is important to use monitoring software that are specifically designed to handle such users and cannot be disabled regardless of the level of privilege user has.
- **Monitor third parties and remote users.** Various third parties, such as service providers and subcontractors are not necessarily have the same level of security from both insider and outsider threats as your organization. In this case, action monitoring is your best bet at reliably protecting your data from any misuse. When sensitive data is accessed remotely, whether by third parties, or by your own employees, make sure that it is transferred only while encrypted and that all remote sessions are fully monitored. This will allow you to prevent insider network attacks and make sure that remote employees are not misusing sensitive data.
- **Use custom alerts or behavior analysis tools**. One of the biggest challenges of action monitoring is the efficient processing of a large amounts of data you receive. More affordable monitoring solutions, such as Ekran System, usually employ customizable alert systems that can be used to create alerts best suited for your particular situation. Such alerts will fire upon particular suspicious events, allowing your security personnel to check for data breaches or misuse. Some solutions use more sophisticated behavior analysis systems that try to detect suspicious events automatically. Such systems are convenient to use and can give good results, although they are much more expensive and tend to produce many false positives.

Conclusion

When creating this practical guide on how to prevent insider threats, we went through many recommendations and best practices employed by security professionals, as well applied our own experience in the matter. Resulting six steps are the basic, yet the most important ones you can take in order to thoroughly protect your company from insider threats. We hope that this guide was useful to you and gave you a good idea on how to improve security posture of your organization.

About The Author

Dennis Turpitka is the CEO of Ekransystem, an expert within Digital Security solution business design and development, Virtualization and Cloud Computing R&D projects, establishment and management of Software Research direction. Successful entrepreneur, who organized several security start-ups. Dennis can be reached online at @Dturpitka and at our company website https://www.ekransystem.com/en

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CyberSense 2016

The Cyber Defense & Network Security Summit

28th-29th November, 2016 | Crowne Plaza, Muscat, Oman

CYBER-CRIMES HAVE EVOLVED.

HAVE YOU?

Explore the latest in cyber security at www.cybersenseworld.com

info@umsconferences.com

CyberSense World

Early Bird Discount – Use promocode **CSW20**

Official Supporting Partners:

سلطنة عمان
هيئة تقنية المعلومات
Sultanate of Oman
Information Technology Authority

عمان الرقمية
e.oman

المركز الوطني للسلامة المعلوماتية
Oman National CERT

Media Sponsor: Bloomberg Businessweek Middle East

Media Partners: CDM, DIGITAL FORENSICS Magazine

Organised By: ums conferences

Wi-Fi Security Worries and the Critical Nature of Classification

By Ryan Orsi, Director of Strategic Alliances at WatchGuard Technologies

Open public Wi-Fi hotspots are experiencing explosive growth. According to Cisco's latest Visual Networking Index Forcast, by 2020, public Wi-Fi hotspots will reach 432 million – nearly seven times the total in 2015. To most, this figure wouldn't come as a shock. You'd be hard pressed to find an airport, store, hotel, gym or coffee shop in business today that doesn't provide public Wi-Fi. The rise of connected or "Internet of Things" (IoT) devices and cellular offloading onto Wi-Fi as a method of easing capacity demands are a few strong drivers of this growth. The ubiquitous nature of wireless connectivity itself has resulted in seeding Wi-Fi radios into almost everything around us: smartphones, laptops, tablets, watches, TVs and even cars. In fact, Gartner estimates that 26 billion IoT devices will be connected by the year 2020.

It's safe to say that the widespread proliferation of Wi-Fi hotspots and connected devices makes our lives easier. But as convenient as anytime access to Wi-Fi may be, when everything is connected to everything, there are very real security concerns to consider.

Understanding Wi-Fi Security Risks

In a world consisting of only your laptop and a Wi-Fi access point, you're perfectly safe checking your bank account balance over a public hotspot. The main security risk with public Wi-Fi is the risk of a third party diverting your Wi-Fi traffic either on its way to the internet or back to your client device. This strategy is called a man-in-the-middle (MitM) attack and has been well-known since the original release of Wi-Fi. A MitM attack allows malicious hackers to examine the wireless traffic, login credentials, credit card numbers or other personally identifiable information being used by people who are unknowingly connected to a rogue access point.

When you connect your smartphone, tablet, laptop, or even a smart watch to a public Wi-Fi hotspot, the name or SSID of that hotspot is typically automatically saved so that the next time you walk back into that same establishment, your device will conveniently re-connect on its own. But, once you leave that airport or coffee shop, your smart devices continue to send out probe requests in the air looking for the SSID of the hotspots on your "auto connect" list. A Karma attack is one that takes place when an attacker takes advantage of your device's automatic beaconing and attempts to use a spoofed SSID to connect you to a rogue access point under their control.

Bad actors are known to dwell in public Wi-Fi areas frequented by employees of investment banks, technology companies, and healthcare organizations in order to target them with a MitM attack. This is typically done by forcing the Wi-Fi clients off the legitimate access point broadcasting the hotspot SSID and pulling them onto the rogue access point that also is imitating the same hotspot SSID. The client connection disruption is minor and falls within the

Copyright © Cyber Defense Magazine, All rights reserved worldwide

realm of “must have been a Wi-Fi glitch” and the victim’s traffic is now unknowingly flowing through the MitM.

Impractical Wi-Fi Hotspot Security Advice

The wireless security threats discussed above have been talked about often throughout the past decade amongst the information security community. That being said, the advice on how to protect ourselves hasn’t really changed during that time and isn’t very practical for the world at large. Some common Wi-Fi security tips include:

1. Use a VPN client to encrypt your traffic over public hotspots
2. Check for the “lock” symbol in the web browser to verify the connection is HTTPS (S for secured and encrypted) when connected to public hotspots
3. Don’t use public hotspots

First, although technically sound, the VPN client advice isn’t practical for the droves of everyday public Wi-Fi users who probably aren’t familiar with that acronym and aren’t equipped for this kind of setup. Next, far as HTTPS goes, I’m confident that someday the masses will understand what it is and even how to verify SSL certificate authorities, but right now, this just isn’t a practical method of protecting the world of public Wi-Fi users. Additionally, at the time of this writing, there is at least one well-known method of easily bypassing HTTPS during a MitM attack. And lastly, simply advising the public to not use public Wi-Fi just sounds like giving up.

So naturally, a good portion of responsibility for the security of public Wi-Fi rests on the shoulders of businesses that provide it. Luckily, there are Wi-Fi security solutions that companies can use to provide quality Wi-Fi access for customers and users while making security a priority. First developed in the early 2000’s, Wireless Intrusion Prevention Systems (WIPS) are a common network security solution designed to control Wi-Fi radios and mitigate wireless attacks and rogue access points.

The Problem with WIPS

WIPS solutions were originally meant to defend airspace through detection, classification and prevention. WIPS “prevention” is a setting that, when enabled, shuts down attacks by sending standard IEEE 802.11 de-authentication packets to the rogue access point, telling it to disconnect from any connected clients and to any connected clients telling them to disconnect from the rogue access point.

But the full promise of WIPS hasn’t been realized in the mass Wi-Fi market because of one serious technical flaw: the method used to classify access points and clients as good or bad (authorized or rogue) is plagued with false positives and negatives. The result is that industry IT leaders, service providers and technologists often disable the “prevention” piece of WIPS for

Copyright © Cyber Defense Magazine, All rights reserved worldwide

fear of legal consequences in accidentally shutting down neighboring Wi-Fi networks which may conduct business critical operations such as hospitals or retail stores over Wi-Fi.

The Missing Piece: True Prevention Through Accurate WIPS Classification

Without complete confidence in their WIPS solution's ability to differentiate between genuinely rogue and neighboring devices or APs, businesses have to rely on manual verification and classification of each connection, which can be a less accurate and more time-intensive process. Essentially, without classification, WIPS can't actually prevent much at all.

While no solution can truly guarantee zero false positives and 100 percent accuracy of WIPS classification, there is an elegant new technique that stands apart from the rest. A very short rebroadcast packet from known good (authorized) access points or WIPS sensors is sent either across Ethernet cabling or over the air. Thankfully to the open standard of the IEEE 802.11 protocol, when another 802.11 access point or client device receives this packet, it will rebroadcast it over the air or across the Ethernet cabling.

This tiny packet can traverse within all areas of a network and get the digital fingerprint of everything it touches. The MAC address correlation and signature based methods are limited in that they are performing the detection outside the perimeter of the network meaning the whole wired and wireless network is more or less a black box.

Through this packet technique, the WIPS system can very accurately classify access points and clients and do so automatically with no manual intervention. This auto classification can allow IT administrators to confidently define prevention policies without the fear of accidentally shutting down neighboring Wi-Fi networks.

It's safe to say that Wi-Fi provides an incredible convenience and accessibility for businesses and end users. But along with those benefits come serious security challenges. Wireless attacks may not be all over the news, but they are often the initial touchpoint bad actors use to access credentials that enable them to pull off the massive data breaches that steal the headlines. True prevention is the best way to defend against Wi-Fi attacks, and it all starts with classification.

About the Author

Ryan Orsi - Director, Strategic Alliances at WatchGuard Technologies

A senior network security and wireless technology expert, Ryan has a diverse background including more than 10 years' experience in business development, sales and marketing. He holds a high distinction Electrical Engineering Degree from the university of Nevada, Reno, as well as a Master's Degree in Business Administration.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

How to Defend Against the Next DDoS Attack

Cricket Liu, Chief DNS Architect at Infoblox

I'm sure you've been following the news the recent distributed denial of service (DDoS) attack against Dyn. Here's my take on what happened and what we need to do to survive the next big one.

The Dyn attack is a wake-up call to the world – not just to DNS providers, but to all parties involved, including the DNS community, Internet of Things (IoT) device manufacturers, businesses and consumers.

The sheer volume of traffic involved and huge number of web sites affected may make the Dyn attack seem overwhelming, but the truth is, by following some simple best practices, we can not only survive attacks like this, but also reduce their size and scope.

Get back to the basics: 3 best practices

1. **Build in redundancy.** Many companies rely on a single DNS provider like Dyn, leaving them vulnerable to attacks. Instead, businesses need to either deploy some on-premises appliances that can serve as external authoritative name servers – the servers that advertise their DNS data to the Internet – or bring in a second DNS provider. This is no different from ensuring that your company has redundant connections to the Internet.

   If one set of name servers goes down or is attacked, companies will still have name servers available. Making the external DNS infrastructure more heterogeneous ensures that companies are not putting all of their eggs in one basket.

2. **Mix it up, manufacturers.** IoT devices are here to stay, from cameras to thermostats to fitness trackers. And traffic from IoT devices will continue to grow. But many IoT devices are inherently insecure from the get-go. Why? Many manufacturers sell these devices with the same default administrator password, which consumers rarely change. Or even if they want to change it, sometimes they can't figure out how to do it.

   Either way, attackers have access to a vast network of devices from which to launch DDoS attacks. Simply put, IoT devices cannot be sold to consumers without some basic security measures, starting with unique, randomly generated passwords for each device.

3. **Lock it down, consumers.** In general, we have a terrible track record when it comes to protecting our information with passwords. The majority of passwords

Copyright © Cyber Defense Magazine, All rights reserved worldwide

consumers use are easily guessable. We have to try harder. The same goes with Internet-connected devices. Consumers must be savvier about changing the default passwords on everything including cameras, DVRs, routers and printers.

And, device manufacturers, in addition to providing each device with a unique preset password, must prompt consumers to create more sophisticated passwords and make it more intuitive for people to be able to do it.

Finally, an attack should be a reminder to consumers to check the security of their devices: to make sure passwords aren't easily guessable, and that devices have been upgraded recently to versions of code without known vulnerabilities.

Take action now

Gartner projects there will be 26 *billion* IoT devices installed by 2020. That's more than three devices for every person on the planet. A survey Infoblox conducted of 400 IT executives revealed that although 75% of businesses already have Internet-connected equipment on their networks, 35% say they're not ready to support IoT yet.

Even more eye-opening is that we found that nearly 60% of IT professionals say they're not doing anything to prepare for the impact of IoT. Do we really want to be ruled by toaster and refrigerator overlords?

The IoT threat isn't even the future – it's already happening, as demonstrated by the Dyn attack. Implementing best practices for IoT device security must be a top priority for all of us.

About the Author

Cricket Liu is one of the world's leading experts on the Domain Name System (DNS), and serves as the liaison between Infoblox and the DNS community. Before joining Infoblox, he founded an Internet consulting and training company, Acme Byte & Wire, after running the hp.com domain at Hewlett-Packard.

Cricket is a prolific speaker and author, having written a number of books including "DNS and BIND," one of the most widely used references in the field, now in its fifth edition. He is the owner/inventor of 10 DNS/IP address management patents within the U.S.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBER IQ Proudly presents

CDANS

CYBER DEFENCE & NETWORK SECURITY

Pre-conference workshop: 24th January 2017 | **Main Conference Dates:** 25th – 26th January 2017

Prospero House, London, UK

Improving national resilience to cyber threats

- **150+** Attendees
- **20+** Senior Cyber Security Speakers
- **14+** Hours Reserved For Networking
- **Insight** from across government, law enforcement and military

> ***The CDANS event was valuable as I was able to meet several key personnel that face the very same problems as I do, their experience is a great reach back. The topics were all interesting and valued the discussions***
>
> Branch Chief, DoD

Register online at www.cdans.org

Key Speakers for 2017 include:

Major General Jim Hockenhull
DCI3
UK MoD

Don Davidson
Deputy Director, CS Implementation & Acquisition Integration
Chief, CS Lifecycle Risk Management
DoD CIO's Office

Sherill Nicely
CISO
CIA

Deborah Petterson
Head of Energy Cyber Security, Department of Business
Energy & Industrial Strategy

Philip Quade
Chief of Cyber Task Force
NSA

Staying on Course in The Aftermath of a Security Breach

Fortunato Guarino, Solution Consultant, EMEA and Cybercrime & Data Protection Advisor, Guidance Software

It's the news that every security team fears, yet, the fact is that any business can – and will – be the victim of a data breach at some point, many more than once.

This is a particular concern for businesses in the Middle East – according to a March 2016 report by PwC , 85% of respondents to the survey believe that businesses in the Middle East are more likely to suffer from a cyber-attack compared to the rest of the world (global average of 79%).

Worse still are the monetary losses, with 56% of Middle East respondents reporting losses greater than $500,000 compared to 33% globally.

Despite this reality, there is little guidance available for most companies on what to do in the immediate aftermath of a breach.

Critical decisions need to be made immediately after a breach is discovered to assess its scale and scope.

This will determine the most effective next course of action, from which resources to mobilize, to which chains of command need to be activated and what evidence needs to be collected.

When, what and how to share information with law enforcement and other external authorities is also critical to help prevent further damage and help reduce future attacks.

With preparation in advance, organisations can ensure that, when the worst happens, they can respond quickly to protect themselves, their customers and their stakeholders.

Implement a Tested Incident Response

Being adequately prepared to deal with a cyberattack can significantly reduce the cost of a breach. However, having a plan in place and testing that response process to ensure that it works, are two different things.

That's why a critical part of the preparation process is to stress test the robustness of the response process.

Many organisations may think that they have sound policies in place but have not drilled these in a test scenario. The processes - for knowing which systems to shut down or who owns which assets and processes - need to be mapped and thoroughly practiced.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

In the pressure of a real incident, confusion can waste valuable time, so test the plan, review it regularly, and test it again.

The starting point after an attack is determining the extent of the damage, the type of data that has been targeted and any specific endpoints affected.

The scene of the digital crime then needs to be preserved correctly: any system or device which has been impacted should be swiftly identified, with forensic images made as soon as possible.

Without this, any forensic investigations can be seriously impeded.

These digital forensics provide the information needed to identify the risks, determine the next course of action and then take steps to prevent it from happening again.

Organisations should collect any relevant network logs, suspect communications and files. To maintain authenticity and a chain of custody, access to any preserved materials should be restricted to prevent any compromise of evidence.

Preserving digital evidence can also assist law enforcement agencies to identify and prosecute the perpetrators.

Prevent Additional Damage

In the immediate aftermath, organisations need to take steps to prevent further exfiltration of data; intrusions often continue past the initial detection. If data is found to be leaking from the network, steps need to be taken to close it down quickly.

Depending on the types of attack, they may need to re-route network traffic or isolate parts of the compromised network to prevent further damage. Any systems suspected of being compromised should not be used to communicate information about an incident.

Keeping a detailed record of response activities is important in both recovery and further threat prevention. The incident response team should keep information on the systems, services and data affected by the incident, and any changes made to systems and devices during the incident response.

Working with the Police and Crime Agencies

In many instances, there is a reluctance for organisations to share information with law enforcement agencies, often for fear of reputational issues at stake in disclosing security incidents.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

However, reporting an incident to the police can often provide insights into an attack that minimises further harm. Law enforcement has a significant role to play which goes beyond the remit of private organisations; they can gather evidence, prosecute and bring down cybercrime infrastructures, recover stolen data, and cut off their revenue streams.

This is the most effective way of policing cybercrime; we need to get better at reporting crimes and pooling information. It is this collective intelligence that can build a more accurate picture of the nature and scope of threats, its long term impact and how to allocate resources most effectively.

The bottom line is that we can't predict when or where the next incident will occur and as such, the 'assumption of compromise' now must inform key decisions on how security resources are allocated.

What every organisation can do is take control of the processes to minimise damage, preserve digital evidence and aid quick recover.

With improved information sharing, the industry, as a whole, stands to benefit in identifying and closing down crime syndicates.

About the Author:

Fortunato Guarino joined Guidance Software in June 2016 as a solution consultant and cybercrime & data protection advisor for the EMEA Region. Prior to joining Guidance, Fortunato spent more than 18 years working in IT with a focus on Cyber Security (IAM, DLP, DRM, PKI), Computer Forensics solutions, Corporate Counterintelligence, Cybercrime fighting, Compliance and legal obligations, including retention delay, BCR, cross-border ESI data transfers, track and management of ESI legal holds process, and foreign (China) joint-ventures agreements in regard with forensics & IT security management. In his previous positions, Fortunato served in a variety of roles, including CISO, Head of Cyber Security Business Unit, eDiscovery Officer and IT Court Expert.

He has strong experience managing EC, NAO, SAO and Asian regulations regarding privacy and discovery, and is an expert in corporate WW security policies management, security for intellectual property protection & IT forensic services support for legal, compliance, internal auditing and human resources.

Fortunato holds post graduate degrees in IT from Jussieu University of Paris, politics from the Sorbonne University of Paris, as well as a Master's Degree in Economics, also from the Sorbonne.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

How to protect an enterprise from physical attacks

By Yana Yelina, Tech Journalist, EffectiveSoft

Nowadays, none of the enterprises is immune to cyberattacks, data breaches, malware, and other types of damage. As a result, news about information leakage in different types of organizations is continuously cropping up in the mass media.

Taking into account the fact that cyberattacks are becoming more sophisticated, enterprises tend to spend much money on employing high-quality software or linguistic tools to protect corporate info, clients' personal data, intellectual property, etc. Thus, according to one survey, in 2015, about 20% of worldwide companies allocated a cybersecurity budget at the amount of $1-4.9 million. Beyond that, the cybersecurity market is expected to reach $170 billion by 2020.

Nevertheless, cyber security is not the only problem organizations should handle to avoid considerable losses from insider and outside threats…

Physical security

This type of security entails the protection of personnel, hardware, software, networks, and data from physical actions that are sometimes taken with brute force.

Physical security is often a second thought when it comes to information security and it is overlooked as organizations concentrate their efforts on combating cyber criminals with the help of trusted software developers. But it's a must to remember that sensitive data may be easily stolen by outsiders and insiders from laptops, USB drives, tablets, flash drives, or smartphones. Malefactors can get an entry to secured areas through tailgating, hacking into access control smart cards or breaking in through doors.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

It may seem surprising, but the below listed examples show that ***insider*** threats are becoming really numerous and should be addressed in a proper way.

1) At a major US bank a contract janitor and two co-conspirators stole a number of customer accounts and personally identifiable information from hard-copy documents. The criminals then used the data to steal the identities of over 250 people: they opened credit cards, submitted online change-of-address requests and, as a result, the victims did not get bank notifications about fraudulent activities. That case cost the organization $200,000.

2) The UBS PainWebber incident shows that sometimes attackers don't set a goal to steal data, they just want to damage. The example is Roger Duronio who planted a "logic bomb" that disabled 2,000 servers around the country in UBS PaineWebber offices. As result, the company didn't manage to make trades for several weeks and then reported to spend $3.1 million to recuperate from the attacks.

3) An insider stole trade-secret drawings within his organization and sold them to a rival, inflicting a $100-million loss. However, after losing a lawsuit, the company that received the stolen documents was forced to declare bankruptcy.

Security and protection systems

One security professional is not able to cover the whole range of physical security, that's why it's reasonable to plan a separate security program and address the 3 important components: access control, surveillance, and training.

First, physical sites should be protected by fencing, locks, access control cards, biometric access control systems, and fire suppression systems. Second, the company locations should be monitored via surveillance cameras and different kinds of notification systems: physical intrusion detection systems (IDSs), alarm systems, closed-circuit television (CCTV), heat sensors and smoke detectors. Third, it's indispensable to raise awareness among the employees, delivering valuable info on disaster recovery policies, as well as on physical attacks prevention and response procedures.

Security management software

Like in case of cyberattacks and intellectual capital protection, here an ideal variant is the implementation of specific enterprise software to control and manage staff and guest access to specific areas in a given physical facility to avoid insecure attendance.

To maintain such a complete control, the software is to include certain subsystems and management tools:

1) Data Manager

The era of physical locks and keys has ended with no hope of a return. For now, electronic access cards that interact with intelligently controlled devices represent one of the most secure

Copyright © Cyber Defense Magazine, All rights reserved worldwide

building options. Such systems give business owners a high degree of control over physical facility attendance.

The embedded Data Manager tool can be used to track employees' electronic entries, assign card holders to certain user groups depending on the access area and time.

The tool also allows recording card holders' locations and shows at what time and at which door the user was granted or denied access. To prevent data loss in case of system failures, controllers should be synchronized with the central database.

2) Security Manager

Any type of interaction with the system should be also tracked. That's why it's vital to use a special tool to control card holders' actions: logins, addition records, different kinds of editing, deletion, and more.

3) Hardware Manager

To avoid damage caused by malefactors, it also seems logical to use a hardware management tool to configure diverse hardware, such as controllers, doors with door panels and door readers, etc. Such a tool allows running all the needed reports; it is easy to implement and integrate, that's why Hardware Manager can be effectively used by companies of all stripes and colors.

To fulfill its function of an insider and outside threats/attacks tracker and show all its possibilities (including reports delivery), the above-mentioned software has to be correctly integrated into the enterprise control system, as shown in this case study, and if needed to go through a proper customization process.

Conclusion:

The article touched slightly upon the problem of physical security enterprises constantly face. With the development of new sophisticated techniques, both cyber and physical attackers feel free to conduct illegal deceitful activities to pursue their own aims, that's why a response should be also refined and effective.

About The Author

Yana Yelina graduated from Minsk State Linguistic University with a bachelor's degree in Translation/Interpretation (English, Spanish, and Italian) and Public Relations. After that, she has worked as a copywriter/journalist for a number of Belarusian companies. At EffectiveSoft Yana holds a position of a Tech Journalist and writes about modern technologies, covering software development practices in a broad array of business domains: trading and finance, e-commerce, education, healthcare, logistics, etc. Yana can be reached online at contact@effectivesoft.com or http://www.effectivesoft.com. You can also connect with her on LinkedIn or Twitter.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

WHERE FINANCIAL CYBERSECURITY EXPERTS *CONNECT*

InfoSecurity CONNECT

March 6-8, 2017 • The Rancho Bernardo Inn, San Diego, CA

Private, One-To-One Meetings with *Very* Senior Level Cybersecurity Executives

See more info at www.infosecurityconnect.com

Threat intelligence collection in a developing world

By Milica D. Djekic

As it's known – threat intelligence collection is mainly increasing in developing countries. These countries could be a source of the real risks, threats and challenges which should be managed carefully. It's especially concerning to investors coming from a developed world to deal in such an environment for a reason of quite huge level of the risk to their business reputation and much more.

Through this article, we would talk about how threat intelligence being gathered in a developing world could be used by "the first line on defense" community to update some national strategies, plans and decisions. In other words, we would try to discuss how intelligence services could be used to prevent their countries for a cybercrime, organized crime or even terrorism.

Many businesses from the western countries would be outsourced or run into developing societies. The reasons to that decision could be somehow different, but the interest is the same – the investors believe they may make a good profit taking advantage over inexpensive and skillful workforce.

Practically, that would be the case in the past and such a strategy would demonstrate some results. New times bring new customs, so maybe we should think how to overcome some of today's obstacles.

For instance, the mass usage of computers with the internet connection worldwide would begin through '90s and such an occurrence would make us to think about the cybersecurity. Today – the world is dealing with nearly 3 billion internet connections and much more computing devices being stationary or mobile.

Also, many people would use their mobile phones to log onto some public networks. For such a reason, it's clear how the world has changed and why it's important to adapt to those changes.

For instance, this new time would bring many advantages and some disadvantages being reflected through the lack of a good cyber defense practice over the globe. Many western businesses would try to outsource their production, services or manufacturing into a developing world primarily being led with the intent to make a good profit.

They would use computers and their networks being exposed to the global web to exchange the electronic mails or some confidential information through their communications and correspondences. The trick is that those offices or companies are not isolated there.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

They would use the local internet, telecommunication connections, utility, electricity and many more infrastructural advantages offering them a suitable work process. Also, they would deal with the local suppliers and contractors which would produce many of those to them.

So commonly, the companies coming from a developed world would use a certain amount of cyber protection being aware of the consequences of hacker's attacks and the rest of intruder's activities.

On the other hand, the trouble is they would stay open to attacks coming from their suppliers or unreliable local internet providers.

Let's say that some local small business may be a supplier to some big western's company offering it some qualitative goods and services for a quite suitable price. Maybe, such a company would get set up some cyber defense infrastructure and deal with some sort of security procedures and policies at a work, but its small supplier would not pay any attention to a cybersecurity.

Those suppliers would so easily get a target to a skillful hacker's attack and the bad guys would obtain many confidential information about everyone including that successful western's business.

Following such a track – they so easily may come to the origin of the business being in that developed country, so they may sell some details on a black marketplace or eventually publish some information on the web making those small businesses collapse and that developed country's company getting a compromise to its reputation.

Also, we would mention that the local internet providers would not offer a top quality web service and so often many malware and the other malicious applications would get present with that region's web.

It's a usual case that every area worldwide would have their local malware developers who would share their efforts with the hacker's community, so quite frequently those pieces of code would stay undetected using some standard anti-malware software.

That's how many computers in the US and Europe could be infected and people would not recognize that, because their anti-malware database would not match such malicious software to any known malware being discovered until then.

For all of those reasons, it's important to raise awareness about these concerns worldwide. The developed countries would get an interest to invest into developing regions for a reason of taking advantage over their inexpensive and qualitative workforce, while poor countries would see that activity as a chance to create new employments and decline the level of poverty there.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

So, it's significant to understand that only the international collaboration getting everyone aware about the importance of cyber defense in a modern business could produce the good result to all.

Finally, we see this as a good approach to make better world dealing with the knowledge and education and not with the ideology and religion making it returns several decades back.

Practically, it's all about the security and a good risk management which could offer to everybody to live in a peace and make a progress through their lives.

So, as technology brought a progress to the entire human kind – it's clear that such advancement could unite us all in bringing the better future to the coming generations of people.

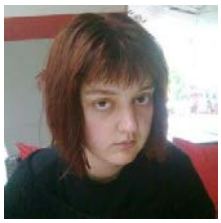
It's obvious that we would always cope with the changes and it's recommended to keep some of the good practice from the past and try to adapt it to the present times.

As theory of evolution would suggest – only being capable to survive through many times are not those being the strongest ones, but rather those being the most adaptive ones.

In conclusion, it's so important to deal quite intelligently in any situation and try to overcome your obstacle not going through it, but rather around it.

No matter how that stone got strong and you believe you can push it – you would just lose your time and energy, while an elegant walk next to it could take less time and energy being so necessary to get saved to the next obstacles.

About The Author



Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Securing the Hybrid Cloud: What Skills Do You Need?

Raj Samani, chief technology officer, EMEA, Intel Security Group

Hybrid cloud models offer many well-documented benefits, but they also introduce more complexity for securing data and applications across the enterprise. And this added complexity requires an increasingly diverse skill set for security teams. That's a challenge, considering the growing cybersecurity skills shortage. In one recent study, 46% of organizations said they have a "problematic shortage" of cybersecurity skills – up from 28% just a year ago. One-third of those respondents said their biggest gap was with cloud security specialists.

Modern security teams require a broad and deep mix of technology skills, ranging from twists on traditional network and OS technology all the way to security on data itself, to address a rapidly evolving threat landscape. But they also need "softer" expertise, such as knowledge of compliance regulations and vendor-management skills. Driving this dual focus is the public cloud's "shared responsibility model," in which service providers and enterprises divvy up various levels of protection across the IT stack. These responsibilities – and the requisite skills – vary depending on the type of public cloud service.

Security Skills

Certain skills are required across all uses of public cloud. For example, you'll need in-house expertise with encryption and data loss prevention controls for content-rich cloud applications. Your IT teams need to know (and track) where your enterprise data resides in the cloud, what offerings your cloud service providers offer for data protection, and most importantly, how to integrate data protection policies in the cloud with your own company policies. On a similar note, your team will need sophisticated identity and access management (IAM) and multifactor authentication, including tokenization, regardless of whether you're deploying SaaS, PaaS, IaaS, or a combination of those services.

For SaaS, your security teams needs to be familiar with the various applications in use and how to use logging and monitoring tools to detect security violations and alert appropriate IT staff. Post-incident analysis is a critically important skill for mitigating active threats and improving your security posture for future threats.

For PaaS deployments, you will also need to add skills to ensure that native cloud applications are being developed with security built in at the API level. Adoption of open security APIs can help to bridge the gaps among proprietary cloud environments.

For IaaS environments, the ability to provision software-defined infrastructure carries the need for highly technical security professionals who can create policies for server, storage, and network security on AWS or other platforms. These skills include the ability to monitor usage of compute, storage, networking, and database services, as well as the ability to manage security incidents identified in the cloud platform you're using.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Audit and Compliance Skills

Many of the softer skills needed for cloud success stem from the need for organizations to gain more visibility into hybrid environments that are becoming more complex as SaaS, PaaS, and IaaS services are cobbled together with each other and private clouds.

Audit rights can be built into a service level agreement (SLA) as a way to make sure the provider complies with corporate security policies and industry or government regulations. This is one reason why the ability to develop comprehensive SLAs with service providers is an increasingly important skill. IT and security teams will need to work together to negotiate terms that provide maximum protection and visibility into third-party services, to ensure that data, applications, and other components of your cloud environment are secure and compliant.

In addition to formal audits, security professionals require skills (and tools) for continuously monitoring compliance and threats across SaaS, PaaS, and IaaS deployments in two key areas: threats and applications. Starting with threats, achieving (or maintaining) visibility to specific threats across these environments so your organization has a full view of attacks is critical. That visibility needs to extend across endpoint, infrastructure, and network elements in order to recognize and respond to coordinated, multi-angle attacks.

Second, application security experience with cloud access security brokers (CASBs) will help security professionals increase the visibility into user behavior and their needs across public cloud service providers.

That said, we see convergence between the need for application visibility, threat visibility, and data security for SaaS applications, so look for skills that bridge those three areas as you build an organization for the future. The same need for a blended skill set will increasingly be true as threat and application needs converge.

Organizations in highly regulated industries also need to devote resources to tracking how third-party providers handle data and applications to ensure compliance with industry-specific regulations. The same goes for global players: Requirements around data storage can vary dramatically by country, requiring in-depth knowledge of local regulations regarding where data resides and how it is transmitted for any geography in which you do business.

Skills for Hybrid: the New Private Cloud

Security practices for a private cloud deployment – which enables enterprises to keep data and applications under their control – would seem to be more traditional than public deployments. But the virtualization technology that is inherent in the private cloud model creates a need for new security skills beyond those for traditional on-premise environments.

The first is understanding the difference in the infrastructure itself, for example between a traditional virtual machine and a framework like OpenStack. Second, as organizations explore software defined networking (SDN), they see a need for more automation skills, as security policy must co-exist with the orchestration to fully exploit an SDN environment. Third, the

Copyright © Cyber Defense Magazine, All rights reserved worldwide

security operations center will need more network insight as the east-west traffic becomes more material to threat analysis. These skills become especially important as virtualization expands beyond servers and into networks and storage.

That said, most private clouds are truly hybrid clouds – and these will be the default moving forward. Hybrid clouds demand cross-domain threat visibility, along with the skills across the various cloud types to prioritize and respond to them. This requires both a broader level of technical depth but also more cross-team facilitation and leadership to analyze and respond to critical threats. Revisiting the soft skills points made earlier, this also includes leadership not just within the organization but across the set of SaaS providers relevant to a given situation.

The Bottom Line on Cloud Skills

The takeaway for security leaders: It's time to optimize the skills of your team to the different types of cloud. Public cloud security – spanning SaaS, PaaS, and IaaS environments – is (a) more about policy, audit, analysis, and teamwork skills rather than pure technical depth, and (b) will include more cross-domain skills than are required in the more silo'd on-premise structure. Creating the proper mix of skillsets for all of these scenarios will help build your confidence as you build out your hybrid cloud model.

About the Author

Raj Samani is an active member of the Information Security industry, through involvement with numerous initiatives to improve the awareness and application of security in business and society. He is currently working as the EMEA Chief Technical Officer for Intel Security, having previously worked as the Chief Information Security Officer for a large public sector organisation in the UK. He was inducted into the Infosecurity Europe Hall of Fame (2012), won the Virus Bulletin Péter Ször Award for the paper/investigation he co-authored on the takedown of the Beebone Botnet, and was named in the UK's top 50 data leaders and influencers by Information Age.

He previously worked across numerous public sector organisations, in many cyber security and research orientated working groups across Europe. He is also the author of Syngress books 'Applied Cyber Security and the Smart Grid', "CSA Guide to Cloud Computing", and technical editor of "Industrial Network Security (vol2)" and "Cyber Security for decision makers".

In addition, Raj is currently the Cloud Security Alliance's Chief Innovation Officer and previously served as Vice President for Communications in the ISSA UK Chapter where he presided over the award of Chapter Communications Programme of the Year 2008 and 2009. He is also Special Advisor for the European CyberCrime Centre, also on the advisory council for the Infosecurity Europe show, Infosecurity Magazine, and expert on both searchsecurity.co.uk, and Infosec portal, and regular columnist on Help Net Security. He has had numerous security papers published, and regularly appears on television commenting on computer security issues.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Ransomware: Not Your Typical Threat

Lower Ransomware Risk with Education, Planning, and Relationship Building

by Jon Leer, Writer, Leer Technical Communications, LLC

Interviewed: John Galda, Director of Risk/Security at Charles River Development

© Valerijs Novickis

While security solutions continue to sprout up all over the globe promising firewalls of protection against barbarians at the gate, ransomware attacks increase against small and critical businesses. Rather than going for the big trophy enterprise, ransomware hackers use unsophisticated, easy to build malware to harvest the easy cash from their victims. Before the attack, the potential threat goes undetected by IT – there is no known signature. After the attack, local, state, and federal authorities have difficulty tracking the culprits.

What's So Unique about Ransomware?

What is it about ransomware that is making malware vendors scramble, small businesses cringe, and authorities close cases as "unresolved"?

Ransomware is an elusive threat from unknown and often unsophisticated entities. Its key attributes are:

- Attacks small businesses often with critical services (e.g., healthcare)
- Hard-to-detect because it has no known signature and is easily modified

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- Blackmails the victim by shutting down data access and promises a significant loss of business
- Demands a cash ransom to restore data access and prevent loss of data
- Leaves negligible fingerprints for identifying a signature with threat code left behind for analysis
- Remains under the radar of local, state, and federal authorities

John Galda, Director of Risk/Security at Charles River Development, notes that larger companies typically make large investments in sophisticated security solutions. When such a company is attacked, it is by a hacker who is a code expert and deploys a sophisticated malware package with severe intent, such as data theft (e.g., privacy and financial data) or chaos (DDoS).

Small companies typically do not have the resources to invest in such comprehensive security solutions. These companies are the "low hanging fruit". They are unprotected by limited IT resources, ignorant about cybersecurity best practices, and unable to detect and remediate threats unknown to their Anti-Virus software – a perfect recipient for ransomware.

© Clifford

> *"[consider] the planes of the Serengeti. The lion takes down a water buffalo and will eat well. If the lion were to turn to eating mice it would starve… We're not seeing the lions in ransomware. It's a lot of jackals and dogs who are going after the easy targets, buying other people's crimeware… Going after the low-hanging targets."*
> **John Galda**

Galda suggests that ransomware will continue to grow and elude the experts, focusing on smaller businesses and vulnerable enterprises (e.g., healthcare) where security controls may not be as diligently deployed and monitored, and employee security hygiene less than pristine.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Pain Points

Consider the difficulty of dealing with ransomware.

Limitations of Signature-Based Detection

John Galda adds, “The problem with current malware solutions is that they are signature-based.” Only when somebody is attacked and the malware code retrieved and analyzed does the signature become known and is finally added by security vendors to their updates.

Ransomware attackers are betting on being able to “harvest” the ransom before the ransomware count-down timer hits no time left (i.e., pay up or lose all your data).

Should I Pay the Ransom?

Apparently, many companies would rather pay the ransom than go through the lengthy data analysis and recovery. Another sore point is that the authorities and courts will probably never catch the bad guys. The malware might be retrievable, but identifying a signature may be fruitless since the malware can so easily be modified.

The common victim mindset during an attack is that “I need it now” and “I don’t want to pay the attacker.” But the time is running out before all data will be lost. And restoring the infected system is going to take a while. In the end, without any immediate response plan in place, the company may need to pay the attacker.

There are ways to reduce the risk of a successful ransomware attack. These include educating your employees, assessing your data assets associated risk, creating and practicing a recovery plan, and building better understanding with other management about common security risks and strategy.

Educate and Share Best Practices

At the SC Congress Boston, John Galda sat on the Ransomware panel, which noted the importance of in educating employees, partners, and customers about good security practices in non-technical terms to help mitigate not only threats from outside but also from within. Top suggestions include:

- Schedule on-going backups of critical data
- Share good security hygiene
- Set up strict change control and access
- Schedule application scanning
- Purchase cyber insurance
- Perform risk assessments

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- Train employees throughout the year (relationship building)
- Build better relationships within the C-suite (CIO/CSO) and board
- Build in redundancy
- Monitor programs and procedures for a culture of security
- Plan for the worst, and ensure there is a rational response plan in place and TEST IT – consider different scenarios
- Be careful what you say about your security to others
- Run desktop exercises to test dealing with an attack
- Test restoring data from backups
- Layer your security on email. John Galda adds, “Office 365 has a layer of security, but it may not be enough. You may need to add something stronger, such as adding a Baracuda solution.”

John Galda comments that ransomware is typically a reactive experience, so you want to be prepared. Essentially, you do not want to “have a flat tire, and discover that there is no tire in the trunk.” Because ransomware is “opportunistic” (you will not know what part of your data infrastructure is affected), you should create a heat map of where critical data is located and identify what needs to get backed up regularly. If an attack occurs, you know the critical data is already backed up no matter what data is affected by the ransomware.

Commit to Building Better Relationships

Ensuring a successful outcome following a ransomware attack depends on the commitment to being proactive. The key stakeholders are the employees, IT, and management. Management must be on the same page to devise a practical plan that can be implemented by the entire team.

CSOs and CISOs are recognizing that they need to bring the other executives in the C-suite into the security fold. This requires relationship-building skills. CSOs are usually looking over the horizon, and should be performing risk assessments on an annual basis. However, they also need to work in conjunction with the CISOs to strengthen their credibility with CFOs and CEOs so that they can share in the ownership of risk assessment and planning.

The bottom line is that the more educated the entire team is about cybersecurity, threats, and possible intrusions, the lower the risk of a successful attack.

Think Ahead of the Curve: Evil is as Evil Does

To go beyond relying on only known malware signatures, we need to think differently. John Galda notes that the new paradigm is to consider behavior-based activity which detects evil is as evil does. For example, you download something to your machine, and it is not recognized as the signature from known malware vendors and it starts “doing stuff”, such as doing an unpack and writing something to memory, port scanning, or making a copy. Ideally, the behavior

Copyright © Cyber Defense Magazine, All rights reserved worldwide

analysis software would detect “you aren’t supposed to do that”, and move the activity to a sandbox for further testing before allowing it into production.

However, looking at behavior is difficult, because what is evil? Unfortunately, log analytics alone cannot define and detect evil. We should look at both user and machine behavior for answers. Many malware vendors are now on this quest. For example, MalwareBytes Labs advanced threat research arm researches and investigates telemetry data from millions of installations, and offers an advanced behavior-based detection engine. John Galda predicts that approach will be a good end game for threat detection and remediation, but getting there will probably be painful

In Conclusion

We may not have a 100% failsafe solution for ransomware attacks, but you can greatly reduce the risk by educating your employees on security hygiene, religiously following best practices such as backing up and testing restores, and building better relationships amongst members of the C-suite for improved security and risk assessment and disaster recovery planning and execution. To extend automated solutions to further, we must embrace new technology that shortens the time to recognize bad behavior as threats, and isolate those components for successful remediation.

About The Author

Jonathan Leer, Director of Communication, of Leer Technical Communications, LLC. For the past 25+ years he has been providing technical and business writing services to small-to-large businesses. Several are in the security industry, including RSA and Bradford Networks. He has published articles for Entrepreneur, Workforce Management, Sales Management, and Training. Jon can be reached online at jleer@leertech.net and at http://www.leertech.net.

About the Subject Matter Expert

John Galda, Director of Risk/Security at Charles River Development. He is an expert in Risk Management, IT Governance, and Security Awareness, John has 30+ years of experience in information technology at Fortune 500 companies such as General Electric, Liberty Mutual, United Technologies, and Textron. John is a Certified Information Systems Security Professional (CISSP) from ISC2, Certified Information Security Manager (CISM) from ISACA and is also certified in ITL, LEAN Six Sigma and Project Management from George Washington University. He has a Bachelor's of Science in IT, done graduate work at Harvard, and has two Master degrees, the most recent an MBA from Boston University.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Who is afraid of the sea monsters?

By Rodrigo Ruiz

Abstract

From very young we are trained to fear the monsters Fig 1, the dark and the unknown. It is bringing an analogy of these children's fables that this work presents a counterpoint to DarkWeb. By exploring day-to-day aspects of users, security companies, large corporations and governments, this text is intended to demonstrate that the danger lies not in the abysmal depths. The cybernetic danger is too closer.

Fig 1 - Image by Pixabay

Pedophilia, murder, espionage, heinous crimes. In general, we have the feeling that all of this is always very far from us whether in the real world or in the cyber world. But no matter the distance, the sight of the abyss always terrifies us.

The symbiosis between fear and the security market is fed daily by some extreme cases of great repercussion and by the imagination of every ordinary citizen who has ever watched a chapter of C.S.I Las Vegas or C.S.I Cyber. These are stories that usually involve big criminals or government agencies.

The term Dark Web, undoubtedly is scary and causes chills in every type of user. I have to confess that I have already written about the danger of major global cyber attacks with the potential to paralyze an entire country right here at CDM (Rogerio Winter 2015). After attending the great Inside Dark Web event at The Army and Naval Club in Washington DC 11/2016 I considered it relevant to make those comments.

But something I learned in years of security research was that we should fear what is close to us, fear, respect, and take preventive action for all that is within our reach. People are afraid of flying, but this is the safest means of transportation in the world. These same people cross the street without looking to the side and when they are behind the wheel they cross the red light.

In this line of thought the care with the quality of software should be our biggest concern. In fact, as always says Colonel Rogerio Winter of the Brazilian Army, "worry is not tactical action". To take care of more of the basic routines of physical security and the correct handling of

Copyright © Cyber Defense Magazine, All rights reserved worldwide

passwords and credentials even in the use of encryption software (Ruiz and Winter 2016) and (Ruiz, Amatte and Park, Security Issue on Cloned TrueCrypt Containers and Backup Headers 2014).

In addition to being careful about credentials, it is essential that your company's users be warned not to act like ostriches. Usually people are induced to navigate privately or incognito. This type of functionality, besides not working as promised, causes the user to lower their guard and expose themselves even more than normal. No matter what operating system or browser, including TorBrowser, everything the user browses will be recorded on your computer (R. D. Ruiz, FP Amatte, et al., Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode 2015), (Ruiz, Amatte and Park, Making Public Navigation the "InPrivate" 2012) (Ruiz, Amatte and Park 2014).

Humans can lose their lives in a few centimeters of water in the same way that thousands of dollars can be lost due to basic security flaws allied to an overconfidence of developers.

Be safe. Ever!

References

Rogerio Winter, Rodrigo Ruiz. “Apoc@lypse: When the anti-malware is sick.” Cyber Defense Magazine - Cyber Warnings, 2015: 26-28.

Ruiz, Rodrigo de Souza, Fernando Pompeo Amatte, and Kil Jin Brandini Park. "Security Issue on Cloned TrueCrypt Containers and Backup Headers." The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014). Kuala Lumpur - Malaysia, 2014. 11-19.

Ruiz, Rodrigo de Souza, Fernando Pompeo Amatte, Kil Jin Brandini Park, and Rogério Winter. "Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode." International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4, no. 3 (2015): 404-416.

Ruiz, Rodrigo de S., Fernando Pompeo Amatte, and Kil Jin Brandini Park . "Opening the “Private Browsing” Data – Acquiring Evidence of Browsing Activities." Proceedings of the International Conference on Information Security and Cyber Forensics. Kuala Terengganu, Malaysia, 2014. 72 - 79.

Ruiz, Rodrigo de Souza, Fernando Pompeo Amatte, and Kil Jin Brandini Park. "Tornando Pública a Navegação “InPrivate”." Proceedings of the IcoFCS2012. Brasília - Brazil, 2012.

Ruiz, Rodrigo, e Rogério Winter. “Corrosive Secrecy and Confidence: the Paradox Among Bypassing Cryptographic Software, Loss of Provacy and Information Security.” Cyber Security Review, 03 2016: 66-74.

About the Author

Rodrigo Ruiz is researcher of CTI – Information Technology Center - Renato Archer, Campinas, Brazil, also he is a member of the SDIWC (The Society of Digital Information and Wireless Communications) have some papers about privacy and he is co-author of Apoc@lypse: The End of Antivirus and he is author of papers about privacy and security.

rodrigosruiz@outlook.com | https://www.researchgate.net/profile/Rodrigo_Ruiz3

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CYBER SECURITY EXCHANGE ASIA

27-29 November 2016 ■ Phuket, Thailand

DID YOU KNOW?

- **75bn USD** - is how much the worldwide **cyber security market** is currently worth and expected to **grow two fold** by 2020
- **$32.95bn USD** is how large the **Asian cyber security** market is expected to grow by 2019
- **$200bn USD** is the forecast for connected devices by 2020
- **$30bn USD** is the predicted growth for the **global managed security services market** by 2020

MAJOR TOPICS TO BE COVERED AT CYBER SECURITY EXCHANGE ASIA

1. **Detecting an attack**, how to and how not to address a data breach
2. **Discussion of the Asian regional** cyber security policy
3. **Ransomware** – best practice risk assessment, prevention and response
4. **The role of the Chief Risk Officer** in an organisation's cyber security strategy
5. **How to get the most out of your systems** using your staff
6. **Strategies for implementation** with the convergence of IT, OT and physical security

SOUNDS INTERESTING? WE WANT YOU!

Come be a part of **Cyber Security Exchange Asia 2016, 27-29th November 2016 in Phuket, Thailand**, as we bring together 45 CIOs, CISOs and Heads of Cyber Security from across Asia, to discuss the challenges faced. Visit **www.cybersecurityexchangeasia.com** to find out more information on this unique event.

If you would like to request an invitation to see if you qualify to attend this event, email **enquire@iqpcexchange.com** referencing code **CSCDM_Del**

OR

If you would like to have 30 minute pre-scheduled meetings, to offer your solutions to these CISOs and Head of Cyber Security, email **enquire@iqpcexchange.com** to find out what opportunities are available referencing **CSCDM_SX**

How a Cyber Attack Could Kill Your Website – Permanently

by Phillip Adcock, Managing Director, Shopping Behaviour Xplained Ltd

Shopping online has become the standard way to do things. But with many shoppers wary of online services, site owners should be aware that there are serious consequences for sites that have been hacked.

With it becoming easier and easier to have your identity stolen, shoppers are becoming hyper-cautious, with many people afraid to bank online due to security fears. In addition, Google has stiff penalties for hacked sites with consequences that can be hard to reverse.

Younger generations are the most likely to use online services, with 65% of millennials using their phones to shop online. As well as being more technologically savvy, they often work long hours. The convenience of not having to shop in-store and instead have products delivered is attractive, with many choosing to shop online over physical stores.

But as well as being quick to adopt online services, they are quick to jump ship if the site is having security issues, especially if the site has been hacked. This, in combination with Google's policy of delisting sites with security issues, means that you need to pay a lot of attention to your online security.

Loss of Customer Trust: The Short-Term Effects of a Hack or Data Breach

Hackers like to make their work obvious to the site owner and visitors, leaving a signature of some kind. And even when they don't, they often leave behind malicious code which is visible to Google.

If you are hacked, many customers will leave you out of fear for their own online privacy, whether their information was leaked or not. It's little wonder, as a hacked site is inherently unsafe. It may bombard your customers with ads or even steal their payment information. The recent hack of TalkTalk led to a loss of 101,000 customers.

But what happens in the long term after a breach?

The Long-Term Effects

You might think that once the malicious code is removed, your site can return to its former ranking and reliability. But it's more than likely that the hacking activity will have been noticed by search engines. Google is quick to penalise suspicious activity, with penalties including having

Copyright © Cyber Defense Magazine, All rights reserved worldwide

your site delisted from Google altogether. That may not sound too major an issue. However, most of the world uses Google as a search engine, with processing around 40,000 searches per second. It is likely that the majority of your traffic will be coming from there.

Penalties from Google are difficult to remove and your site's trust rating can take time to heal. In some cases, with a low-ranking site, it is better to start again with a new domain. This may sound drastic, but a website that no one can find is essentially useless.

Why Does Google Downgrade?

You might be wondering why Google downgrades sites if it has such a drastic effect on the sites that it hits. In short, Google has its own reputation to maintain. By delisting sites with spammy or negative behaviour, Google gives more reliable results and prevents users from visiting sites with malware. Google's search engine covers millions of sites, so rather than visiting each one manually, Google has software that detects suspicious activity. Telling the difference between a site that was hacked and then restored and a site owner with consistently suspicious behaviour is tricky, so Google errs on the side of caution.

What Can You Do to Protect Your Website?

The best way to protect yourself is to be prepared and to have up-to-date online security. Know who you need to contact in the event of a hack and move quickly. The smoothest way to restore your site is to keep previous versions of your site on-hand to replace it with, should there be any issues.

Like any business, you should also have a backup plan ready and waiting in case the worst happens and your site is delisted. For example, are you able to increase your social media following through giveaways or paid advertising? Or would you benefit from email marketing (perhaps offering vouchers to any customer who has been affected)? The key is restoring customer trust.

About the Author

My name is Phillip Adcock and I am the founder and Managing Director of Shopping Behaviour Xplained Ltd. We use psychological consumer insight and retail technology to explain and predict customer behaviour. SBXL operates in seventeen countries for hundreds of clients, including Mars, Tesco, and B&Q. Phillip can be reached online at info@sbxl.com or on Twitter @SBXplained, Facebook, LinkedIn, and our company website www.sbxl.com.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Enterprise Systems Security Assessment Challenges: What Mitigation Strategy Can Be Utilize?

By Dr. Daniel Osafo. Harrison, D.C.S., Security+.

Loghry and Veach (2009) stated that a risk assessment is "a qualitative measure of the potential for losses resulting from the occurrence of uncertain events in a specific period of time" (p. 31). This means that the organization must anticipate the challenges with loss that the company may have so that these areas can be fixed. Loghry and Veach suggested that any safety or security professional could conduct a risk assessment with some practice and a little research. A risk assessment will include logical thinking to the hazards or threats that the organization may go through on a daily basis.

Introduction

Organizations working with data and personal information from clients should be sure to assess their enterprise security on a regular basis. Risk assessment is one of the most important assessments an organization can do because it provides an organization with information about the security measures taken and whether these measures are protecting the company.

Clark (2014) stated that organizations should have a team of people who are available to do the risk assessment so that they concentrate on the entire organization instead of only on IT matters. This team should be assigned to only deal with risk management. The team should be responsible for bringing together all the people who will need to be involved with the risk assessment (Clark, 2014).

Clark (2014) identified several steps to take in doing an adequate risk assessment. Some of those steps include:

• Identify and map what is important – the organization must understand the different aspects of the security risks that are important. The organization must map out processes and how they are done to understand better those areas that may be at risk.

• Determine what could go wrong – the most difficult part of any assessment is to try and anticipate what the threats to the organization could be and how to stop them. The organization must look at the processes as though there were no controls in order to see where they are most vulnerable. Some things to look at are employee theft of data, unauthorized access and unauthorized changes in codes or unexpected data manipulation.

• Determine the likelihood of the threat happening and its impact – The organization must look at where they are most vulnerable and what would happen if the situation did occur. For example, they must decide whether the threat would impact them financially, loss of business,

Copyright © Cyber Defense Magazine, All rights reserved worldwide

loss of data or in other ways. Also, if threats have happened in the past, these must also be factored in because they provide more information to the organization.

• Evaluate the controls already in place – key controls and non-key controls should be observed and the organization should evaluate how these controls are currently working. Also, controls should be looked at as to whether they are needed or not.

Types of Security Assessments

Liu, Kuhn, and Rossman (2009) stated that there are two types of security assessments that include analysis and evaluation. In analysis, Scarfone (2012) stated that there are several types of reviews that an organization can do that include reviews of documentations, logs, ruleset and system configuration, network sniffing, and file integrity checks.

There are also target identification and analysis techniques and network assessments.

All of these assessments can be done by an organization over time. Atyam (2010) suggested that there are several stages within the security assessment process. All phases should be centered on identifying the various aspects of the business and understanding how each aspect of the process is functioning to prevent security risks.

Atyam also stated that assessment is the first step in determining whether security is working.

Who Should Be Involved

Radack (2012) stated that all people within an organization have role in the process of security assessment because managing risk s both comprehensive and complex and involves many different activities within the organization.

Radack suggested an integrated approach to security assessment because different individuals have valuable information to provide in the assessment. When the assessment should be done depends on the regulations set out by local, state or federal information.

Conclusion

There are many issues to take into consideration when creating a risk assessment. The organization must first analyze what they are going to look for and then evaluate the process. All employees within the organization should be a part of the process of evaluation and this evaluation can be done internally because the employees have a better understanding of the organization.

Assessments are done depending on the regulations from the local, state, or federal programs.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

References

Atyam, S. B. (2010). Effectiveness of security control risk assessments for enterprises: Assess on the business perspective of security risks. Information Security Journal: A Global Perspective, 19(6), 343-350. DOI:10.1080/19393555.2010.514892

Clark, J. (2014). Conducting a risk assessment: Key components you can't ignore. Fishnet Security. Retrieved from https://www.fishnetsecurity.com/6labs/resource-library/white-paper/conducting-risk-assessment-key-components-you-cant-ignore

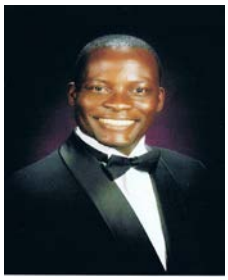
Liu, S., Kuhn, R., and Rossman, H. (2009). Understanding insecure IT: Practical risk assessment. IEEE Computer Society, 3(11), 57-59. DOI.ieeecomputersociety.org.contentproxy.phoenix.edu/10.1109/MITP.2009.62

Loghry, J. D., & Veach, C. B. (2009). Enterprise risk assessments: Holistic approach provides companywide perspective. Professional Safety, 54(2), 31-35. Retrieved from http://search.proquest.com/docview/200325280?accountid=458

Radack, S. (2012). Conducting information security-related risk assessments: Updated guidelines for comprehensive risk management programs. Itl Bulletin For October 2012. Retrieved from http://csrc.nist.gov/publications/nistbul/itlbul2012_10.pdf

Scarfone, K. (2012). Intro to information security testing and assessment. PowerPoint Presentation. NIST Special Publication 800-115. Retrieved from http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-6_kscarfone-rmetzer_security-testing-assessment.pdf

About The Author



Dr. Daniel Osafo. Harrison, D.C.S, Security+

Daniel is a Doctor of Computer Science in Information Assurance, Information Systems Security Officer (ISSO) for Industrial Control Systems at Bechtel Nuclear Security & Environment and a member of Cyber Security Team at Pueblo Chemical Agent-Destruction Pilot Plant for Department of the Army. He functioned across the enterprise as a technical liaison between governance and administration, regulatory compliance and implemented and managed cyber-security solutions.

Daniel can be reached at odharrison4@yahoo.com and at our company website http://www.bechtel.com/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Best Practices for Remote and Branch Office Data Protection

Gregg Petersen, Regional Director, Middle East and SAARC, Veeam Software

We've all heard about fantastic new data centre technologies, but all too often it looks like these technologies only seem to apply to the largest organizations with a wealth of centralized resources. Because data doesn't just live in the data centre, we often face daily challenges when data is put to use in the field at remote offices and branch offices (ROBOs).

Business and IT leaders need to recognize the unique needs of ROBOs. For instance, teams based in remote offices need constant, reliable and fast access to essential data, without sacrificing data security and integrity.

A challenge for IT leaders is how to ensure that data is available, even without a dedicated local IT team to govern and control it. The *2016 Veeam Availability Report* showed that half of the respondents only test backups on a monthly basis, or even less frequently.

Long gaps between testing increase the chance of issues being found when data needs to be recovered – at which point it may be too late for these organizations. And out of those who do perform such tests, just 26 percent test more than five percent of their backups. This means that the vast majority of backups are not verified and could fail. The percentage is even higher when it comes to ROBO locations.

The good news for ROBOs is that it's now easier than ever — with the help of the right solutions — to extend data centre backup, replication and Availability capabilities all the way out to the edges of an entire organization.

So, how can ROBOs achieve excellent levels of Availability *without* facing complexity?

The Modern Data Centre Extends to ROBOs

The modern data centre has three key attributes – it is highly virtualized, it uses modern storage solutions and has a cloud strategy in place.

Each of these attributes is critical to a ROBO's success. However, because of each ROBO's specific needs, there are no real roadmaps for building and implementing architecture for a remote office.

Virtualization has had a huge impact on ROBOs. From reduced equipment footprints and lower setup costs, to simpler management workloads and faster deployment of new services, virtualized environments have become the natural choice for ROBOs.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Modern storage systems have also made life a lot easier for ROBOs. Whether it's a new solution rolled out to serve every branch or a solution that's just deployed on site, new storage solutions are helping ROBOs store — and what is more important, backup and replicate — their data more intelligently.
The cloud is now a suitable option to move and store backup and replicated data, unlike the leased private lines that are often a significant performance bottleneck to perform this task.

Best Availability Practices for the Branch Office
Many organizations struggle to select the best solutions for on-site and off-site backup, because there really isn't a one-size-fits-all approach for remote office architecture.

Organizations often end up choosing between taking on-site backups, writing backups off-site or doing replicas both on and off-site — instead of considering how they could utilize them all.

There is the long-promoted 3-2-1 rule for Availability that can be the best solution in this situation. It states that there should be: **3** copies of important data, on **2** different media, with **1** off-site.

The 3-2-1 rule is highly versatile and can address just about any failure scenario imaginable by ensuring that all data is both backed up in multiple locations, and also quickly recoverable. This approach means that companies don't have to worry about getting locked into any particular technology or specific vendor and can stay flexible as their IT environment evolves and expands.

Replicas are more suitable than backups in true disaster situations, when the RTO needs to be reduced to a minimum and all production loads need to be moved to another site in the least amount of time possible. Replicated virtual machines (VMs) are inventoried and ready-to-run VMs in their own right, so when the worst happens, they can be failed over very quickly on dedicated and similar hardware that's pre-deployed on the Disaster Recovery (DR) site.

This is why replication needs a higher investment when it comes to storage and computing power at the DR site. Backups don't offer the same speed for recovery time objectives (RTOs), but are more flexible and portable and require lower storage consumption.

Backups can be copied on different support media and are much more manageable when addressing day-to-day recovery scenarios typical in ROBO environments.

With a large number of sites and locations, companies need to make a choice about where to do their backups and replication. This can be a challenge because some sites may require replicas, others may need backups as well, and they all need to have their individual specifications and requirements considered.

Having backups taken on-site provides some important benefits:

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- **Backup times are fast** because no information needs to be sent off-site;
- **Restore times are fast** because all data is very close to the host;
- **New replication features open up new options** such as creating a backup file and replicating a running VM at the same time.

Balancing Budgets and Business Requirements

Unfortunately, the best solutions for a remote office rarely line up to what most companies can afford to implement. It's widely understood and accepted that replication grants the greatest availability benefits for ROBOs because of the fast recovery times, but budgetary constraints often just allow for the use of backups.

Generally speaking, setting up backups is a very versatile and cost-effective solution. Setting up replicated virtual machines grants prompt business continuity, but requires a higher infrastructure investment.

The real challenge is finding the right solutions for rolling out across diverse remote office environments. No two locations ever look exactly the same; they often are designed and deployed on different dates and include their own individual requirements. This challenge can make it very difficult to roll out global backup and recovery policies across an entire organization. It can also lead to increased inefficiencies and longer restore times.

With a cost-effective hybrid solution in place that merges the advantages of on-site backup with the high availability and security offered by off-site replication, IT leaders can take control of this complex environment. They can ensure that everybody plays by the same rules and, regardless of the location, can recover data as quickly as the data centre at headquarters.

About the Author

Gregg Petersen is an IT industry veteran with over 17 years of experience. As Regional Director, MEA and SAARC at Veeam, he has been instrumental in creating brand awareness, growing the company's regional market share, driving profitable revenues jointly with partners, alliances and associates and continuously positioning Veeam as a leading provider of Availability solutions for the Always-On Enterprise.

Under his leadership, the company reported a record 54 percent increase in total bookings revenue in the Middle East in FY 2015 over the previous fiscal year, a 43 percent year-over-year revenue growth in enterprise orders, nearly 30 percent increase in net new customers and over 20% increase in new ProPartners compared to the previous year. The company has made significant inroads in the region with major customer wins such as National Bank of Abu Dhabi, The Arabian Geophysical & Surveying Company (ARGAS), Abu Dhabi Gas Industries Ltd. (GASCO), the Electronic Government Authority of Ras Al Khaimah and American University of Sharjah (AUS) to name a few.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

.comex

Exhibition & Conference

28 March - 1 April, 2017

Oman Convention & Exhibition Centre
Muscat - Sultanate of Oman

Under the Patronage

e.oman

www.comex.om

NO. OF EXHIBITORS **100**

PARTICIPATING COUNTRIES **10**

VISITORS ATTENDED **90,000**

For more information please contact:

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

Ahmed Farag, Sales Manager
+968 9411 3434
a.farag@oite.com

BOOK YOUR STAND NOW!

Media Partners

CDM CYBER DEFENSE MAGAZINE · thebusinessyear · TELECOM Review telecomreview.com · TEKNOTEL Technology & Business · Telecom Era · Dossier · Cyber Security Review Unique content / Global reach / In print and online · Enterprise IT WORLD · SMECHANNELS · عين الرياض Eye Of Riyadh · عين دبي Eye Of Dubai · India's Best Known Knowledge & Information Magazine SME WORLD · EASYFINDER OMAN'S LOCAL BUSINESS SEARCH ENGINE

Organiser

OITE TRADE FAIRS

The king of objections: the typical objections to deploying security

Balancing the corporate strategy with the need for information security controls

by: Corey Wilburn

There is a disturbing trend when it comes to security. We tend to think that only the big brands that are constantly hit with the types of breaches that color the headlines are at risk.

That is the fallacy of security, "if I'm not a big brand I can afford to skimp on security, since our organization too obscure to be a target."

From the IT lab to the board room we need to rethink how individuals go about assessing risk and what the actual risks are for the organization.

Of course, the Board and C-level are interested in costs, but it's important to enable people to take risk and move from a conversation focused on budgets and technology and also consider risk mitigation and business strategy.

When speaking to colleagues in the field, some common elements come up in conversations. Luckily many people *"get it"*. There are still some outliers in the mist, that will make, what appear to be reasonable (at the time) assessments.

Bottom-lines, budgets, cost, and ROI – are all valid business justifications for determining acceptable risk thresholds in an organization, and basing decisions on what is considered a good security investment vs a bad security investment.

Assessing risk and mitigating controls to ascertain the true value of an investment takes a bit of operational overhead if it is not already a component of the business culture.

With the prevalence of cybercrime, every organization must assess its risks thoroughly:

1. Take it from the top:

   Start your assessment from the examination of what your senior leadership hopes to accomplish in the long term. Ensure that the assets moving you toward that objective are secure.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

2. Minimize threats:

   It's impossible to eradicate a threat, but knowing is half the battle when it comes to minimizing their effect on your end goal. One useful technique is to set some policies and procedures and the regular cadence to review their success.

   You can also employ the knowledge and valued opinion of a third-party assessor to see if your risk evaluation is accurate and whether your policies and procedures do align with the protection of your most coveted assets.

3. Embrace the pain points in your security:

   No matter which stage you are at you will face growing pains. Identify them, face them, and overcome them.

One thing to consider, when facing the virtual ban hammer of budget land, is that there are plenty of open source tools available for use.

Many of these tools do great things, with the only investment needed being a little elbow grease and perhaps some fractions of compute.

They can help offset budgets and fill gaps. Many of offer actionable insight that will enable you to turn the tables on common objections you might face and allow you to further motivate business leadership to invest in an information security strategy.

Identify:

- OpenVAS is a great open source vulnerability scanner that utilizes commercially acceptable databases for vulnerability identification. A CVE based report will show….what the vulnerability is and what patches can remediate it. The tools will scan for devices live on the network (printers, servers) to get a result of the vulnerabilities in the environment and steps you can take to mitigate those vulnerabilities.

- Solve:
  - From this assessment, create an actionable report. For someone who is new to this process the reports often have little value in and of themselves, but by working with a third party, outside of your organization you can find prioritize the most critical vulnerabilities..

    Keep in mind that you are always vulnerable: identify, protect, and detect

Copyright © Cyber Defense Magazine, All rights reserved worldwide

- Patch based remediation can only go so far:
    - Typical remediation is accomplished through patch management which is the basic assignment of tickets and ensuring those patches are deployed.

      The push back and biggest hurdles often come with legacy systems that must be replaced with modern infrastructure.

- Quantify the remainder:
    - For the vulnerabilities that pose the greatest threat and take more than just a patch to remediate the best method to motivate action is to quantify the potential harm that this vulnerability may cause.

      Do the math and use sound judgement to come up with good numbers based on probability of occurrence and financial loss. The business tends to react swiftly when it can relate to the potential monetary loss incurred by an exposure.

Building motivation for information security investment can be an uphill battle. Being proactive about raising awareness about risk, threats, and vulnerabilities that your organization faces is the best approach. Use what tools and skills you have available and build from there.

When facing objections from above always be sympathetic to needs of the business. The more the business sees security as a restraint to its agility the tougher you are going to make the battle for yourself. At this level, everything is a balancing act.

Money talks; when a business can see that its inaction will likely result in financial loss it is more likely to take the steps necessary to protect itself.

About the Author

Corey Wilburn is the Security Practice Manager at DataEndure where he specializes in the design of strategic solutions, aimed at delivering high-value operational intelligence, leveraging best-in-class products as well as services built around current and emerging standards. He has a passion for InfoSec Policies, Processes, and Procedures.

He loves working with clients to help them realize the potential of their security strategy; maximizing ROI while reducing their attack surface, and helping them become more resilient in the face of an ever-evolving threat landscape.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

The implementation of SOCs with the SMEs

By Milica D. Djekic

The security operations centers (SOCs) are cybersecurity systems which are capable to provide a security in the both – technological and organizational manner. Through this review, we would deal with the SOCs that could be implemented with the small and midsize enterprises (SMEs) and offer a certain level of protection to those assets.

So commonly – these sorts of SOCs would include only one employee being the part of that SME who would be responsible for resolving the wide spectrum of IT and organizational concerns.

This IT Security Professional could be the part of SME asset or even outsourced depending on the small businesses' needs.

In an economical manner, the SMEs are from a strategic importance to the majority of commerce worldwide. Many countries including those the most developed would classify the SMEs as the part of their critical infrastructure.

The sabotage or diversion of such an asset could seriously disadvantage or even produce the catastrophic consequences to the economy of any nation.

For such a reason, it's crucially important to invest into a cyber defense of SMEs as one of the key factors to their functionality and operational capabilities.

It's well-known that those assets are not that highly protected as they should be in a cybersecurity manner, so it's so recommending to take care about their security in a technical and organizational way.

The SOCs could offer some level of defense in the both – technological and organizational sense, but how could we apply that to the SMEs?

Copyright © Cyber Defense Magazine, All rights reserved worldwide

One of the ideas would suggest that such an organization as an SME is deals with up to 50 employees and practically – it's sufficient to hire only one IT Security Professional who would maintain a level of the risk at an acceptable stage.

Such a practitioner could work in the office or remotely depending what the businesses' needs are.

So often, such a way of arrangement could get seen as an *ad-hoc* workplace. It's also significant to mention that such a SOC should use some IT tools for prevention, monitoring and incident response to a threat.

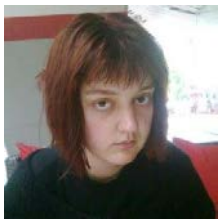
Finally, we would suggest to such an organizational solution to try to combine IT tools it uses. For instance, many developing countries could rely on open-source and freeware software which can be downloaded from the web for free.

On the other hand, the suitable societies dealing with the much higher budget could try to invest into the most optimal solutions which would satisfy the both – technical and economical requirements.

In other words, we would propose some cost-effective opportunities which would cope with the SMEs' capabilities.

At the end, we should always have in mind that SMEs are the part of critical infrastructure and it's highly advisable to equip them with some sort of cyber defense capacities for a reason of saving the both – private sector's and nation's budget.

About The Author



Since Milica Djekic graduated at the Department of Control Engineering at University of Belgrade, Serbia, she's been an engineer with a passion for cryptography, cyber security, and wireless systems. Milica is a researcher from Subotica, Serbia. She also serves as a Reviewer at the Journal of Computer Sciences and Applications and.

She writes for American and Asia-Pacific security magazines. She is a volunteer with the American corner of Subotica as well as a lecturer with the local engineering society.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

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 :

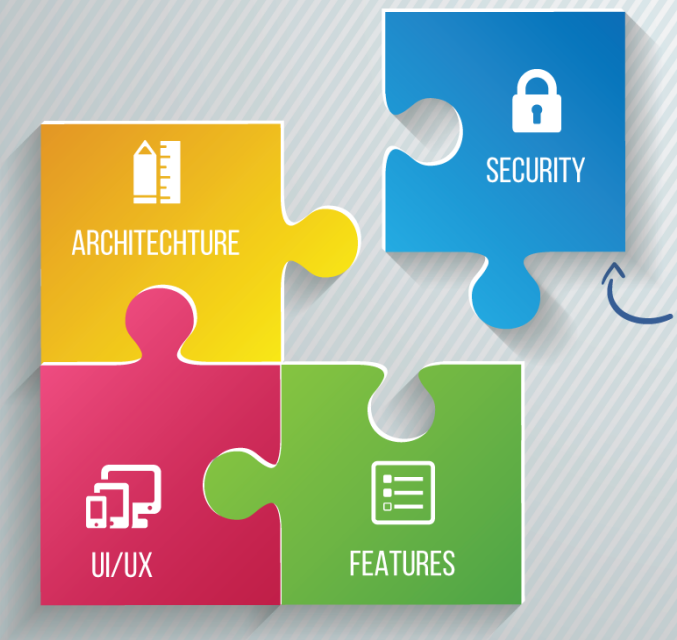
1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement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

Copyright © Cyber Defense Magazine, All rights reserved worldwide

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

AppCrusher is patents-pending, trademark and copyright © 2015, SnoopWall, Inc. All rights reserved worldwide. Other trademarks are properties of their respective owners.

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

AppCrusher is patents-pending, trademark and copyright © 2015, SnoopWall, Inc. All rights reserved worldwide. Other trademarks are properties of their respective owners.

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)

Copyright © Cyber Defense Magazine, All rights reserved worldwide

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. It's the NAISG.org's best kept secret.

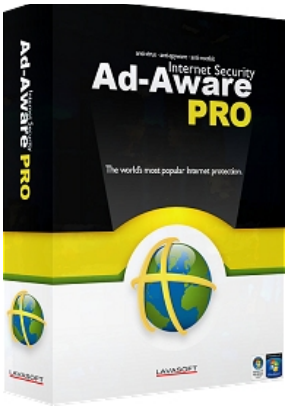
So use it by going here:

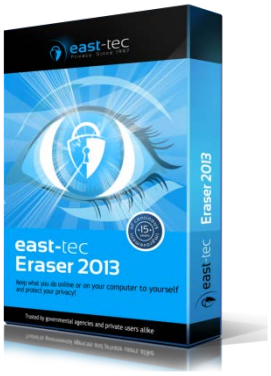
http://www.naisg.org/techtips.asp

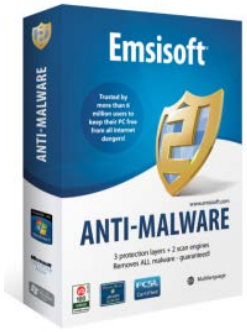
SOURCES: CDM and NAISG.ORG

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.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

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.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine November 2016

Sample Sponsors:

RSA CONFERENCE

StillSecure

PORTCULLIS

Hawk Mobile Monitor — Monitor Mobile Devices Remotely From Your Computer

AFORE — SECURE THE CLOUD. TRUST THE CLOUD.

NETCLARITY — PREEMPTIVE, PROACTIVE PROTECTION

CENTER FOR INTERNET SECURITY

Software Developer's JOURNAL — new ideas & solutions for professional programmers

SWIVEL — the power of knowing

SnoopWall — RECLAIM YOUR PRIVACY™

KASPERSKY lab

dekart — MAKE IT SECURE

INFOSEC WORLD

PWNIE EXPRESS

EncrypTight™ — BLACK BOX WAN Encryption

GO ANYWHERE™

BLUESPACE

CYBER SECURITY SUMMIT 2014 — June 5 DC Metro — Sept. 18 New York City

CYBER INTELLIGENCE USA — 18-20 JUNE 2014 - ARLINGTON/V.A

NETWORK MONITORING REDEFINED — See How RSA Security Analytics Detected Heartbleed — Watch video » — RSA EMC²

INDUSTRIAL CONTROL CYBER SECURITY — OCT 6/7 USA

INDUSTRIAL CONTROL CYBER SECURITY — SEPT 29/30 UK

2nd Annual Privacy, Policy & Technology Summit — January 26-27, 2015 New York

INFOSEC WORLD Conference & Expo — March 23-25, 2015 | Orlando, FL

January 21–22, 2015 • Calgary, AB — Cyber Security for Energy

CYBERTECH 2015 — THE EVENT FOR THE CYBER INDUSTRY

The UK Energy Cyber Security Executive Forum — London, 5th February — 20% discount (CYSENCDM)

CYBER SECURITY FOR FINANCIAL SERVICES — June 14 - 16, 2015 • Charlotte, NC

THE CYBER SECURITY SHOW — 13-14 April 2015 — etc venues 155 Bishopsgate, London

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

Copyright © Cyber Defense Magazine, All rights reserved worldwide

CDM
Secure Your IT World

CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Don't Miss Out on a Great Advertising Opportunity.

Join the INFOSEC INNOVATORS MARKETPLACE:

First-come-first-serve pre-paid placement

One Year Commitment starting at only $199

Five Year Commitment starting at only $499

http://www.cyberdefensemagazine.com/infosec-innovators-marketplace

Now Includes:

Your Graphic or Logo

Page-over Popup with More Information

Hyperlink to your website

BEST HIGH TRAFFIC OPPORTUNITY FOR INFOSEC INNOVATORS

Email: marketing@cyberdefensemagazine.com for more information.

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Cyber Warnings Newsflash for November 2016

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…

Malware uses Facebook and LinkedIn images to hijack your PC (updated)

https://www.engadget.com/2016/11/27/ransomware-exploits-facebook-and-linkedin-images/

Healthcare Is Prime Target of Gatak Trojan Malware

http://www.information-management.com/news/security/healthcare-is-prime-target-of-gatak-trojan-malware-10030348-1.html

'Watch Dogs' for Real: Malware Makes SF Bus Rides Free

http://www.tomsguide.com/us/ransomware-san-francisco-muni,news-23929.html

Office Depot caught claiming out-of-box PCs showed "symptoms of malware"

http://arstechnica.com/security/2016/11/accused-of-running-support-scam-office-depot-stops-using-dubious-scanner/

Malware is making ATMs 'spit cash'

http://www.bbc.com/news/technology-38063142

Copyright © Cyber Defense Magazine, All rights reserved worldwide

This Malware Turns Headphones Into Microphones

http://gizmodo.com/this-malware-turns-headphones-into-microphones-1789281461

Hospital info thief malware puts itself into a coma to avoid IT bods

http://www.theregister.co.uk/2016/11/22/healthcare_trojan/

This security camera was infected by malware 98 seconds after it was plugged in

https://techcrunch.com/2016/11/18/this-security-camera-was-infected-by-malware-in-98-seconds-after-it-was-plugged-in/

Malware and Mysteries: Secret Surveillance in Argentina

https://www.eff.org/deeplinks/2016/11/state-surveillance-argentina

Troubleshooting some nasty Safari malware

http://www.macworld.com/article/3142041/os-x/troubleshooting-some-nasty-safari-malware.html

Junk images on Facebook Messenger lead users to malware

http://www.geektime.com/2016/11/22/junk-images-on-facebook-messenger-lead-users-to-malware/

OneDrive for Business linked to malware menace

http://www.techradar.com/news/onedrive-for-business-linked-to-malware-menace

Researchers Design Malware to make a PC Perpetual Audio Tapping Device

http://www.spamfighter.com/News-20609-Researchers-Design-Malware-to-make-a-PC-Perpetual-Audio-Tapping-Device.htm

Copyright © Cyber Defense Magazine, All rights reserved worldwide

New malware poses frightening threat to cash machines

http://www.techradar.com/news/new-malware-poses-frightening-threat-to-cash-machines

Gugi/Fanta/Lime Malware Takes Over Androids

http://www.infosecurity-magazine.com/news/gugifantalime-malware-takes-over/

Hackers Are Using MailChimp to Spread Malware

http://motherboard.vice.com/read/hackers-are-using-mailchimp-to-spread-malware

Ad Tech Players Agree to Comply With Anti-Malware Measures

http://adage.com/article/digital/ad-tech-players-agree-comply-anti-malware-measures/306772/

Copyright © Cyber Defense Magazine, All rights reserved worldwide

Copyright (C) 2016, Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC. 848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide. marketing@cyberdefensemagazine.com Cyber Warnings Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC.Cyber Defense Magazine, CDM, Cyber Warnings, Cyber Defense Test Labs and CDTL are Registered Trademarks of STEVEN G. SAMUELS LLC. All rights reserved worldwide. Copyright © 2016, Cyber Defense Magazine. All rights reserved. No part of this newsletter may be used or reproduced by any means, graphic, electronic, or mechanical, including photocopying, recording, taping or by any information storage retrieval system without the written permission of the publisher except in the case of brief quotations embodied in critical articles and reviews. Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

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

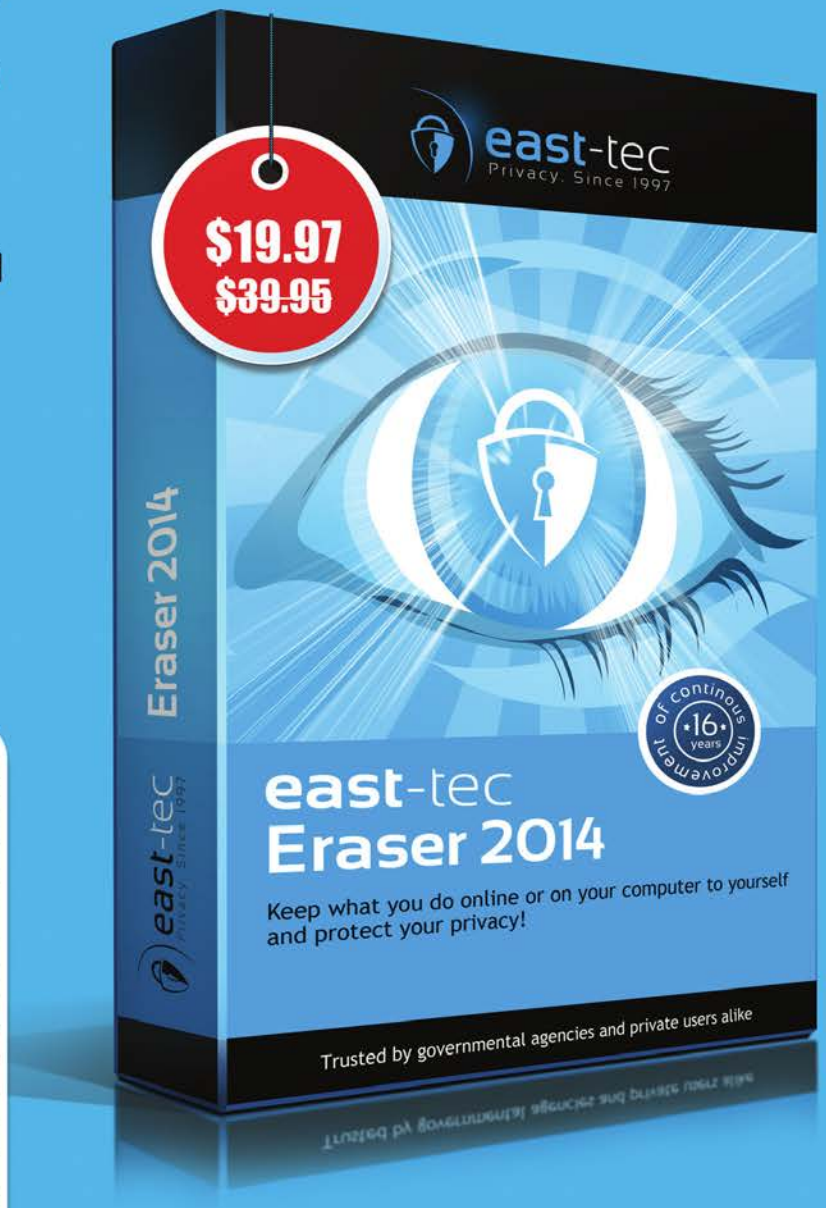
Cyber Defense Magazine - Cyber Warnings rev. date: 11/29/2016

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

private evidence protection traces from 250 + apps history
pages online privacy secure search pictures
cookies security emails