CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

Financial Cyber Security
Security Basics & Best Practices
Employee Training
IoT & Cloud Security

September 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

Stephen Stuut
MacLane Wilkison
Scott Montgomery
Ammar Enaya
Milica D. Djekic
Jamie Madison
Greg Mancusi-Ungaro
Eyal Benishti
Tom Gilheany
Marc Saldana
Matthew
Bill Graham
Dr. Daniel Osafo
John Brenberg
Harold Chanin

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

Executive Producer:
Gary S. Miliefsky, CISSP®

National Cyber Security Awareness Month is Around The Corner

Friends,

Why not make this International Cyber Security Awareness Month? As many American IT Security experts know, National Cyber Security Awareness Month (NCSAM) is observed each October since its inception in 2004 in the United States of America. It is sponsored by the National Cyber Security Division (NCSD) within the Department of Homeland Security and the National Cyber Security Alliance (NCSA, a non-profit organization), National Cyber Security Awareness Month encourages vigilance and protection by all computer users.

Wouldn't this be the best time to hop on the 'awareness train' and start focusing your October cybersecurity initiatives on end-user, employee, partner, executive, board, and shareholder cyber security awareness? You could simply copy the NCSAM themes, memes, tips and tools – sharing them throughout your organization throughout the month. What I like about the theme is that it reflects the notion that cyberspace cannot be secured without the help of all users. Each year, the month has weekly themes that deal with specific groups and trends in cybersecurity.

Some of the subjects I'd recommend you focus the initiative on are:

- Spearphishing and Malware
- Passwords Best Practices
- The BYOD Dilemma and Cleaning Up your Smartphones and Tablets
- Social Media Do's and Don't's
- Public Wifi Risks

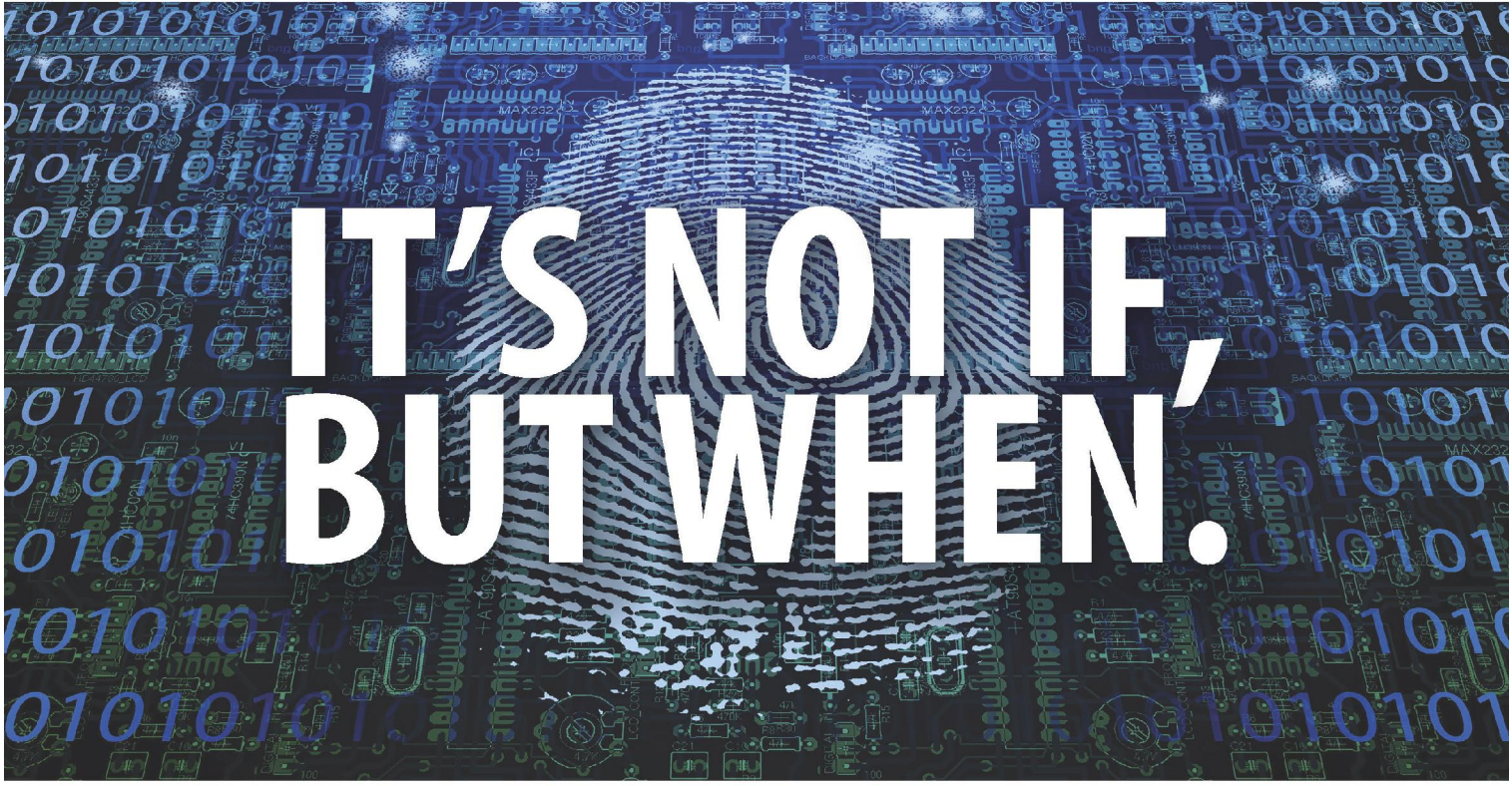
These are just a few of the ideas you could discuss with your organization throughout the month of October as part of your own Cyber Security Awareness campaign.

Remember, that most breaches happen behind firewalls and on systems already protected by antivirus software. It's usually an accident by a trusted insider and in some cases a malicious insider. Now is the best time to start your early Fall Season cleanup. Take the time to share your ideas on 'great' cyber hygiene and show your organization how a few steps of proactivity will go a long way to prevent a very expensive breach. On that note, I suggest you read on as you'll find more articles in this edition on the theme of best practices, so you can get one step ahead of the next threat.

To our faithful readers, Enjoy

Pierluigi Paganini

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



GET CYBERSEC FIRST RESPONDER CERTIFIED

TO BECOME THE FIRST LINE OF DEFENSE AGAINST CYBER-ATTACKS

The ProCert Accredited Logical Operations CyberSec First Responder (CFR) certification validates the ability to perform active network analysis and incident response techniques, moving well beyond security fundamentals and prevention measures common in other IT security certifications.

Our holistic approach to security ensures you understand the tools, processes, and strategies necessary to protect your organization's data not only before, but also during and after an attack – regardless of your company's hardware and software configuration.

PROTECT YOUR ORGANIZATION. Learn more at CFRcertified.com

Logical Operations™
CERTIFIED

CYBERSEC FIRST RESPONDER

A Culture of Cybersecurity: The Only Way Forward

A Logical Operations Whitepaper

Logical Operations

Is the Russian government actively trying to influence the U.S. Presidential election? Is the House Oversight and Government Reform Committee's assertion that we must treat federal employees the same as outside threats in order to prevent data breaches correct? Are American businesses truly losing the battle against hackers? Recent media headlines suggest the American public is hungry for news about cybersecurity incidents. Given that media outlets stay in business by getting eyes on the screen, it seems a safe bet to say they're right. And, with good reason.

Attacks are hitting users and systems in frightening numbers. According to the Kaspersky Security Bulletin for 2015, more than one in three user computers (34.2%) experienced an attack while the owners were online last year. Given the number of computer users worldwide, that's a staggering figure. Security breaches, identify theft, and malicious attacks on critical infrastructure, quite simply, have people scared. And when people are scared, they want information. And these days, there's no shortage of it.

However, outside of general public-awareness campaigns and media attention, the only exposure to cybersecurity training most people receive is through programs delivered to them, as either employees or contractors, through companies and other organizations. Unfortunately, this type of training typically comes in one of two forms: buried within other onboarding paperwork as part of Human Resources processing, or through self-paced learning modules that employees begrudgingly complete on a second computer monitor while attending to "more important" matters.

In addition to the relatively low standards of the security training programs offered by many organizations, these programs often also overlook a critical component of knowledge retention: engagement. Many security awareness programs simply don't answer the questions "why should I care?" and "how does this impact me?" The general public still has this pervasive sense of cybersecurity being an "IT issue," despite the mountain of information publicly available indicating that end users represent the single greatest risk to information and system security. Consider these two additional facts from the latest Kaspersky Security Bulletin:

- More than 75% of all web-based attacks last year came in the form of malicious URLs (how many end users in any large organization could have clicked just one of them?).
- The United States accounted for nearly a quarter (24.18%) of all cases of infected online resources (as measured by antivirus systems blocking known exploits).

Until organizations, their end users, and the population as a whole adopt a culture of cybersecurity, all of the awareness training, system hardening, and resource allocation could be for naught.

But, there are signs of progress. As cybersecurity threats have increased, both in frequency of occurrence and media attention, some organizations are formalizing their training and awareness efforts as a way to protect the massive amount of data they generate, especially as data has become an increasingly valuable asset. Instead of simply providing their employees and customers with policy updates or basic instructions on how to identify and report potential threats, organizations are beginning to understand that systems threats have taken on many new forms, and that training must be delivered by an expert facilitator in order to convey the true importance of this issue.

Recognizing the need this new understanding is creating, Logical Operations released its "CyberSAFE: Securing Assets For End-users" education program to commercial training providers, corporations, and consumers in 2015. The program was designed from the ground up to be delivered by an expert facilitator (in either live, virtual, or blended environments), which helps to ensure the transfer of knowledge and skills—along with the critical importance of them—to learners who might otherwise gloss over the material on their own. The result? Organizations with staff and customers who have a much greater sense of the dangers of the virtual world and how to mitigate against them, and consumers with a heightened demand for cybersecurity protection from the vendors they trust with their digital information.

While practical, engaging training programs are beginning to have a positive impact on end users and how they interact with technology, the most promising approaches for addressing cybersecurity training needs into the future will feature a way for people to validate their new-found knowledge and skills. Well-designed and implemented training programs are unquestionably effective. But, it's critically important to be able to measure or verify that effectiveness. As a student, it's common to attend a training program (whether self-paced or instructor-led) and come out on the other side feeling as if he or she retained all of the important information. As someone responsible for implementing a training program, it would be easy to review a program's content, verify that it is sound, observe live training sessions, and assume that attendees achieved the desired result. The problem, though, is that it's still an assumption.

Neither of these scenarios actually demonstrates that students retained knowledge. And without proof that the desired outcomes have been achieved, what was the point of putting the training program into place to begin with? Cybersecurity is simply a topic that can no longer be given only passive attention. The addition of a knowledge-verification process, such as a credential or certification program, provides the mechanism necessary to, if not guarantee, at least verify training effectiveness.

As part of Logical Operations' CyberSAFE program, all students are provided the opportunity to earn their own CyberSAFE credentials, which demonstrate competence in key areas of cybersecurity awareness. And, Logical Operations' approach to the credentialing process avoids some of the pitfalls of other similar programs. Perhaps the most appealing part of this approach is the fact that CyberSAFE credential candidates are not forced to schedule and take an exam at a remote testing center. This is a huge convenience for students and it allows their organizations to save the time and money that they'd otherwise naturally expend if they had to rely on third-party facilities. CyberSAFE candidates can access the credentialing process through Logical Operations' CHOICE LMS platform, providing them with anytime, anywhere access (via nearly any device) to complete the credentialing process in a way that makes the most sense for them.

In addition to the convenience this approach provides, it also helps students avoid feeling trapped by the constraints they might otherwise be faced with. Formal, high-pressure situations that tether candidates to a specific place at a particular time leave them feeling stuck, rather than empowered. This fosters a sense that cybersecurity is something with which they must comply, rather than a problem they can actively help to solve. Providing a positive experience simply makes the process seem more realistic and achievable.

Another key differentiator of Logical Operations' approach to the credentialing process is what happens to candidates who don't pass the exam on the first attempt. To expand on the idea of being trapped, candidates who know they have one chance to pass an exam might either cram for it, or try to cheat in order to get by on the first try. The downside of failing, which is having no ability or encouragement to earn the credential without significant cost or effort, actually works against the goal of having more people be able to demonstrate a comprehensive understanding of key security principles and practices. This is precisely why candidates have ready, ongoing access to CyberSAFE course materials through the CHOICE LMS and can retake the assessment at their convenience.

Another positive aspect of Logical Operations' approach is that it provides successful candidates the ability to broadcast their understanding of cybersecurity awareness principles to their colleagues and peers. The traditional method of sending an email announcement or mailing a certificate is static and old; it isn't inspiring for the certificants, and it doesn't allow them to serve as advocates for more participation in the process. Instead, Logical Operations issues successful candidates an electronic badge that can easily be shared via social media platforms, such as LinkedIn, and in email signatures. Enabling people to broadcast their achievements not only provides them a platform for demonstrating their understanding of this critical issue, it also helps raise the general awareness level of cybersecurity concerns among their peers.

So, what can we do collectively in the coming years to better address the challenge? Launching an effort to promote engagement, whether for employees within an organization or the public at large, is critical, and we should capitalize on the mechanisms for doing so that are already in place for a number of other efforts. Think about how an organization drums up support for an effort such as a blood drive or a charitable-giving campaign. People put cards and table tents out in common areas, they hang signs in hallways, they give out coffee mugs and t-shirts, members of the management team engage with their direct reports, the marketing team produces and shares awareness videos, and so forth. The same approach would absolutely work when promoting security awareness. Businesses should look beyond the tired, and often ignored, email from the IT department when trying to engage with staff, and public service organizations need to be using all of the tools they have at their disposal to get the message out.

All of this should be pointing all of us in a single direction: fostering a culture of cybersecurity in which everyone has a stake and can play an active role in keeping critical data safe. Ongoing internal marketing efforts and public awareness campaigns can engage people throughout the training and certification process—and beyond. This is a far more effective approach than simply reaching out to people once every three years when it's time to recertify. In the rush of daily life and the complex operations of large organizations, it's easy for people (who are the weakest link in the security chain) to simply forget, even if just momentarily, their roles and responsibilities when it comes to keeping systems safe. A single click on a malicious link can lead to a major security breach costing millions of dollars—the latest global analysis from the Ponemon Institute puts the figure at an average of $4 million per breach. We simply cannot go on thinking cybersecurity is somebody else's job.

Moving ahead over the next decade, organizations need to execute a plan for routinely verifying the comprehension of key cybersecurity knowledge while promoting the idea of security as everyone's responsibility. The pace at which new types of cybersecurity threats emerge is, as an understatement, rapid. A training session from last year is rarely reflective of the current security threats that could impact to the average data consumer or employee. The same holds true for a certificate or certification program associated with the topic of security awareness. Organizations need to routinely assess both their customers and their employees in order to identify weak spots that expose their data to cyber threats. And, we as consumers need to do the same in terms of our daily habits. We need to identify the specific areas of cybersecurity we are unfamiliar with, and then educate ourselves on them, in order to adequately protect our personal data.

Along the same line, organizations absolutely must start adopting a prevention-first mindset. Though the importance of cybersecurity is unquestionable and the resulting damages from attacks are daily fodder for news outlets, many organizations still feel it is more cost effective to wait until they experience a breach and then react to it, rather than invest the necessary time and resources into hardening their systems and training their people ahead of time. It is this type of shift in paradigm that is desperately needed in the coming decade and beyond to ensure data consumers and employees alike are vigilant against cyber attacks. Given the number of people who experience identity-theft issues, the incredible amount of compromised personal data, and the hugely expensive organizational attacks that have become all too common, it's astonishing that people and organizations are still slow to react.

While end-user training and certification are critical to helping solve the current information gap, it is important that organizations of all sizes continue to invest in training and certification for the people specifically charged with designing and maintaining a secure network. All too often, organizations that do send their IT staff for training are sending that staff to classes built around certifications that were cutting edge a year, or substantially longer, ago. A lot has changed, and continues to change, in the realm of IT. Gone are the days of an organization using purely Microsoft software or Cisco hardware solutions. Organizations today are vendor agnostic; they use the most appropriate vendor technology and solutions for the tasks at hand. And potentially more disruptive yet, these solutions are increasingly shifting to the cloud.

To prepare for these challenges, Logical Operations has launched additional training and certification programs within the market that are geared toward

the IT professional within a typical organization. These programs take a fresh look at training, and ensure applicability against both the latest and the emerging trends in IT.

"CyberSec First Responder" (CFR) is an IT security program designed to prepare candidates for the key job tasks of actively analyzing a network for security threats, and then responding to incidents. While many IT security programs focus on core IT security principles and prevention measures, the CFR program takes a different approach, placing the emphasis on disrupting a live attack and then working to mitigate its negative effects from not only a data perspective, but also the perspective of employees and an organization's customers.

Although the program demonstrates a more specialized skill set than those presented in common fundamentals programs available on the market today, CFR also addresses the roles played by nearly all members of an IT team during a breach. When a breach does occur, it's all hands on deck…period! And, it's critically important for those hands to be specifically prepared to respond to an IT security incident. The CFR exam, administered at Pearson VUE testing centers worldwide, is maintained continuously by Logical Operations' various training content and certification development subject matter experts and practitioners. The content and the exam are updated multiple times each year to ensure the program is keeping pace with the latest security threats. And, a key part of the program is focusing on the responsibility security practitioners have to research and keep up with those emerging threats. Similar to other Logical Operations offerings, CFR is also vendor-agnostic. A quick review of basic CFR information, such as the course outline or the exam objectives, demonstrates broad coverage of various technology environments and security tools that reflect the realities of working as a security professional in a variety of organizations.

Cybersecurity has emerged as one of the critical issues of the current era; no one is disputing this. What continues to challenge organizations and society as a whole as we combat this issue is a combination of poor prioritizing, a cultural misunderstanding of our own responsibilities, and the challenge of attacking an extremely fast-moving and rapidly-evolving problem with constructs and institutions that were put in place long before cyber threats could have even been imagined. However, like with so many past issues that seemed too big to grapple with, a change in mindset, proper education, and innovative thinking can help all of us make consuming data and storing critically valuable digital assets on network systems safer while still allowing us to embrace the incredible benefits offered by the digital landscape. But, we have start thinking differently…now.

Facial Recognition: Killing the Password One Photo ID at a Time

By Stephen Stuut, CEO of Jumio

In today's complex cyber security landscape, the notion of utilizing a password to validate a user's authenticity is rudimentary.

Cybercriminals can retrieve passwords through a variety of ways. One of the more common processes is via a breached network or public Wi-Fi services found in public areas like transportation venues and restaurants. And it's a simple three-step process:

- The fraudster creates a Wi-Fi hub that's identically named to the venue's legitimate Wi-Fi hotspot.
- Customers then log onto the fraudster's hotspot, which contains malware that allows the fraudster to access their machine.
- The fraudster then accesses the customer's online accounts, at the same time hacking their password using fraudster cryptography tools.

Recently, a large search engine provider experienced a major data breach in which a hacker was able to steal login information for 200 million email accounts. The stolen records are currently up for sale on a darknet marketplace that offers illegal goods. For 3 bitcoins, or $1,824, anyone can buy the stolen records and, once retrieved, can likely access personal information for each user. Passwords remain a vulnerability within the threat landscape. To combat this threat, companies need to implement more secure means of verifying the person making the transaction is in fact who they say they are. Biometric facial recognition with liveness combined with a government issued form of identity is the next trend in securing individuals and businesses.

A password is a secret string of letters, numbers, and symbols that validates someone's identity, and allows that user to access proprietary information such as email messages, medical records, social media accounts and more. However, passwords remain targeted by cybercriminals because of their value. When breaches occur by cybercriminals or hackers, passwords are often released to their "dark" network and can be sold or purchased for malicious intent. The cyber tech industry needs to do more to maximize consumers' security; starting with replacing passwords with facial recognition.

Facial recognition is quickly helping address fraud issues within a number of industries, such as financial services, travel and transportation, businesses that fall within the shared economy, online gaming and more.

With online and mobile transactions on the rise, there are more ways to pay than ever. Whether it's opening a new account, transferring money, or adding a payment card to an application that's used frequently (such as shared ride services), online and mobile payments are sky

rocketing. This growth also comes with an increased security risk, and companies offering these payment methods are continually challenged to provide processes that will build trust, ensure safety and reduce fraud, while simultaneously maintaining convenience.

In a recent Business Insider article, Malcom Marshall (Global Head of Cyber Security with KPMG International) sheds light into the problems with passwords: "It's time we found ways to get rid of the password. They are no longer viable and considering the extent of how much we live our lives online, we need to find ways to make ourselves more secure. After all, think of how many passwords we use and how hard it is to remember them all. Even I have had to constantly reset my passwords because I keep forgetting them," said Malcolm Marshall, Global Head of Cyber Security practice at "Big Four" accountant and consultancy KPMG International. While a step in the right direction, multi-factor authentication methods are missing the mark; the use of a password or security code is not a secure way to confirm an individual is the said owner of an account. Password and codes passed via mobile devices can be hacked and there is no proof that the mobile device is in the passion of the owner.

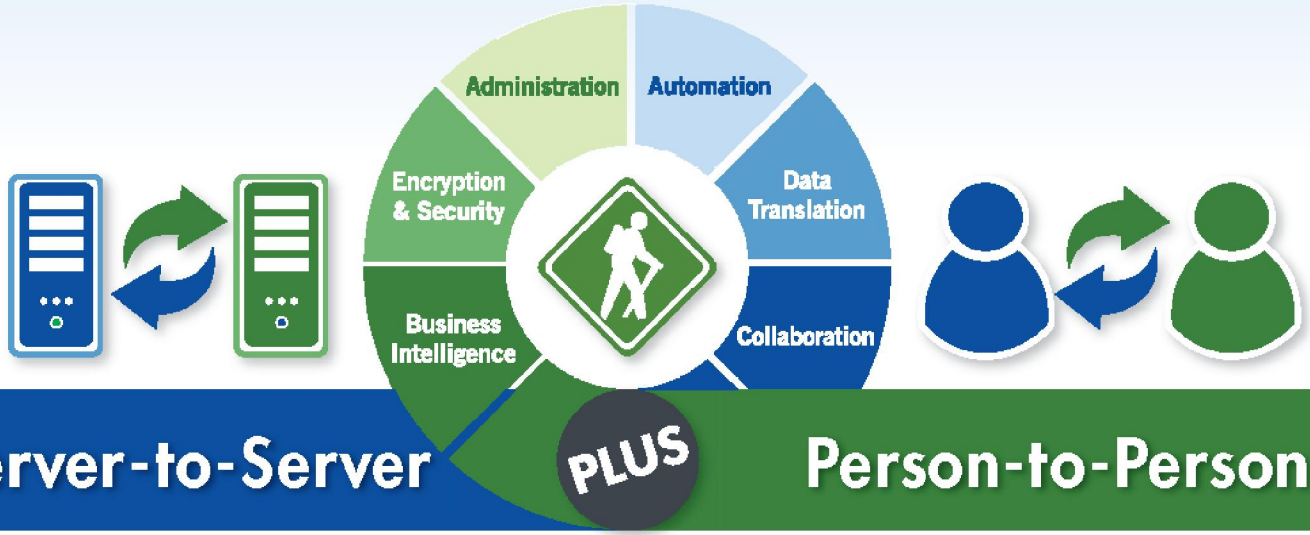
A recent report from the National Institute of Standards and Technology referred to the process of multi-factor authentication as insecure because the phone may not be in possession of the number and the SMS may be interrupted. However, for a better approach, utilizing a combination of one or two government issued IDs with live photo and facial recognition, companies can ensure that an ID is valid and the person in possession of the ID is in fact the genuine ID owner.

Facial recognition is also the first step in knowing a business' customer – and ensuring that the person trying to access private information is in fact the appropriate person attempting to do so. Facial recognition providers can turn a smartphone or computer into an ID scanning terminal that captures and verifies an ID and other credentials to meet Know Your Customer (KYC) requirements – and ultimately reduce fraud. The missing piece within the password puzzle is one that offers digital identity verification – or facial recognition that includes liveness. This technology can replace passwords by identifying and authenticating users for all online services, including commerce and banking. It enables apps, websites and other services to recognize users, and therefore dramatically change how we make online transactions all while decreasing the potential for fraud and identity theft.

About the Author

Stephen Stuut, CEO of Jumio

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

Why Security Remains the Biggest Issue for FinTech and Financial Services

Financial cybercrime and fraud is big business. With billions of dollars lost to hackers and cyber criminals each year, it has never been more important for financial firms to ensure their - and their clients' - security.

MacLane Wilkison of ZeroDB explains just why security measures are so important to the financial sector.

Money makes the world go round, at least, that's how the saying goes. So it stands to reason that anything that prevents access to money, or serves as a hindrance to the flow of capital, is a problem for global business and economic development.

Sadly, financial fraud - a significant obstacle to access to capital - is big business. The total global worth of financial cyber crime is predicted to hit $2 trillion by 2019 and according to Ginni Rometty, the chairman, president and CEO of IBM, cybercrime is "the greatest threat to every company in the world".

According to a report from Symantec, financial organizations - including banks - remain the most likely victims of cybercrime.

While simplistic "script kiddie" attacks aren't typically effective against financial institutions, banks are being increasingly targeted by well resourced and sophisticated attacks.

Bankers are rightly worried. According to a report from the Big Four accountancy firm Deloitte, cyber crime is the biggest single economic risk to the financial services sector. If that weren't enough, the finance industry suffers from 300 times more attacks than any other industry.

In the face of such persistent attacks, constant vigilance with regard to security is the only way for financial institutions to protect their and their customers' data.

The Rise of FinTech and FinTech Crime

In recent years, FinTech - financial technology - has grown exponentially. The United States is the leading country for FinTech development, where bank spending on new financial technology is predicted to top $19 billion by 2017.

Globally, peer-to-peer (P2P) lending hit $1.82 billion in 2014, a staggering figure.

However the rise of FinTech has seen an equivalent increase in financial fraud. According to research from PwC, another of the world's Big Four accountancy firms, more than one third of businesses experienced some form of economic crime in the last 24 months, of which cybercrime was the second most reported form.

Similarly, financial cybercrime was the only form of economic crime to see an increase in the last year, highlighting how online fraudsters are developing new techniques at a faster rate than those working to stop them.

While banks have been all too pleased to champion the benefits of FinTech, they have been less keen to discuss the increasing level - both in strength and frequency - of the attacks they are experiencing.

In a survey conducted by the Centre for the Study of Financial Innovation, one anonymous respondent warned about the systemic risk of "a cyber-attack so powerful on an individual bank that it has the power to bring down the institution, necessitating a state bailout".

Fixing the Problem

According to PwC, the prevalence - and success - of cybercrime should not be treated as an IT problem. Rather, the firm says, financial cybercrime is an issue that needs to be addressed from the top of each and every organization if it is to be overcome.

As if it wasn't bad enough that more than a quarter of PwC's respondents said they had been affected by cybercrime, a catastrophic 18% said they did not know if they were victims of cybercrime. In 2016, this is inexcusable.

Businesses are simply not taking the necessary precautions to prevent becoming victims to financial fraud and cybercrime.

Social media websites are also becoming a prime hunting ground for would be fraudsters, with LinkedIn becoming a go-to choice for those hoping to commit cybercrimes, and firms need to educate staff about the security risks around social engineering posed by social networks.

Using fake profiles on LinkedIn, criminals can coax employees to give up vital information, including emails, that will increase their ability to commit fraud later on.

One cyber criminal gang, Carbanak, managed to steal more than $1 billion from financial industry businesses by using employee email address that had been willingly given up.

As in all battles, it's important to know your enemy in the fight against cybercrime and financial fraud. Another of the Big Four accountancy firms, KPMG, has extensively profiled those who are most likely to commit financial crime.

The vast majority of fraudsters are male (71%) while a staggering 65% are employees at the company they are defrauding.

Additionally, 69% of all fraudsters are between the ages of 36 and 55, meaning that businesses are most likely to experience fraud committed by a male employee over the age of 35. Investing security is the only way for businesses in the financial industry - as well as other industries - to protect themselves from financial crime.

Earlier this year, J.P. Morgan Chase & Co. spent half a billion dollars on cybersecurity, a move followed by nearly every large financial institution.

Forensic accountancy firms like Kroll specialize in protecting businesses and financial services firms from both internal and external cyber attacks.

They use software to analyze log data and communications to identify potential cyber attackers in advance.

However, these services do not come cheaply and, with the rising number of FinTech firms and startups, the need for affordable security that's available to smaller firms is significant.

The United States' Small Business Administration (SBA) recommends that small and medium sized businesses (SMEs) secure their IT infrastructure in order to protect against financial fraud. Similarly, financial regulators are exerting increased pressure to see finance firms step up their cybersecurity.

Higher security is not just good business sense, it is frequently a legal and regulatory requirement.

Last year the UK government pledged grants to small businesses to help protect them against cyber threats. All financial businesses will need to assess their own security strategy and decide what is right for them.

The important thing is start that process now, before it is too late to protect from an attack.

About the Author

MacLane Wilkison is the co-founder and CEO of ZeroDB, a Y Combinator-backed startup that provides enterprise security and encryption for big data in the cloud.

ISACA

EXPLORE. EXCHANGE. EXCEL.

Boost Your Cyber Security Knowledge

Join the Experts at CSX 2016 Asia Pacific

Cyber threats affect your enterprise every day. Threats don't take holidays and they are becoming more intrusive and potentially devastating. Stay ahead of the most critical issues, meet global colleagues and find effective solutions to the ever-changing security landscape at the must-attend event of the year—CSX 2016 Asia Pacific Conference.

Build your cyber security knowledge and leadership skills as you learn about new tools and trends from globally renowned speakers. Test your skills and compete in the innovative new CSX Cyber Challenge.

Hosted by ISACA's Cybersecurity Nexus (CSX), this event brings together many of the brightest minds in information systems and cyber security. Take the next step in protecting your enterprise and boosting your career.

CSX™ 2016 ASIA PACIFIC

CYBERSECURITY NEXUS

AN ISACA CYBER EVENT

14 – 16 November | Singapore

Earn up to 32 CPE hours.

Register by 4 November 2016 and Save!

www.isaca.org/CSXSingapore-CDM

Presented by ISACA®'s Cybersecurity Nexus™ (CSX).

Why Enterprises Need a Multi-Layer Approach to Public Cloud Security

Security has long been the principal fear that weighs on cloud investments. While perceptions are improving, Intel Security's recent State of Cloud Adoption study found that data breaches remain the biggest concern of companies deploying Software as a Service (SaaS), Infrastructure as a Service (IaaS), and even private cloud models. A 2015 survey by Crowd Research Partners found that nine in 10 security professionals worry about cloud security.

These concerns, however, are not stopping enterprises from investing in the cloud. The Intel Security study found that while the survey shows that confidence in cloud security is increasing, only one-third of respondents believe their senior executives understand the security risks. Investments in cloud security should be commensurate with the level of migration to cloud services.

But budgeting for security in the public cloud is distinctly different than planning for on-premise prevention. One fundamental shift is that cloud providers use a "shared responsibility model" that spreads risks between vendor and customer.

Another difference, customers don't buy the same mix of products and equipment to secure the cloud that they do in the data center.

Budgeting for security in the public cloud begins by considering which applications and infrastructure components will live there. Some, like website hosting and document serving, are of relatively low risk and don't demand the most stringent safeguards. Also consider the consumption models you'll use.

SaaS providers generally assume responsibility for security and the application and system levels. However, IaaS providers tend to cede those responsibilities to the customer. What's more, no public cloud provider is likely to assume responsibility for user access and data protection, although there are measures they can take to support your own efforts.

There are three levels of security to consider as you build out your public cloud strategy:

System-level security for IaaS

This is secured plumbing: systems-level components such as operating systems, networks, virtual machines, management utilities and containers. Here, you want to invest in cloud providers that make it easy for you to keep your systems current with the latest patches and updates.

The service provider should also provide thorough visibility into your cloud instances so that you can see all instances that are running.

One of the challenges of public cloud is that it's so convenient to spin up new VMs and containers that you may forget to shut them down later. These so-called "zombies" are latent security threats because they present potential attack vectors into more business or mission critical systems.

If you plan to use containers, as a growing number of enterprises are, be diligent about the level of security protection they offer. The market for containers is still immature, and security – while improving – is considered one of the technology's weakest areas.

Remember, you are responsible for system-level security in your Infrastructure as a Service (IaaS) and Platform as a Server (PaaS) instances.

Integrating these security controls and reporting in with your on-premises systems will create efficiencies. Be sure to include the appropriate controls for the type of server employed.

These may include tools such as intrusion prevention, application control, advanced antimalware solutions and threat detection. These should all be centrally managed for visibility and compliance in addition to policy and threat intelligence sharing with your on-premises infrastructure.

Application-level security

This level is primarily about identity and access management. Your best investment here isn't financial; it's a policy that limits the ability of users to deploy cloud applications without IT's knowledge.

After ensuring policies are in place that offer IT visibility, the next step is to invest in multifactor authentication and identity management. The first approach uses two or more devices or applications to permit access.

Identify management locks down application access by requiring users to authenticate through a secure resource such as LDAP or Active Directory.

If your organization already uses a directory, consider investing in cloud brokering software that supports single sign-on so that users can authenticate to all their cloud services through their local directory.

This gives IT complete visibility and shifts access control from the cloud service to your own IT organization. Consider also investing in a secure VPN tunnel so sessions are never exposed to the public Internet.

Data-level security
This level of protection involves securing the data itself. No cloud provider will take responsibility for your data, but there are solutions you can purchase to help.

Many cloud providers, for example, offer encryption as a standard option, but you may be surprised at how many do not, or who encrypt data only part of the time. Anything less than 256-bit encryption is considered inadequate these days.

More important is that you have full control of the encryption keys. If a cloud provider insists on owning them, you have no guarantees that your data will be safe. Seek another provider.
In addition, make sure your data is unencrypted only when in use.
Some providers require that data be transmitted to their facilities in plain-text format. That's a security risk.

Whatever cloud provider you adopt, make sure their security guarantees spelled out in their contract and SLA.

A good contract should spell out exactly what procedures will be employed, along with any penalties the provider will face for non-compliance, how they will report upon it, and how you can audit to ensure your contractual terms are being met.

A strong SLA ensures that you don't simply toss the keys to your cloud provider as you're walking out the door.

About the Author:

Scott Montgomery is vice president and chief technology officer of public sector at Intel Security. He runs worldwide government certification efforts and works with industry and government thought leaders and worldwide public sector customers to ensure that technology, standards, and implementations meet information security and privacy challenges. His dialog with the market helps him drive government and cybersecurity requirements into Intel Security's products and services portfolio and guide Intel Security's policy strategy for the public sector, critical infrastructure, and threat intelligence.

With more than 15 years in content and network security, Montgomery brings a practitioner's perspective to the art and science of cybersecurity. He has designed, built, tested, and certified information security and privacy solutions—including firewalls, intrusion prevention systems, encryption, vulnerability scanners, network visibility tools, mail and web gateways, strong authentication tokens, embedded systems, and more. Prior to its acquisition by Intel Security, Montgomery ran worldwide product management and corporate strategy for Secure Computing.

BYOD Could Mean 'Bring Your Own Disaster' if Organizations in Middle East Don't Plan for Security Risks

As adoption of wearables becomes more mainstream in the Middle East, it brings added complexity to BYOD in an enterprise. One of the more interesting features of wearable tech is its ability to tether to, and control, smartphones over a remote connection. So even if wearables are denied access to enterprise networks, they may already be able to access it. Which means they can download and store company data. Many come with built-in cameras. This will understandably make IT departments worried.

According to recent studies by Aruba, the new generation of employees –#GenMobile – expect mobility at the workplace to be a given, so any blanket decision to ban such devices from the workplace will be highly unpopular. In fact, almost two thirds of study respondents say they use mobile devices to help them manage their work and personal lives better.

If the decision is made to accept wearables into the organisation, it is unlikely that existing BYOD policies that govern the use of corporate data be enough - new policies will be required.

When tinkering with these policies, CIOs have to keep in mind the fact that there will be other IoT-based devices coming along that could be embedded into an employee's clothing or even office kitchen appliances. The acronym "BYOD" will soon have to be replaced with "BYOX", with the "X" symbolising "practically anything".

Failure of First Generation of BYOD policies – Lessons to be learnt

The first generation of BYOD devices received similar levels of access to the network, in a fairly uniform approach. This needs to stop. CIOs should now turn their attention to the context of the use case, and the underlying communications network. This means putting in place solutions that can secure any mobile device that connects to corporate Wi-Fi; giving them complete visibility of the number, type and frequency of mobile devices assessing their network.

Today's network should be capable of enforcing flexible security policies that are capable of analysing – and acting on - the context of how an employee uses the mobile device. For instance, an employee using a smartwatch at a coffee shop to access corporate data may not be granted the same level of access as one who uses a PC during office hours. Depending on the context, different policies should be applied to make sure that the right balance between flexibility and security is met.

By incorporating these new levels of network visibility, companies will also be able to identify specific applications and who is using them. After these apps are identified and visualised, access controls and policies should be applied to prioritise the performance of business-critical apps over personal ones. By analysing and controlling access management systems, it is possible to get as granular as disabling a device's camera in restricted locations.

Key security considerations for BYOD

People talk about BYOD or 'choose-your-own-device' - but it could really end up being BYOD 'bring-your-own-disaster' if you haven't thought about the fallout of that going wrong. There are a number of security habits companies need to adopt to adequately protect themselves against a breach:

1. Regulate Wi-Fi traffic with intelligent policy firewalls that can keep track of app usage. This ensures that different apps are classified according to its security rating based on the role of the employee within the organisation. These apps would be allowed to be used on select mobile devices by select users, only if they satisfy live security monitoring by the policy firewall and cloud-powered content filtering.

2. Make sure that all communications over the air are encrypted and sent over secure channels. This requires a smart combination of encryption and VPN-on-demand technologies that prevent information from being snooped on, and – even in the event that the information falls into the wrong hands – is rendered gibberish.

3. Focus on the interactions between users, apps and data. The perimeter has shifted from the idea of building a wall around your enterprise and fortifying your organisation with a firewall. The Internet of Theft (IOT) and Bring your own Disaster (BYOD) have become prevalent in the organisation, considering that business users and consumers nowadays demand access to data and business insights anywhere and in a commoditised form.

4. Managing the security of BYOD, IoT, BYOX, whatever you'd like to call it, requires a secure yet flexible wireless network within the workplace. Companies should deploy flexible security policies that are capable of analysing – and acting on - the context of how an individual employee is using a mobile device, and where they are accessing information from.

By all means, organisations in the Middle East should embrace #GenMobile's penchant for openness, innovation and collaboration, using any device they wish. But only when they can understand and plan for the security risks these behaviours bring along.

About the Author

Ammar Enaya, Regional Director, HPE Aruba, Middle East & Turkey

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**

+65 6725 9921 | enquire@iqpcexchange.com | www.cybersecurityexchangeasia.com

The ways of responding to a terrorist encryption

By Milica D. Djekic

The encryption may get a crucially significant point in some communication or information exchange activities. It's not only important to a Defense Force as it may get from significance to some terrorist organizations using cryptography to plan and prepare their attacks. Some terrorist groups may use software tools to protect their sensitive data, while many would rely on hardware solutions which would offer them somehow better level of protection. As it's known, many software solutions may get hacked, but is that the case with the encryption hardware? Through this effort, we would want to analyze how to apply a skillfully prepared state-sponsored attack – that could make it possible to damage some hardware remotely taking advantage over its physical imperfections.

Why terrorist groups use the encryption

Many terrorist groups would use cryptography to protect their sensitive information or communication channels from being breached from the outside. Sometimes encryption software would be enough to protect a certain amount of data, but – would it get resistive to skillfully organized hacker's attacks? Our answer to this question is – no. Once the intelligence community discovers some of machines using the cryptographic tools, it would become feasible to disable such a computer with its entire network.

Also, the current software cryptography would offer many weaknesses such as the encryption keys that should get delivered through the special channels. We know that terrorist may use e-mails, web or even mobile devices to obtain such a confidential information transfer. The intelligence community got its methods to discover the terrorist organizations and their members, while the state-sponsored hackers got plenty of skills and expertise to attack their information sharing systems.

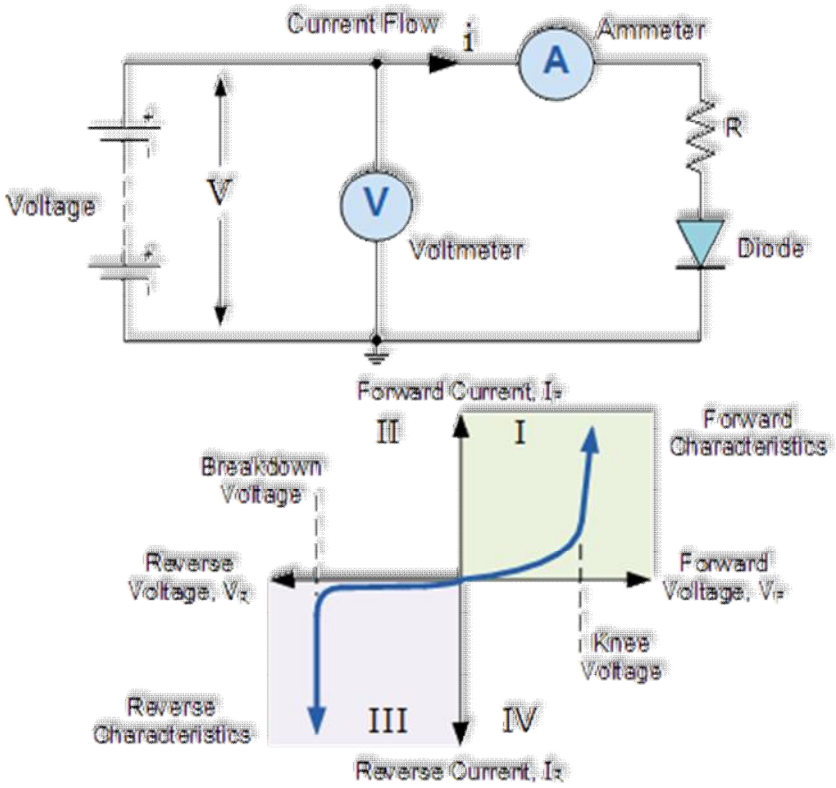
A bit better situation is with the hardware-based encryption solutions. These solutions may appear as the smaller boxes or even computer sticks which would do data encryption and its transmission. It appears much harder to affect such a solution, but the question is – would that be possible?

The experience would suggest that it's not easy at all to break into that cryptographic system, but we would want to suggest that it's not necessary to deal with that protection from the inside or, in other words, send your intelligence agent to a highly risky task – it's simply sufficient to get well-trained staffs with the appropriate technology operating from the outside.

The challenges of hardware encryption

The hardware cryptography would, as we said, include some physical devices being based on a digital technology. Those devices may cover up printed boards or any other micro-packaging technologies. So commonly, in case of skillfully prepared hacker's attacks – it's possible to see the external devices being connected to that computer or its network.

Many times the hackers would try to disable those gadgets, but – is that the case with the encryption equipment which may get some sort of the access control. In a practice, the hardware-based encryption would include some interface software being capable to communicate with the cryptographic hardware.



It sounds like a challenge. Well, basically – it is. Before we explain how complex could be to threaten the well-protected encryption hardware from the outside, we would want to make a brief overview on how digital technologies work in a reality.

The majority of digital systems would use the logic gates and some electronic components being applied for their operations. Those logic elements would include transistors, diodes, resistors, capacitors, integrated circuits (ICs) and so on. So, all of them would be real components being made from the real materials with their physical performances. We would not go deeply into the analysis, but let's say those elements – even being used for the terrorist printed boards – would get their physical limitations.

For instance, they would get considered as a low-voltage circuits and in such a case – the binary 0 would include a range between 0 and 2 V, while the binary 1 would deal with the spectrum from 3 to 5 V. So, it's clear that if we try to apply some electrical network's voltage being between 220 and 230 V in Europe or 110 V in the US – we would definitely cause such an equipment damage.

Let's say that computers and their supporting equipment would use the power from the standard electrical networks as well as many voltage convertors offering them to work within the supposed range.

Finally, we would give some illustration explaining how diodes work and suggesting that it's quite simple to burn them using the amplified voltage.

The physical disadvantages of hardware solutions

So, we would see above that hardware solutions would deal with some physical limitations causing them be so sensitive to the higher voltage. That's practically the point for a reason that even if terrorist groups deal with the hardware-based encryption or not – it's possible once they got located to burn their equipment using the amplified signal.

For instance, if the circuit's diode suffers its current's breakthrough or – in other words, if it gets burned applying the heat which would be the consequence of Joule's law – it would work as a short circuit to the entire solution and produce its destruction.

The concluding remarks

The aim of this review got to provide a closer insight to the challenges of hardware-based encryption especially being used for the terrorist purposes. It appears that our world could be much securer place to live and work in – once we decide to rely on our scientific findings.

That's the reason more to combat terrorism and bring the progress to the entire Human Kind.

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.

6TH SCADA WORLD SUMMIT

Quote
"CYBER DEFENSE"
to qualify for extra
10% discount*!
*discount applicable to 2-day summits.

- Main conference: **9 & 10 November 2016**
- Post Conference Workshops: **11 November 2016**
- Pre-conference Workshops: **8 November 2016**
- Venue: **Kuala Lumpur, Malaysia**

What Makes 6th SCADA World Summit 2016 A Must-Attend Event!

Recipe for Success Hear from **Cross-industry SCADA Professionals and Project Owners** share their experiences in managing SCADA system integration, upgrading and maintenance within an energy efficient environment through various large scale projects globally

Interactive Discussions Join **exclusive panel discussions featuring SCADA industry experts** as they share their challenges and perspectives in eliminating cyber security threat and adopting smart applications to elevate SCADA system operational efficiency

Eye-opening Presentations Gain strategic insights from **over 20 industry experts** on overcoming major challenges in managing SCADA system including **Cyber security risk, complicated SCADA system integration and upgrade, achieving accuracy on real time data acquisition, improving connectivity between MTU and substations, data management and protection, reducing human errors in SCADA operation and amongst others**

In depth Workshops Attend the **6 Expert-Led Pre-Summit Workshops** to grasp the nuts and bolts in achieving effective SCADA system management

Researched & Developed by: EQUIP GLOBAL

Media Partners: GAS, AISA, APSM, Security, CHIEF IT, CSEAN, CDM, GeoConnexion, Gulf Oil & Gas, SGCyberSecurity.com, WorldOils, Global Information, Inc.

PHONE: 65 6376.0908 EMAIL: enquiry@equip-global.com
WEB: http://www.equip-global.com/6th-scada-world-summit-2016

We Have To Act Now To Build A Secure Internet Of Things

The Internet of Things will be transformative, but only if we invest in security now.

The Internet of Things already provides substantial benefits to consumers and businesses. Millions of smart connected devices generate vast volumes of data, empowering businesses to offer innovative new services.

More data means greater insight into and control over everything from manufacturing to marketing.

Over the next few years, the number of connected devices is likely to increase by orders of magnitude — some estimates put the number at 40 billion by 2020.

But many smart connected devices aren't so smart where security is concerned. In fact, the nascent IoT industry has a woeful security track record.

A quick glance at Shodan, a search engine that can find vulnerable connected devices, reveals what's likely to be the tip of the iceberg. Poor IoT security is bad news for everyone, businesses and consumers alike.

Although there hasn't yet been a substantial security breach that can be definitively blamed on the Internet Of Things, it's only a matter of time, as James Lyne, global head of security research at Sophos points out:

> "Very soon, we're likely to see a big breach. It's quite probable that some really shiny, cool, new product is going to come along in the next year which will see massive adoption by consumers and enterprises. When that happens, I think attacker interest will rise"

A major reason for lax IoT security is that businesses simply aren't motivated to invest the time and effort to build secure devices and networks.

In a highly competitive market, IoT device manufacturers are incentivized to compete on price, cutting costs wherever they can.

Security is hard, time consuming, and requires substantial research and development investment to get right — none of which is attractive to a company looking to churn out devices at high-volumes and minimal cost.

> "Consumers do not perceive value in security and privacy. As a rule, many have not shown a willingness to pay for such things. As a result, manufacturers slash costs to maximize their profit, often on narrow margins."

The benefits of the IoT are hard to ignore as an enabler of improved efficiency and productivity for enterprise operations, and as a potential market for consumer- and enterprise-focused products.

The IoT is here to stay, but businesses have to think long and hard about the IoT they want to build.

Enterprise organizations will not deploy smart devices within their networks if those devices can easily be used to compromise them.

No one wants a connected fridge or webcam that could potentially be responsible for a massive data leak.

Enterprise organizations have recognized the seriousness of the problem. Groups like the IoT Security Foundation were created to facilitate cooperation between major enterprise players in the field. Members include Vodafone, IBM, BT, and ARM.

But all the good intentions in the world won't make a lick of difference if companies continue to market ever greater numbers of devices with security flaws that would have shamed a home router manufacturer a decade ago.

The Internet of Things has the potential to be transformative, but only if the enterprise aligns itself with security best practices, even if they result in marginal cost increases.

About the Author

Jamie Madison is the Marketing Director at Steadfast, a leading IT Data Center Service company. Steadfast specializes in highly flexible cloud environments, robust dedicated and colocation hosting and disaster recovery.

North Africa Banking Technology 2016 Exhibition

8-9 NOVEMBER 2016
CAIRO INTERNATIONAL CONVENTION CENTRE

CUTTING EDGE BANKING TECHNOLOGY

50+ PROMINENT MENA BANKERS SHARE THEIR EXPERIENCE AND PERSPECTIVES!

SPEAKERS INCLUDE:

J.P.MORGAN CHASE
Ahmed Afifi
Egypt & North Africa Head - Global Trade & Loan Products

ABU DHABI ISLAMIC BANK
Amr El Zomor
Head Of AML Compliance & Corporate Governance

ABANK
Ahmet Ertan Algan
Unit Head: Digital Banking and Card Payment Systems

COMMERCIAL INTERNATIONAL BANK, EGYPT
Mohamed El Sabban
Group Head, Digital Banking, Consumer Banking Group

SECURE YOUR COMPLIMENTARY PASS NOW

WWW.NORTHAFRICABANKING.COM

Sponsors: Infosys Finacle, wacom BUSINESS SOLUTIONS, Profile Software, Login

Media Partner: CDM CYBER DEFENSE MAGAZINE

For more information contact:
Kaleesha Rajamantri
+44 207 111 1615
kaleeshar@irn-international.com

Organised by: irn International Research Networks

ThreatQuotient Enters Middle East IT Security Market Through Partnership Agreement with Help AG

As a fully certified Gold Level Partner, Help AG will now deliver consultancy, implementation and support services for the ThreatQ threat intelligence platform to large enterprises across the region

Dubai, United Arab Emirates- 04 September, 2016: Help AG, a leading information security services and solutions provider in the Middle East, today announced the signing of a reseller agreement with ThreatQuotient.

As the vendor's first regional partner, Help AG has achieved the Gold Partner status under ThreatQuotient's Threat Alliance Program (TAP) and will offer the ThreatQ threat intelligence platform to enterprises looking to augment their Security Intelligence and Event Management (SIEM) capabilities or build their own Security Operations Centers. Help AG will also utilize the platform for its own 24x7 Managed Security Services (MSS) offering.

"In recent years, even large organizations with significant IT security investments have been falling victim to data breaches that disrupt business, cause the loss of sensitive company data that ultimately results in irreparable damage to their brand. This makes threat intelligence a critical element of a business's security posture," said Stephan Berner, CEO at Help AG. The benefits of threat intelligence are widely backed by the IT security community.

As a case in point, recent research by the Ponemon Institute found that 80% of IT decision makers whose organizations suffered data breaches believe having threat intelligence at the time of the breach could have prevented or minimized the consequences of the attack .

The focus of the agreement is on enterprise-sized customers and Help AG intends to offer ThreatQ to organizations from the Banking and Finance, Government, Oil and Gas, Retail, Telco, and Media sectors.

ThreatQ centrally manages and correlates unlimited external sources with all internal security and analytics solutions for contextual and operationalised intelligence in a single view. As a result,

ThreatQ enables threat intelligence teams to shift their focus to analysis, and improve their security operations by reducing the amount of effort traditionally exerted into combining data sources.

As part of the partnership agreement, Help AG was required to have a team of security analysts with a keen understanding of incident management methodology and best practices such as SANS.

The reseller's Managed Security Services Analysts, Implementation Engineers and Support Engineers have been fully trained and certified on the product and will deliver consultancy around ThreatQ starting from implementation to advanced services like integrations and support.

Commenting on the partnership, Berner said, "ThreatQuotient was a natural choice for Help AG.

Having worked in the SIEM space for the last decade and spoken to a lot of customers facing challenges in terms of responding to security incidents,

Help AG was looking to partner with a company that had insights into how security incidents should be handled and responded to.

We conducted thorough evaluation on similar products and ThreatQuotient stood out from the crowd as adoption of SANS best practices was inherent to their solution.

ThreatQ's seamless integration with major SIEM solutions, advance persistent threat solutions and the likes were also some of the deciding factors."

"Moving forward, threat intelligence will be a deciding factor in the success of many cyber security strategies and it is vital that organisations are staying ahead of the curve by actively looking at how they improve communication, operationalise threat intelligence and manage risk.

Help AG is an expert at bringing new, best of breed solutions to market in order to help its customers. It has an excellent reputation as a leading cyber security services and solutions provider in the Middle East.

We are absolutely delighted to form this strategic partnership with Help AG," said Anthony Perridge, Regional Manager EMEA at ThreatQuotient.

About Help AG

Help AG is a leading IT security solutions, services and consultancy company, founded in Germany in 1995 and active in the Middle East since 2004.

A winner of multiple reseller, partner and channel awards, the Company was even recognized in 2013 as one of the Top 100 SME businesses by Dubai's Department of Economic Development (DED).

Focusing solely on the security aspects of Information Technology and maintaining an unprecedented 80% of staff in technical positions has enabled Help AG to stand out as the region's trusted advisor capable of delivering the most complex and innovative IT security solutions spanning Application Security, Network Security, Enterprise Mobile Security and Next Generation Modern Malware Protection.

This unmatched technical expertise has enabled Help AG to establish a dedicated Security Analysis division offering customers Security Review, Penetration Testing,

Configuration Architecture Review, Vulnerability Assessment and Social Engineering and Exploitation services.

As a key player in the security arena, the company remains dedicated to raising regional awareness about IT security threats and trends and regularly conducts informative vendor-agnostic events such as its flagship Security Spotlight Forum (SSF) and CIO Circle of Trust. More information is available at: http://www.helpag.com

About ThreatQuotient

ThreatQuotient provides ThreatQ, the only Threat Intelligence Platform (TIP) that centrally manages and correlates unlimited external sources with all internal security and analytics solutions for contextual, operationalised intelligence in a single pane of glass.

ThreatQ is also the first TIP to provide Indicator Nurturing, which goes beyond enrichment to help customers tailor indicators of compromise (IOCs) more specifically to their infrastructure: https://www.threatq.com.

Media Contact:

Ian Saldanha
Procre8

Tel: +97155 450 6073

Email: ian@procre8.biz

Paula Elliott
C8 Consulting

Tel: +44 1189 497736

Email: paula@c8consulting.co.uk

CI CONNECT

Cyber Security Connect North America

Nov. 15, 2016 | Marriott at Metro Center | Washington, DC

An Invitation-Only Forum for Senior Executives in Cyber Security across North America. Hear from industry experts, including:

Nickolas Savage
Supervisory Special Agent (SSA)
Federal Bureau of Investigation (FBI)

Vivek Khindria
Director, Information Security
Bell Group of Companies

Jon Boyens
Senior Advisor for Information Security and Program Manager, ICT Supply Chain Risk Management, **National Institute of Standards and Technology (NIST)**

Drew Morin
Director, Federal Cyber Security Technology and Engineering Programs
T-Mobile US, Inc.

Rob Fry
Senior Security Architect
Netflix

Richard Starnes
CISO
Kentucky Health Cooperative

TO APPLY, PLEASE VISIT: **CanadianInstitute.com/Cyber**

How Cyber Criminals Can Steal The Election

There has never been anything quite like the 2016 presidential election. More than any other election in history, the campaign has been waged online, via Twitter and other forms of social media. And the electorate has never been more online, too.

Today, with more than 60% of U.S. adults getting accessing news via social media, this election is far more susceptible to social media monkey business than ever before

In 2016 alone there have been numerous examples of online "dirty tricks," online activity by fraudsters and activists that spread messages designed to confuse or mislead the electorate.

These malevolent activities can be generally grouped into the three categories

- Criminals or activists using online schemes to leverage the election for personal profit
- Political operatives taking advantage of social media to distort information or distribute unfavorable information
- Online actions designed to decrease public trust in the election's process or eventual validity

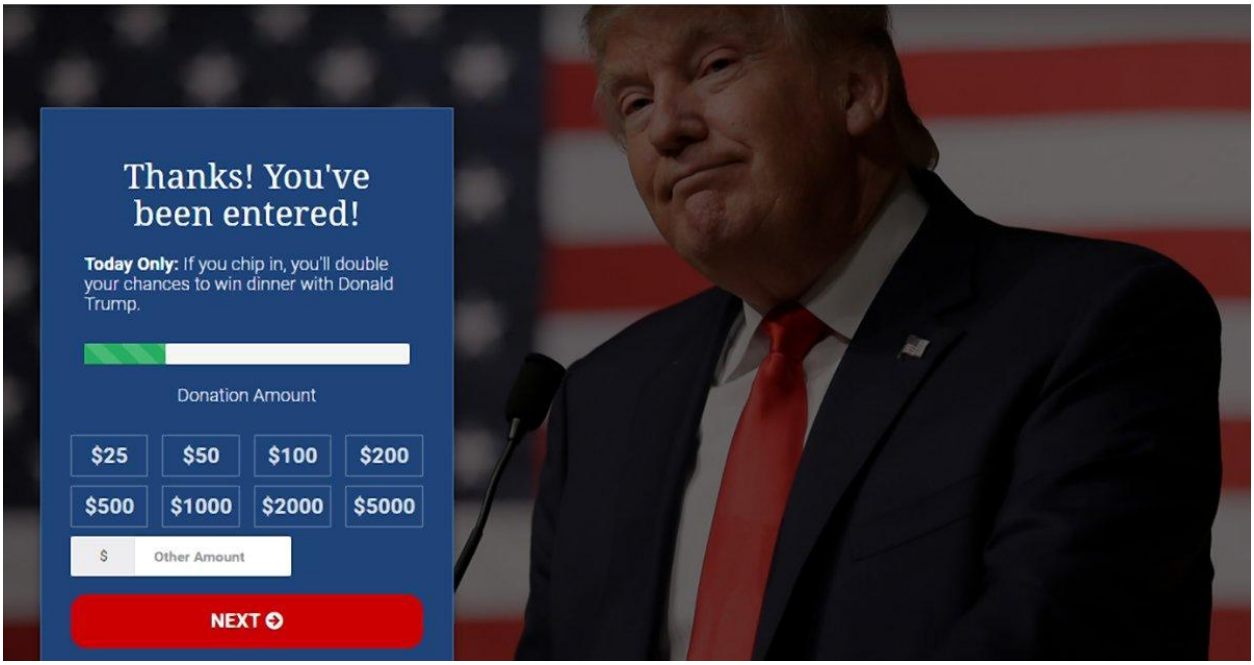
How do the personal profit schemes work? They work the same way a scheme targeted at a trusted corporation or institution – though impersonations, rogue emails, fake social domains, and duplicitous websites.

The election of 2016 has seen numerous online impersonations of both candidates. During a BrandProtect study of Election Social Fraud, we discovered hundreds of domains impersonating candidates, and a similar number of twitter handles.

The Trump campaign is most frequently targeted by fraudsters. We counted almost one hundred copycat Twitter handles, each with a small number of direct followers, but all of them active.

Many of these fake accounts tweeted out a mix of official campaign communications, interspersed with links to porn sites and malware/ransomware. Though these fake accounts may not have a lot of followers, their most outlandish posts have the potential to go viral, or even semi-viral, leaving behind a trail of compromised readers.

The prize for most creative rogue online activity goes to Ian Hawes -- the man behind the infamous dinnerwithtrump.org, a website that looked like a legitimate Trump campaign website, complete with America flags and iconic photographs of the Republican presidential candidate.



The site promised members of the public the chance to win a dinner with Donald Trump, and offered them a chance to make monetary donations to the cause. But according to Politico, the site was not what it appears to be.

Although fine print outlined the site's real purpose, the DinnerWithTump site was so convincing that Hawes reportedly convinced hundreds of individuals into making more than a million dollars of contributions.

There is no telling where those contributions went. What's worse, as part of the scheme, these unfortunate victims have submitted their personal information to Hawes, arming him with valuable data for future exploits.

Not surprisingly, the Trump organization fought back and is engaged with a war of words and legal notifications with Hawes. The campaign reported that it is "concerned about the likelihood of confusion among the public" because of American Horizon's use of "Trump's name, image, likeness, or slogans in connection with soliciting contributions and conducting other activities."

This is a distraction for the campaign, a drain on campaign resources, and a siphoning of cash contributions intended to support the Trump campaign. [Note: the dinnerwithtrump.org site has been removed, and the Dinner with Trump contest has been taken down. The associated Super PAC website managed by Mr. Hawes -- https://americanhorizons.org/ remains up]

Though this kind of online fraud does impact the election, its impact is relatively small. The primary goal of these schemers is to steal "from" the election. But others are thinking bigger. A short-term monetary gain doesn't interest them. They want to actually steal the election.

There have been many reports, stories and investigations about hackers – even some shouting about nation-state-sponsored-hackers – who might try to penetrate the actual apparatus to influence or steal the U.S. Presidential Election.

As everyone now knows, thanks to Bush v. Gore in 2000, the margin of victory can be a hanging chad, the threat of external vote manipulation needs to be taken seriously.

Thanks to the Bush v. Gore vote counting issues, the majority of states have long since implemented electronic voting procedures, citing their more accurate and timely counting. But there is a trade-off. An all-electronic system could be hacked – some of the e-voting systems run on older, less secure operating systems, like Windows XP(!).

Without a paper ballot to ultimately serve as an auditable record of the voting, the U.S. Election could turn on electronic results that cannot be audited. Should this make us nervous about the integrity of the election? Probably not, for two very important reasons.

First, only a few states use all-electronic systems that have no paper component at all. About three quarters of the states employ a hybrid system where paper ballots are marked but are counted electronically, or a pure paper system. In those states, there is always a paper ballot to back up each electronic vote. In those states the results can be carefully audited and confirmed.

But to steal the election by altering the votes, fraudsters would need to concentrate their efforts on the swing states – Florida, Pennsylvania, Ohio, etc. – the states where the races could go either way.

Of those states, Pennsylvania is probably the most vulnerable to election hacking – they have the most complete electronic voting implementation.

In many parts of Pennsylvania, there are no auditable paper ballots, only electronic ones. But the risk of vote alterations is low. Even without a paper ballot audit there is plenty of other data, exhaustive pre-election polling and day-of-election exit polling that will quickly provide election watchers with corroboration that the voting counts reflect the will of the people.

Short of vote manipulation, targeted cyber exploits could also disable voting, or slow voting procedures, creating chaos on election night.

Long lines at polling places reduce turnout. By strategically targeting polling places for “slow-downs” hackers could theoretically reduce the election-day turnout for any district or demographic they wanted.

But in 2016, according to most projections, almost half of votes in the presidential election will be cast early, or cast by mail, bypassing polling place lines. In some highly contested states, the percentage of early votes might approach or even exceed seventy-five percent.

So stealing votes or trying to slow or stop election-day voting in certain districts is not very likely to alter the election. Especially across the Presidential and Congressional races there is just too much scrutiny and knowledge about the way the voting works, making it very difficult to manipulate the elections this way.

The mostly likely way a third party could try to steal the election is not by altering votes that have been cast, but by actually convincing people to cast their votes differently. Hackers and political activists will try to create what politicians and political writers call an “October Surprise.”

For example, consider the effect that damaging or embarrassing information can have on a candidate.

By timing the release of damaging information correctly, election-stealers can try to influence the electorate in the last moments before they cast their votes. To a degree, this kind of activity has always been a part of the election process. What is different now?

In today’s email-centric and social media-driven world, exploitable information is saved electronically, which makes it vulnerable to attack and compromise – it is only a hacked email account or server away from exposure.

It is already happening.

The recent DNC email hack, released through WikiLeaks, revealed compromising information about the Democratic Party leadership’s private views of the Clinton and Sanders primary campaigns.

Although this information had been stolen many months before, WikiLeaks chose to release the information just hours before the start of the Democratic National Convention, when it would have maximum effect on the final nominating process.

The result? A chaotic opening to the Democratic National Convention. WikiLeaks has promised that they have more information to be released. Look for that news in late October!

But even without compromising information, third-parties can wreak havoc on the electoral process.

Think back to Tuesday March 1, 2016 -- “Super Tuesday.” On this day, Democratic voters across eleven states and territories would vote between Hillary Clinton and Senator Bernie Sanders.

During the prior weeks, the Sanders campaign was capturing headlines and igniting populist enthusiasm. The Sanders campaign desperately sought a legitimizing event, an event that could change the trajectory of their campaign.

At the same time, establishment Republicans were eager to slow down the Clinton campaign, with several Republican insiders preferring that Sanders would best Clinton in the Super Tuesday primaries and possibly in the primaries overall.

A key figure in the developing drama was Massachusetts Senator Elizabeth Warren. Warren, a popular, vocal champion of the left, had carefully walked a fine line between the Democratic candidates, conspicuously withholding her endorsement for either Clinton or Sanders.

She wasn't afraid to speak her mind about the issues in public, disagreeing with several Clinton policies, while tacitly supporting elements of the Sanders platform. It was understood that either of the candidates would benefit greatly from a Warren endorsement, and Senator Warren was waiting for the right moment to make her announcement

Midday Monday, Feb. 29, less than 24 hours before the Super Tuesday voting would begin, this news story, apparently from The New York Times appeared in social media posts.

POLITICS | Christie Splits With His Past in Backing Trump

Warren Endorses Sanders, Breaking With Colleagues

By JONATHAN MARTIN and ALEXANDER BURNS FEB. 29, 2016

Sen. Bernie Sanders of Vermont and Sen. Elizabeth Warren of Massachusetts on Capitol Hill Monday.
Cooper Neill for The New York Times

Email

Share

WASHINGTON, D.C. -- In a potentially decisive turn for the Democratic race, Sen. Elizabeth Warren (D-MA) has endorsed her colleague, Sen. Bernie Sanders of Vermont, in his campaign for president. Until now, not a

The "article" was seemingly penned by respected NY Times political reporters Jonathan Martin and Alexander Burns, and included quotes from Ms. Warren, Senator Barbara Boxer of California and the actress Lena Dunham.

It was a strong article, powerful, game-changing news, news that could profoundly affect voters who would cast their primary ballots the very next day.

But it was fake -- a high-quality fake -- an accurate clone of the distinctive NY Times style, right down to the embedded adds. To add to the story's "legitimacy" it was hosted on a copycat domain, one that could easily be confused for the legitimate www.nytimes.com domain.

For about three hours, the story went viral, achieving 50,000 views and 15,000 shares. The story was building momentum so quickly that the NY Times was forced to make a statement, disclaiming the story, and reiterating that Senator Warren has not endorsed either candidate.

A simple prank? It doesn't seem so. The use of a dedicated website host that mimicked the NY Times domain took careful planning.

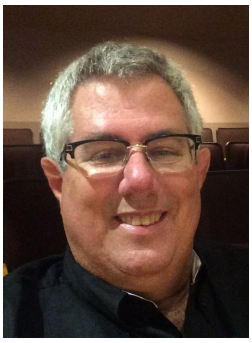
The very next day, Clinton was 7 states and 486 delegates while Sanders claimed 4 states and 321 delegates. Were these results altered by voters who might have been exposed to the rogue story? Was the Sanders campaign the recipient of a "boost" from voters who saw and believed this story? We will never know…

Election Day is coming. What will actually happen? I don't know. As you read these words, the activists and criminals who want to steal the election will be preparing to launch their final exploits.

It could be an attack on voting systems, or it could be the publication of real OR fictitious news that tries to damage the candidates and cause their supporters to break with them.

The only thing you can be sure of is that there will be something. In fact, there will be many things. When the stakes are the highest, the cyber criminals get the most creative. Get ready.

About the Author



Greg Mancusi-Ungaro is the chief marketing officer for BrandProtect, a leader in cyber threat monitoring, intelligence and mitigation services.

He is a frequent author and speaker, and a constant evangelist on cyber security issues, the changing nature of the modern threat landscape, and the emerging technologies that look beyond the perimeter to drive enterprise defenses against cyberattack.

He blogs regularly on cyber threat and cyber security at info.brandprotect.com.

CELEBRATING 25 YEARS OF SUCCESS

"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 Exhibitors | 30 Countries | 150 Speakers from World over | 20,000 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
• Convergence India Excellence Awards • 2nd SCTE India Awards
• Start-ups Showcase • Mobile Devices & Accessories Zone

Co-located Expo

Internet of Things India expo 2017

Convergence • Connecting • Convenience

Support

Department of Electronics & Information Technology
Ministry of Communications & Information Technology
सत्यमेव जयते Government of India

Media Partner

CDM CYBER DEFENSE MAGAZINE

Organiser

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

Phishing Mitigation Must Go Far Beyond Employee Education

By Eyal Benishti, founder and CEO, IRONSCALES

Around the world, phishing attacks have evolved from a matter-of-fact nuisance into an epidemic in which enterprises, on average, spend $4 million per event to remediate. Perpetrated by every type of cyber criminal, from nation state threat actors and hacktivists to script-kiddies and fraudsters, phishing now accounts for 95 percent of all successful cyber attacks worldwide.

In the first quarter of 2016, phishing attacks surged by 250 percent - the highest ever since 2004 - according to the Anti-Phishing Working Group (APWG). These attacks have had the power to victimize millions of W2 employee data records, for example, in large enterprises like Time Warner Cable, healthcare networks, and insurance companies, among others.

Further, ransomware, a type of malware used in 86 percent of phishing attacks in which access to a computer system is blocked until a sum of money is paid, continues to be an increasing threat perpetrated by more determined and aggressive attackers. According to APWG co-founder and Secretary General Peter Cassidy, "The threat space continues to expand despite the best efforts of industry, government and law enforcement." With a record number of phishing-related cyber attacks this year already, enterprises must call to question whether their current phishing mitigation efforts are effective. Most likely, they are not.

The Phishing Band-Aid

Traditional phishing defenses were centered on email filters and anti-virus software, but organizations soon realized that these solutions were ineffective. The current phishing fix – or attempted fix – has centered on human intelligence, or the belief that extensive training can transform ordinary workers into hyper-vigilant phishing detectives.

However, the jury is still out on the effectiveness of employee education. According to the most recent IBM Security Officer Assessment, "95 percent of information security incidents involve human error." In other words, some employees will simply never learn the consequences of opening a malicious email or downloading a suspicious attachment. Additionally, the average 1000-person company saves only 10 percent of attack losses as a result of "substantial training and security awareness activities," according to the Ponemon Institute.

When searching 'phishing mitigation' or similar phrases online, countless articles and organizations that promote employee education appear in the top results. Yet, with malware, bots, spamming and spoofing proliferating in frequency and sophistication, organizations must realize that, while important, education and training alone is simply not enough.

While employee education will continue to play a roll in mitigating phishing attacks, because of the intrusiveness of employee training, the reliance on employees to report attacks, and the burden put on security operations center (SOC) teams to remediate attacks, organizations that rely solely on employee education are likely to remain a primary target for phishing attacks.

The Automation Advantage

In today's threat landscape, the time from phishing attack discovery to complete remediation must be measured in minutes or hours, instead of the current standard of days and weeks. In some instances, employee training may result in immediate attack discovery, but the attack will remain persistent until the SOC team gets involved. Nonetheless, with so many security issues to investigate and analyze, SOC teams are typically unable to meet the real-time attention demands that suspicious emails now require.

Fortunately, advances in cybersecurity have led to the engineering of automation that, through machine learning, can automatically respond to suspected phishing emails upon discovery. With automation, enterprises can exponentially reduce risk by allowing any employee, based on his or her proven awareness level – from the janitor to the CEO – to quarantine and remove suspicious emails with just one click of a button. By doing so, companies can significantly limit the time in which malicious emails reside in the inboxes of employees and lessen the SOC team's workload by reducing the manpower needed to analyze suspected attacks.

For some security professionals, however, company executives and board members, the concept of an automated response is unnerving. To many SOC teams, automation implies that an abundance of false positives are imminent. Some in leadership positions argue that the automatic quarantining of emails, without verification of malice, could be perceived as intrusive. Additionally, many in IT speculate that automation is simply too difficult and costly to integrate with business applications, such as Office 365 and Gmail.

The question for enterprises is this: are existing concerns about automated phishing mitigation enough to prevent them from adopting technology that can expedite the time from attack to remediation to just minutes and reduce the risk of falling victim? For any company that's fallen victim to a phishing attack – the answer is likely no.

Ultimately, no amount of employee education will be sufficient enough to halt the global phishing epidemic, but by adding automation into the mix, enterprises may finally have a fighting chance.

About the Author

Eyal Benishti is the founder and CEO of IRONSCALES, the first and only multi-layered phishing mitigation solution to combine human intelligence with machine learning. He can be reached at Eyal@ironscales.com.

INDONESIA EDITION

ANALYTICS LEADERS SUMMIT 2016

PREDICTING CUSTOMER BEHAVIOUR THROUGH ANALYTICS

19 - 21 OCTOBER 2016 | KEMPINSKI HOTEL JAKARTA, INDONESIA

LISTEN TO THE INDUSTRY EXPERTS

ANALYTICAL PROFESSIONALS ATTENDEES

A 2-DAYS CONFERENCE PLUS A 1-DAY WORKSHOP ON MACHINE LEARNING

ORGANISED BY:

ENIGMA CG
CONSULTING GROUP

3 EASY WAY TO REGISTER

Give us a call at +6032181 7111 ❶

Drop your enquiry to Soraya Sohaimi | soraya@enigma-cg.com ❷

Enquire online at www.enigma-conferences.com /analytics-leaders-summit-in-indonesia ❸

To fight cybercrime effectively, understand the new business model

By Tom Gilheany, project manager, CISSP, Cisco Systems

Malware as a Service? Now that's a nightmare.

Yet MaaS is available—for a fee, of course—for those who know where to look for it and have nefarious reasons to want it.

Welcome to the wild new world of cybercrime organized very much along the lines of legitimate business. Once upon a time, enterprises may have thought regulatory compliance was enough to keep sensitive information safe. Not anymore.

The business model of cybercriminals has evolved in the last few years, and companies that remain unaware and thus fail to keep up will find their data and other precious information assets are vulnerable in ways that cost them dearly.

Back in the early days of the Internet, cybercriminals needed to know how to control, implement and perform the entire theft process. They gained access to machines and identified useful resources.

Then they sold and monetized those secrets. These days, however, they can outsource expertise to contractors who specialize in expertise that includes infiltration, social engineering, malware customization and the sale or brokering of stolen information or access.

Criminal enterprises are leveraging a global network of technical specialists in hard-to-extradite or hard-to-prosecute places, and paying them in hard-to-trace digital currencies. In a few instances, their part in the overall crime they are committing may not even be illegal in their jurisdiction.

With teams dispersed worldwide and specialized division of labor, it is tough to track the entire crime to compile a comprehensive evidence file.

Cybercrime's business-like structure

Criminal organizations nowadays uncannily resemble their legitimate counterparts. They use many of the same tools and are motivated by many of the same factors as regular businesses, with a fraudulent twist. They seek to:

- **Cut their risk**. Criminal enterprises want to lower their operational risk, the same as any other organization. So they use tools such as Tor to gain anonymity and encryption to protect their transmissions from prying eyes, competitors, law enforcement or intelligence agencies.

  Moreover, widespread remote access enables them to manage multiple operations remotely, sparing them from an onsite presence that exposes them to greater risk.

- **Increase efficiency**. Regular enterprises use economies of scale and scope to reach a large number of customers. Hackers use the same to contact a greater number of victims and boost the quality of information they attain.

- **Exploit social intelligence**. Recruiters uses social media to gain background on job candidates. Criminals use it to gather intelligence about their targets.

- **Benefit from contractor competition**. Criminals gain by hiring team members and business partners from a global pool of specialists, who vie with each other for their business.

- **Bank online.** Online transactions make it easier to transfer wealth between jurisdictions using hard-to-trace cryptocurrencies.

- **Offer crime as a service.** Market specialization exists in cybercrime, from botnet rentals to services for hire. Criminals can buy or design custom malware solutions tailored to their desires and needs.

Cybercriminals locate the preceding products and services in much the same manner as do consumers. They go online and look for them among plenty of options.

Gray and black marketplaces hawk malware, DDoS botnets, ransomware kits, malware-as-a-service (delivered from a cloud-based platform), and stolen data are all for sale somewhere.

Like any laissez-faire market, these shadow economies have set prices for specific pieces of data: a Social Security, credit card or bank account number all command different prices.

Many private citizens don't prioritize hardened security on home computers, assuming that they have nothing of valuable to hackers. They are mistaken. Just like in any economy, if a commodity has value and can be commoditized, it will be.

Even those who don't keep any sensitive data on their machine may find that it can still be remotely seized and used for a rogues' gallery of purposes.

Among other things, it can be used as a remote phishing or gambling server, or as part of a botnet engaged in clickbait fraud or spewing out spam messages.

Cybercrime as a profession

When considering information security, legitimate enterprises can no longer afford to ignore the emerging cybercrime business model. It is now far more sophisticated and leads to a number of the following kinds of nightmarish scenarios:

1. An engineer calling the tech support hotline to ask about customizing some off-the-shelf software his organization has just bought. That off-the-shelf software? A ransomware kit.

2. A call center employee logging into her call management database, opening her script and picking up the phone to make the first call of the day. She and her colleagues are posing as bank employees to trick consumers out of their financial information.

3. The manager of a manufacturing plant sitting down with a client to review the blueprints of a new part. The manager suspects that the blueprints are stolen, but doesn't care. His plant produces legitimate and counterfeit products side by side.

4. A hacker monitoring an online marketplace, waiting for the stolen account information from a breached bank to upload. This is a cybersecurity engineer who is tracking how this underground marketplace is disseminating stolen data.

Cybercrime as a profession has vastly increased its efficiency, scale, and scope. As a result, its impact on legitimate enterprises and economies has risen as well. This creates a compliance challenge for industries, executives, IT departments, operations departments, auditors and regulators.

While it is easy to focus on compliance with regulations and standards, it's difficult for regulators themselves to keep pace with the rapidly evolving cyber security landscape. As a result, even perfect compliance is typically insufficient for true security.

Executives and management must read beyond the compliance report and develop defenses against the latest threats.

Beyond compliance to comprehensive security

It's time to use awareness of the organization as a tool to think and act beyond simple regulatory compliance.

Organizations must identify what assets criminals will go after, understand how criminals monetize crimes and use stolen assets, and finally perceive the resulting impact on their daily business.

The following tips can help enterprises down the right path:

- Think like a cybercriminal. Perform internal audits to identify the most valuable organization assets most likely to be hijacked and monetized by online thieves.

- Deploy security to protect assets with widespread visibility.

- Hire staff and train current employees so they possess the skills to recognize security threats (both potential, and when they occur).

- Make security part of everyone's job description. Task the non-IT part of the organization to notice anything suspicious and report it to the security team.

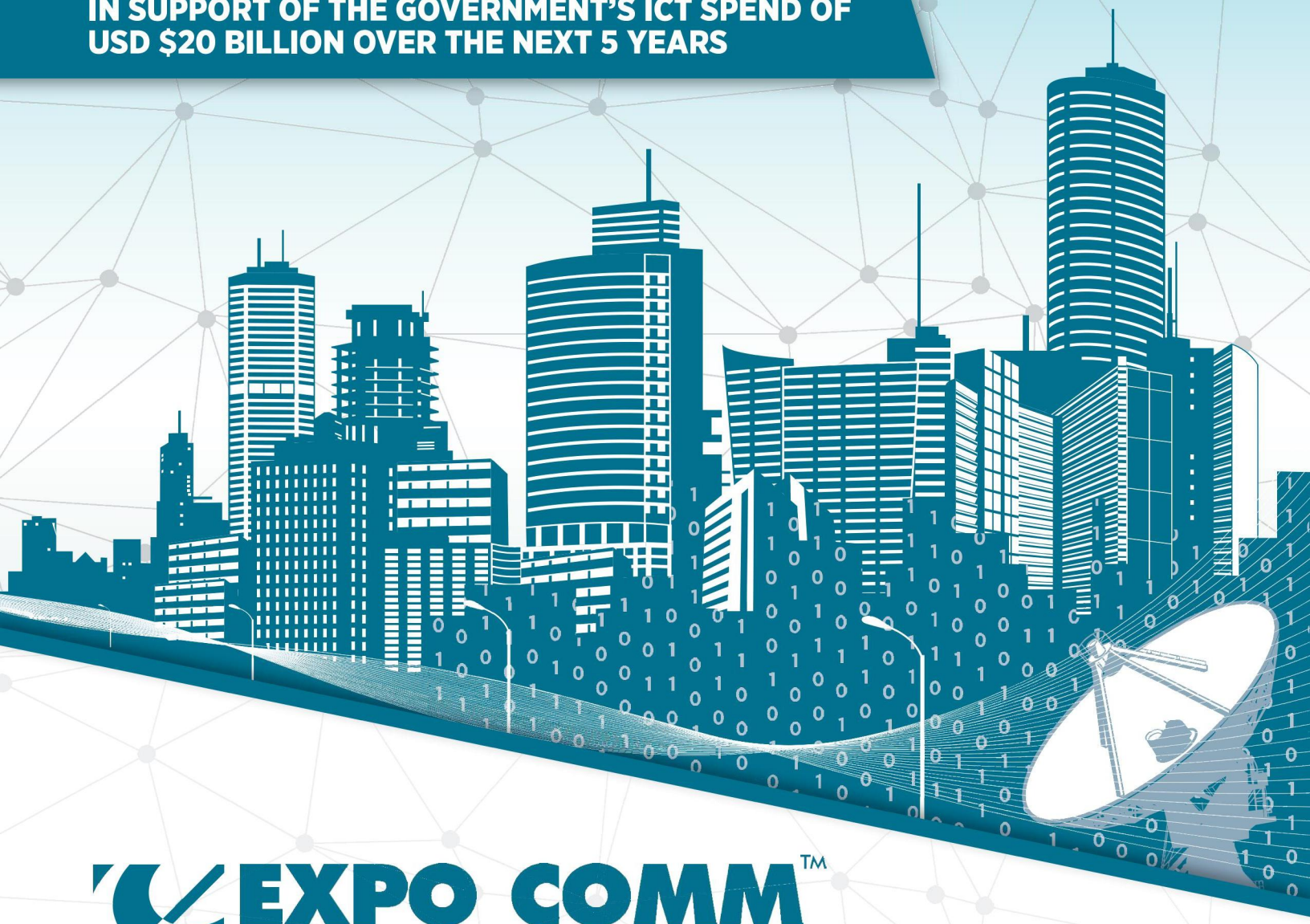
Being mindful of regulatory issues is simply a first step. Really understanding the risks and which assets are the real targets is a far larger and more complicated issue. Companies may think they are covered because they have a security team. However, businesses must describe as specifically as possible the data and systems at risk and the job roles necessary to cover these bases. This is an important part of protecting the entire enterprise.

Cybercrime as a professional is not as captivating an image as that of a rogue hacker lurking in a basement compound. High-level insight into the methods, procedures, approaches, and goals of cybercriminal organizations, can help legitimate organizations focus on the specific data and systems they must protect. Using this information to deploy security technology and train staff to defend the data and systems most targeted by cybercriminals, enterprises can make the smartest, most strategic and effective use of their resources.

About the Author

Tom Gilheany is Cisco's Product Manager for Security Training and Certifications. He has a diverse background in startups through multinational Fortune 100 companies. Combining over 20 years of product management and technical marketing positions, and over a dozen years in IT sand Operations, he has conducted nearly 50 product launches in emerging technologies, cybersecurity, and telecommunications. Tom holds a CISSP, an MBA, and is an active board member of the Silicon Valley Product Management Association and Product Camp Silicon Valley.

IN SUPPORT OF THE GOVERNMENT'S ICT SPEND OF USD $20 BILLION OVER THE NEXT 5 YEARS



EXPO COMM™ INDONESIA 2016

BROADBAND – CYBER SECURITY – SMART CITY INFRASTRUCTURE

9-11 NOVEMBER 2016 | JAKARTA CONVENTION CENTER

DELIVERING SMART SECURE CITIES THAT ENABLE OUR DIGITAL ECONOMY

Hosted by

- Ministry of Communications and Informatics
- ASOSIASI PENYELENGGARA TELEKOMUNIKASI SELURUH INDONESIA — Association of Indonesian Telecommunication Providers

Supported by

- KADIN INDONESIA — Indonesian Chamber of Commerce and Industry
- Coordinating Ministry of Economic Affairs
- WANTIKNAS Dewan Teknologi Informasi dan Komunikasi Nasional — National ICT Council
- APEKSI — Association of Indonesia Municipalities

Sponsored by

- Telkom Indonesia — the world in your hand
- ARIM Technologies

Organized by

- infrastructure asia
- Tarsus

Co-Organized by

- EJK E.J. Krause & Associates, Inc.

Media Partner

- CDM Cyber Defense Magazine

WWW.CONNECTINDONESIA.NET

PART OF Indonesia Infrastructure Week

The Eruption of Ransomware as a Service

By Marc Saldana

Ransomware has been an ongoing and active threat in the cybercrime landscape since late 2013, and is continuing to grow at a rapid pace. First, ransomware tried to trick victims into thinking that not paying would bring about legal consequences besides just loss of data. Now, the authors of ransomware are more transparent, openly saying that the victim has been hacked.

Ransomware as a Service (RaaS), a variant of ransomware, is a data kidnapping distribution scheme in which an attacker encrypts a victim's data. In order to receive a decryption key, the victim needs to pay a ransom, often through Bitcoin. Sometimes, the data is set to be deleted after a certain time period to speed up the payment of the ransom.

What makes RaaS so concerning is that Ransomware authors offer on-demand versions that even the most novice distributor who lacks any kind of technological skillset can deploy. The distributor simply downloads the malware, infects a computer system and then sets the ransom.

Ransomware is usually offered to distributors for a minimal price. The reason the cost to the distributor is so low up front is because the malware author gets their share of any ransom paid. The average ransom is hundreds of dollars, so both the distributor and the author benefit from this setup.

With virtually no technical skills, anyone could be a Ransomware distributor, which presents a big problem for businesses and end users who do not take the proper precautions to protect themselves and their data.

How to Spot RaaS

RaaS is distributed in several ways. The most common method of distribution is as an attachment to a phishing email. Clicking on phishing emails is the number one way networks are infected, data is stolen, and network equipment is damaged. In addition, malicious websites and advertisements can infect the victim's computer.

That's why it is important to train your employees on how to spot RaaS so that they don't become victims of an attack.

Cybersecurity training can educate employees about the dangers of clicking on links within phishing emails, visiting malicious websites, and downloading or installing malicious, non-approved software that can compromise data and the network.

In order to prevent damage and exposure of sensitive data, make sure employees are trained to recognize the signs of a scam.

How to Protect from Ransomware

Ransomware can be costly and time consuming to remove. But with minimal extra effort, here's you can defend yourself and your data from potential threats.

1. Make sure you have backups of all your information. The best way to do this is with removable media, such as an external hard drive (which you should store disconnected from your computer), or through a cloud backup service.
2. The individual has the ultimate responsibility for the links that he or she clicks on or the files that he or she downloads.

   Always be certain that the link or file is from a safe and trusted source.

   Be careful; many sites have "Download" buttons, and only one of them is the right one. If you are unsure about a link or file, always contact an IT Specialist before opening it.
3. Be sure you have an up-to-date Anti-Virus program running on your computers and mobile devices.

   An Anti-Virus program can block the installation of malicious files even if they are inadvertently downloaded.
4. Create volume shadow copies on Windows file shares, setting a max size so as not to run out of space, and keeping copies for at least three months.
5. Keep all operating systems up to date with patches.
6. Ensure you have a robust firewall in place. Geo-block IPs from countries such as Russia and China. Block known malicious TOR IPs.
7. Create and maintain a good Spam filter for email. The filter can be set up to block emails with certain kinds of attachments, such as .exe, .rar, and .vbs files.
8. Make sure the permissions for access to shared drives are tightly controlled. Only give access when needed.
9. Set up Group Policies:
   a. Restrict applications from running in appdata directories
   b. Block executables from running in compressed files
   c. Disable Auto Play
   d. Disable Office Macros

If You Are Infected:

- Don't pay the ransom, unless you have not followed the above suggestions.
- You can restore your operating system to an earlier restore point before the computer was infected.
- You should be able to recover any files from external or cloud backups.
- After restoring files, ensure that your operating system and all Anti-Virus programs are up to date.

RaaS can be costly and time consuming for any business or individual user. And cybercriminals are taking advantage of how easy it is to spread this software around. But with some common sense practices in use, you can protect yourself from ransomware attacks and save your money and your time.

About the Author

Marc Saldana brings more than 28 years of experience supporting the Department of Defense (DoD) and the Intelligence Community (IC) as both a member of the U.S. Navy and a government contractor. His deep and varied professional background includes positions such as: Cryptologic Technician, Sr. Security Analyst, Computer Network Defense Engineer, Computer Network Defense Service Provider (CNDSP) SME, Lead Technical Trainer, Network Defense Watch Officer, Information Systems Security Manager (ISSM) and others. Marc is a service-disabled veteran who served 14 years in the U.S. Navy. His military assignments included diverse roles such as Leading Petty Officer, Information Security System Manager, and Certified Instructor. As a civilian, his experience and background have led him to opportunities supporting operations at distinct, globally-dispersed teams providing critical information technology services to various client organizations, including the Join Task Force-Global Network Operations (JTF-GNO), Counterintelligence Field Activity (CIFA) and currently, Cyber Defense Solutions, LLC. Marc has a degree in Technical Studies (Computer Technologies). He has a CISSP and is certified by the U.S. Navy as an Instructor and Information Systems Security Manager.

About CDS

Cyber Defense Solutions LLC (CDS) is a full-service information technology (IT) company known for cutting-edge cyber security solutions that tackle the most complex tasks. As a Service-Disabled Veteran-Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), and Minority-Owned Business (MOB), CDS is committed to providing government customers with flexible technology solutions and services for today's complex cyber threat landscape. CDS' Cyber Training Institute provides timely access to essential, blended training to improve workforce development and mission success. To learn more, visit www.cyberds.com.

Security Basics: What Is A Cross-Site Scripting Attack?

Cross-site scripting attacks are one of the most exploited vulnerabilities on the web. In this article we explore XSS attacks and how to avoid them.

Once, the web was static and information moved in one direction: from the server to the web browser and thence to the site visitor, but the web has changed. Now almost all sites allow users to submit content, even if it's just in a contact form.

By entering their own content, users change the page that is delivered to their browser. Dynamic sites are what made the web what it is today, without them eCommerce, conversation, and data submission via web pages would be impossible, but allowing user submitted content to influence what appears on web pages introduces a vulnerability that doesn't exist on static web sites: the cross-site scripting attack, also known as XSS attacks, or, less commonly, CSS attacks.

By some estimates, cross-site scripting attacks have overtaken even buffer overflows as the hacker's tactic of choice. They are simple enough to carry out if you have a modicum of coding ability, and the vulnerability exists on thousands of sites.

If you run a website, it's worth understanding how cross-site scripting attacks work.

Consider the fairly simple example of a blog's comment section. Users enter their comment, hit the submit button, and what they wrote is served back to them. It's also served to everyone else who looks at the thread. That's fine if the comment just contains HTML, but in some cases, web applications don't properly sanitize user input.

If instead of just a comment, the user entered some Javascript between <script> tags, and the web application didn't remove it, the comment would still appear as normal, but the script would be embedded within it. Every time someone loaded the page, their browser would run the script. That gives the attacker a huge amount of power.

Frequently, people have to be logged into a blog to comment, which means they have an authentication cookie set in their browser. Their browser trusts the blog, which means it trusts everything that comes from it, including the malicious Javascript.

It's very easy for the attacker to use her script to instruct the browser to send the innocent user's authentication cookie to a server of her choosing. She can then insert that cookie into her browser and the site will give her access to the victim's account.

The above is the simplest example of a persistent cross-site scripting attack, but non-persistent XSS attacks are more common.

For non-persistent attacks, the user doesn't need to make a change to the site's content.

Search engines are frequently used as an example for describing non-persistent XSS attacks, but it can happen with all sort of sites. When data is submitted to a search engine, it's usually passed to the server via the URL query string.

Look at this URL from Flickr:

http://www.flickr.com/search/?q=sad%20puppy

The part following "?" is the query string. If you click it, you'll notice that Flickr fills in the search box with the search query. You can probably see where I'm going with this.

In the same way that it was possible to inject JavaScript in the blog's comment section, with our hypothetical search engine, we'd be able to do the same thing by crafting a URL with our script embedded into it.

Of course, that won't work with Flickr, because it sanitizes its inputs. Many sites do not, or do not do it properly.

Once an attacker has crafted their URL, they can simply email it to their victims, share it on social media, or send an instant message.

The target clicks the link, goes to the page, their browser runs the injected code, and will then happily send whatever information the attacker has requested.

As you can see, XSS attacks are, in theory, fairly simple to avoid by sanitizing inputs, but it's not quite so simple in practice.

In order to let users enter content, they have to be given some degree of latitude.

Hackers can be fiendishly smart, and they are dedicated to exploiting every chink in the armor. It only takes a small bug or oversight in the sanitization code to give them the access they need.

About the Author

Matthew works as an inbound marketer and blogger for Future Hosting, a leading provider of VPS hosting. Follow Future Hosting on Twitter at @fhsales, Like them on Facebook and check out their tech/hosting blog,https://www.futurehosting.com/blog/.


www.isaffuari.com
20TH
ISAF
ISAF
IT SECURITY
5TH INTERNATIONAL INFORMATION & NETWORK SECURITY EXHIBITION
ISAF
SMART HOME
5TH INTERNATIONAL SMART BUILDINGS & BUILDING AUTOMATION EXHIBITION
ISAF
SECURITY
20TH INTERNATIONAL SECURITY & RFID EXHIBITION
"smart solutions"
SEPTEMBER 29TH-OCTOBER 2ND 2016
İstanbul Expo Center (İFM) - TURKIYE
MARMARA
TANITIM FUARCILIK
www.marmarafuar.com.tr | Tel: +90 212 503 32 32 | marmara@marmarafuar.com.tr
This Fair is organized with the audit of TOBB
(The Union of Chambers and Commodity Exchanges of Turkey) in accordance with the Law No 5174
KOSGEB

DON'T TRUST ANY INPUT!

PREVENT VULNERABILITIES FROM BECOMING EXPLOITS WITH TAINTED DATA ANALYSIS

by Bill Graham, Technical Marketing Consultant, GrammaTech

Introduction:
One of the most common attack vectors is user (or other) input into a system. It's very risky to assume that input is well-formed, yet people still do, and it is still a common attack vector.

Security vulnerabilities remain "merely" defects in the code unless the conditions required to trigger the error are present, so the key to a successful attack is to create such conditions.

User input (via UI, terminal access, or other input) is a common way to do this. Tracing the data flow from source to destination (sink) is a key capability of CodeSonar, using its tainted data analysis

What is Tainted Data?
Any unchecked and un-sanitized input into a device is considered tainted – security best practices dictate that all input should be untrusted that comes from outside the limits of the system.

No assumptions can be made about the correctness of this data when designing and implementing the system. SQL injection attacks, using malformed input on websites, are a good example of the risk.

This input, unchecked, can cause the arbitrary execution of SQL within the system, causing data exposure and/or corruption of the database.

Embedded systems are not immune to this kind of problem even if user input or UI isn't provided.

Sources of tainted data include all kinds of external input into the system, such as:

- Environment variables
- File contents
- File metadata, such as a file's permissions or datestamps
- The network
- Network services, such as the results of a DNS query
- The system clock

The location where tainted data is used unchecked is referred to as the tainted data *sink*, which could be a well-known dangerous operation like strcpy().

Once an input has been properly checked, it is considered cleansed and no longer tainted.

Turning a Vulnerability into an Attack with Tainted Data

A vulnerability is a software bug that has the potential to crash a system, expose data, execute injected code, or open the door to other unwanted outcomes.

Vulnerabilities become serious security threats when there is a path to exploit it from the attack surface of the device (i.e. a tainted data source).

Below is a straightforward example that illustrates how reading system environment variables can be risky:

```
void config(void)
{
   char buf[100];
   int count;
   ...
   strcpy(buf, getenv("CONFIG"));
   ...
}
```

In this example, input from outside the system is made with getenv() to retrieve the contents of the environment variable CONFIG. This seems innocuous at first, since the assumption is that any reasonable environment variable would be less than one hundred characters, right? Wrong.

Creating a malformed input in this case could have disastrous effects -- from crashing the system to arbitrary code execution due to a buffer overflow in strcpy().

The tainted data *source* in this case is the getenv() call and the *sink* is the strcpy() function.

Now, this is a simple example. In more complex cases, the source and sink can be in different source files with complex inter-procedural dataflow between them.

A dataflow from tainted data source to vulnerability (sink) is a serious security threat and underlies the need for dataflow analysis as part of a security static analysis tool.

Finding these dataflows manually is very time consuming, so an automated approach is needed.

Automated Tainted Data Analysis

Tainted data dataflow is discovered via internal representations of the code made during static analysis.

Advanced tools like CodeSonar create internal models of the code that describe syntax, control-flow, and dataflow; checkers are created that make use of these representations.

A checker that detects a buffer overflow is augmented with analysis of data sources to see if there is a connection to system inputs.

Discovering this connection means this overflow is not just a serious error, but a potential security vulnerability too. An example of such a report from CodeSonar is below, showing how it indicates sources of tainted data:

Figure 1: A buffer overrun warning where the underlining shows the effect of tainted data.

Software applications are complex and the data and control flow is equally complex and hard to analyze without visualization tools.

Tracing tainted data sources to sinks is an import security audit technique that greatly reduces the risk of vulnerabilities.

GrammaTech CodeSonar provides complete call and data graph analysis and highlights tainted data source and sinks as illustrated below:

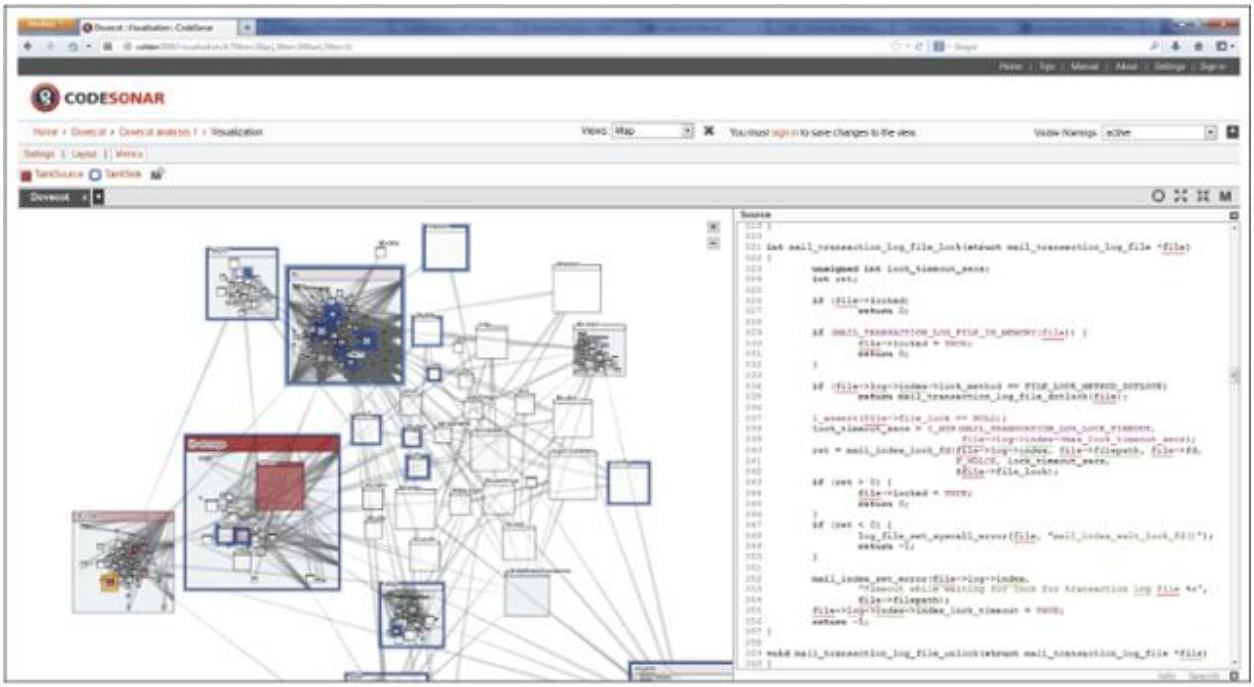


Figure 2: A top-down view of the call graph of a program showing modules according to the physical layout of code in files and directories. The red coloration shows the modules with the most tainted data sources, and the blue "glow" shows modules with tainted data sinks.

Conclusion:

Assuming system inputs are well-formed and reasonable is dangerous, and when paired with vulnerable code, can lead to system crashes, data exposure, and code injection/execution.

The automated tainted dataflow analysis and guidance that CodeSonar provides is essential to discovering these serious vulnerabilities and fixing them efficiently.

About The Author

Bill Graham is a seasoned embedded software development manager with years of development, technical product marketing and product management experience.

Bill can be reached online at @Bill_Graham and at http://iot.williamgraham.ca.

CYBERTECH
29.9.2016 // EUROPE

in collaboration with LEONARDO

FOR CYBER DEFENSE MAGAZINE READERS!
10% OFF
cdm 92783484

CYBERTECH EUROPE

CYBER // INNOVATION // ADVANCED TECHNOLOGIES // INVESTMENT OPPORTUNITIES

29.9.2016 Join us at Palazzo Dei Congressi In Rome, Italy

Cybertech Europe is the premiere event focused on technology, cyber and investment
Also featured is the 'Cybertech Innovation Pavilion' featuring the most innovative startups from around the world

Don't miss this unique networking opportunity!

ORGANIZED BY:
CYBERTECH

E: info@cybertechitaly.com // W: italy.cybertechconference.com

Problems Confronting Systems Certification and Accreditation (C&A) of Government Information Systems

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

Systems Certification and Accreditation (C&A) also known as Accreditation and Authorizations is a Federal process that is used for keeping government information systems and sensitive information that are stored on these systems safe. In the Federal government there are many challenges that include multiple standards in the C&A documents, poor implementation of the process, inability to treat the C&A process as a project (using project management principles), and many complex changes to policies that govern the C&A process. These challenges create the opportunity for sophisticated hackers to break into government systems and attempt to steal valuable data. This study design was a case study that analyzed two case studies that presented challenges in the federal government. The first case study was from the Department of Defense (DoD) and the Department of Veterans Affairs (VA). The results of the study showed that a successful alternative to these breaches was to treat the C&A process as a project.

Keywords: federal government security, information security management, C&A processes, project management and federal government, Certification and Accreditation.

Introduction

The advent of the Internet makes it possible for hackers in the United States and globally, to devise a variety of attack strategies that when successfully implemented, can by-pass any enterprise information system, including the federal information system. Part of the reason that hackers are able to find a way into these systems is because the federal government departments are using flawed Certification & Accreditation processes (Buszta, 2008). Some of the problems that C& A programs have include multiple standards for accreditation, poor implementation of the programs, treating information technology as a separate situation instead of a project (using project management principles), lack of scope definition, lack of foresight, and having too many complex changes (Buszta, 2008). For example, the Veterans Affairs Department puts data for tens of millions of veterans in jeopardy, because of a lack of institutional control over its cyber security evaluation and approval process (Miller, 2013). This is only one part of an extensive C&A process. To alleviate some of these challenges, seeing C&A processes as a full project would be valuable because there would be specific steps involved for each process.

Research Method and Design

The research used was a qualitative case study that analyzed two federal agencies. The researcher did not interview individuals but analyzed two case studies found in the literature on government security. The two cases provided data on how C&A programs failed. Also, the case studies provided an understanding of best practices for designing internet security features that may be successful if used in government programs.

Overview of Security Issues

There are many reasons why enterprise systems have a challenge with security. The global news has exposed several businesses for breaches in security such as Worldcom, Morgan Stanley, Target (Harris & Perlroth, 2014; Pagliery, 2015). The federal government also had security breaches that may have been prevented. For example, a group of Russian hackers breached the unclassified section of the White House computers which caused a delay in services while the cyber security team worked to find and eliminate the breach (Nakashima, 2014). Other departments like the postal service, the FBI, and the Senate experienced breaches within the last 10 years (Ten Big Federal, 2011). These breaches in security show that there is a need for something else to be done.

Organizations are constantly dealing with cyber-attacks which may cost over $70 billion on IT security each year (Soluade & Opara, 2014). In contrast, the Department of Defense (DoD) spent in access of $15 million of the $50 billion budget that the federal government spends on cyber security (Paganini, 2014). In all cases, hacking continues.

Cyber criminals have more sophisticated ways of attacking systems and are able to bypass traditional technologies because hackers have learned where systems are generally most vulnerable (Saluade & Opara, 2014). For example, all systems have loopholes that the organization may find, but when it is found, there exists a time gap between the attack and the repair. This time gap is when the organization is most vulnerable and attackers can use this time to attack.

Many businesses have moved to the cloud thinking that it would be more secure, but there are still problems. Using the cloud means that customers will change software applications frequently (Subashini & Kavita, 2011). All software platforms are vulnerable to hackers and must secure data, the network, authenticity and authorization to secure the organization. The challenge for organizations is that these systems must constantly be updated and many organizations are not sure how to keep up with updates.

Another issue for organizations is the lack of understanding of what is needed to guard networks. The government is not exempt from this problem. For example, Edwards (2013) noted that the Department of Defense (DoD) attempted to move to a unified capabilities strategy to integrate and form a collaborative platform. One challenge for DoD in attempting this was that the system was to bring all data into one place.

Without proper security, the DoD could create more vulnerability, especially because designers have challenges when developing this process that can create challenges to security. Another problem for DoD designers is that they must work quickly to circumvent emerging threats, however, they use traditional ways of testing and validating systems. The traditional methods for certifying a system may not be able to keep up with newer threats (Edwards, 2013).

Khoo, Harris, and Hartman (2010) stated that enterprises have become reliant on the internet for their information infrastructure. Khoo et al. also stated that businesses realize that security goes beyond technical issues. Other issues like confidentiality, integrity, and the availability of information are critical to the organization's success. Keeping information secure for customers is a top priority. As more organizations use the information infrastructure that uses the internet, it becomes a need for legislation to secure cyber space is also important.

Research concerning systems security provides an understanding that although security has become more of a priority to organizations, but for other organizations, security is not a simple task and organizations struggle with how to secure the system over the long-term. In fact, many organizations have misconceptions of what systems security actually means. Also, many organizations treat systems security as separate from other projects. Unfortunately, the DoD is one organization that does not see security systems as a project (Morris, 2012).

Data Collection

Two case studies were analyzed for this study that had major breaches in security at some time in the last 13 years. A comparison was made between the Department of Defense (2001) and the Veteran's Administration (2013) to understand how the breaches had occurred and what could be done.

Department of Defense

At the Department of Defense (DoD), a code red worm attack on the White House infected over 395,000 Internet and client systems in 2001. This attack happened in 14 hours because of several vulnerabilities in the federal government's hosting and general systems. The attack also created $2.6 billion in damages, while infecting 2,000 host systems per minute (Miller, 2013). The DoD used trace analysis results obtained from data collecting and using a global detection worm spread.

The global detection worm spread examined all host systems and their infected properties in all geographical locations, and examined Internet service providers (ISP) and top domains. Results showed that the code red worm was focused mostly on small business and home-based systems, and it leached into the White House because of weaknesses in the federal government host systems (Miller, 2013).

Veteran's Administration

The Veteran's Administration experienced a breach due to poor implementation of the C&A program. The breach happened in 2013 and was the result of an employee's actions. Jerry Davis was a deputy assistant secretary for the VA's office of Information Technology. He stated in documents obtained by Federal New Radio, that he was forced to rubber stamp 250 security certification for IT agency systems (Miller, 2013). Davis would later suggest, in a letter to Congress, that he did not want to sign the documents because he did not think the C&A process was secure. Davis said he did what was required as a condition for release from the VA to take a job as the CIO of NASA Ames in Moffet Field, CA.

He further testified that he saw a clear and present danger as he was sighing the document and a risk of exposing and/or compromise of sensitive data for perhaps millions of veterans. The documents that Davis was asked to sign were Accreditation and Authorizations [now known as C&A programs] (Miller, 2013).

Data Analysis

The analysis of these two case studies found that both were susceptible to security breaches because of the challenges that were brought on by an ineffective security system. The DoD system breach was only found after the system was searched.

The breach lasted 14 hours because there was no alert on the system to show that the system was breached. The Veteran's Administration happened because an employee was coerced to sign certifications for agencies that had not reached accreditation status.

Both cases were shown to have challenges because managers did not understand how the C&A process should work and did not provide a collaboration between IT and the business side of the organization. In both cases, IT was seen as a separate entity that was not connected to other areas of the government.

Conclusion

From these case studies and other research, it is clear that a change in the C&A process must be made. Employing project management techniques to these projects could save time and money. The C&A process will also need good time management, strong leadership and risk management techniques.

References

Edwards, R. (2007). Online: Certification and Accreditation: A dilemma. ISACA. Retrieved from http://www.isaca.org/Journal/Past-Issues/2007/Volume-3/Pages/JOnline-Certification-and-Accreditation-A-Dilemma.aspx

Harris, E., and Perlroth, N. (2014, March 13). Target missed signs of a data breached. Retrieved from http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-. breach.html?_r=0

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management and Information Systems, 14*(3), 49-55.

Konkel, F. (2014). Latest breach at VA has Congress asking more questions. *FCW: The Business of Federal Technology*. Retrieved from https://fcw.com/articles/2014/01/27/congress- Miller J. (2013) VA's security shortcuts put millions of veterans' data at risk, former VA cyber official alleges Retrieved from http://www.federalnewsradio.com/538/3344870/VAs-security-shortcuts-put-millions-of-veterans-data-at-risk-former-VA-cyber-official-alleges-wants-answers-on-va-breach.aspx

Morris, P. W. G. (2012). Cleland and King: Project management and the systems approach. *International Journal of Managing Projects in Business, 5*(4), 634 – 642. doi:10.1108/17538371211268951

Nakishima, E. (2014, October 28). Hackers breach some White House computers. *The Washington Post*, Retrieved from Retrieved from http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html

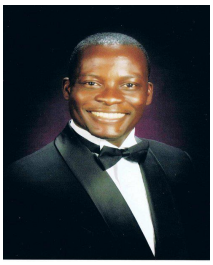
Paganini, P. (2014, March). $5 Billion in military cyber spending fivefold increase over last year. *Security Affairs*. Retrieved from http://securityaffairs.co/wordpress/22952/cyber-warfare-2/5-billion-military-cyber-spending.html

Pagliery, J. (2015, Jan. 5). Morgan Stanley insider exposes rich clients' info online. *CNN Money*. Retrieved from http://money.cnn.com/2015/01/05/technology/security/morgan-stanley-data-breach

Soluade, O. A., & Opara, E. U. (2014). Security breaches, network exploits and vulnerabilities: A conundrum and an analysis. *International Journal Of Cyber-Security and Digital Forensics, 3*(4), 246-281. Retrieved from http://sdiwc.net/security-journal/prev_issue.php

Ten Big Federal Security Breaches. (n.d.). *ARCSITE*. Retrieved from http://cdn.govexec.com/resources/10-big-federal-security-breaches/doc.pdf.

About The Author



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

Daniel is a Doctor of Computer Science in Information Assurance, Senior Cybersecurity Administrator and Compliance Auditor 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 online at odharrison4@yahoo.com and at our company website http://www.bechtel.com/

Why it's important to combat against terrorism

By Milica D. Djekic

These days we would remember one of the greatest crimes a modern history would be witnessing. It's non-doubtly the September 11 terrorist attack which happened in New York City and Washington DC. Those events changed the picture of the modern world and unfortunately took many human lives. Through this effort, we would remember that tragedy and also discuss why it's important to fight and destroy the terrorism at the global level. The September 11 attacks happened 15 years ago and got conducted by the terrorist group called Al-Qaeda and unluckily even today we deal with the terrorist threat called ISIL.

Terrorism would exist probably as long as the entire human history. The historical sources would claim that our world would always deal with the individuals who would believe they may get anything using the force and producing the fear amongst the people. The origin of that word comes from the ancient world *terrere* which would mean trembling, shaking and, indeed, the terrorism would shake the existing human population whenever it occurs. The terrorism is, without hesitating, a crime and as a crime it would bring only suffering to good people. The reasons why terrorism exists in a modern time is mainly economical by its nature and we would believe that the lack of proper education at the international level would make people turn into that crime believing they would get some money through such an activity.

So, what happened after the September 11, 2001? Practically, the world would be witnessing a plenty of horrible terrorist activities and global defense would try to put the situation under the control. The reason why we must win that war is better future to all – especially including the new generations. The terrorism would sabotage the progress and make people feel unsecure within their environment. Also, this war must get won for a reason of bringing the peace to all. Finally, we believe that this world could get much safer place to live in if we reduce the terrorism at the global level. People combating this sort of crime could get seen as the real heroes of the modern era and we are confident such heroes can save many innocent lives over the globe.

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.

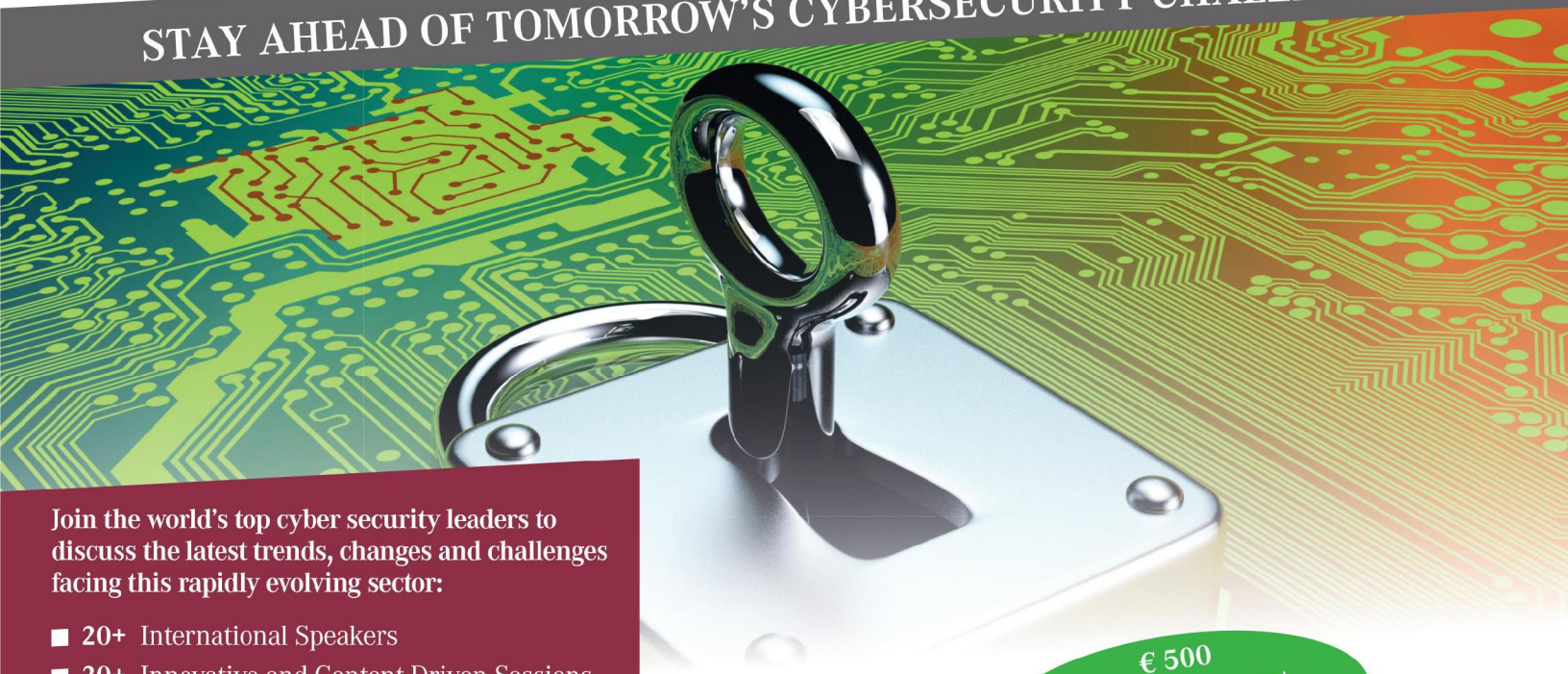
2nd ANNUAL SUMMIT

GLOBAL CYBER SECURITY LEADERS

EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

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

STAY AHEAD OF TOMORROW'S CYBERSECURITY CHALLENGES!



Join the world's top cyber security leaders to discuss the latest trends, changes and challenges facing this rapidly evolving sector:

- **20+** International Speakers
- **30+** Innovative and Content Driven Sessions
- **30+** Hours of Exclusive Networking

€ 500 Special Discount with code GCSL4CDM

Speakers include:

Alexander Oesterle
Global VP Governance, Risk & Compliance and CSO, **SAP, Germany**

Daniel Selman
Cyber Industry Deputy Head, **UK Ministry of Defence, United Kingdom**

Stephan Gerhager
CISO, **Allianz Deutschland AG, Germany**

Scott Stewart
Vice President of Tactical Analysis, **Stratfor, USA**

Taiye Lambo
CISO, **City of Atlanta, USA**

Volker Kozok
Assistant Branch Chief German MoD, **Bundeswehr, Germany**

Kim B. Larsen
CSO, **Huawei Technologies, Denmark**

Arieh Shalem
CISO, **Orange Telecommunication, Israel**

Premium Partner

Warth & Klein Grant Thornton
An instinct for growth™

Promoters

EY Building a better working world

ThreatBook

Hosted by

MANAGEMENT CIRCLE®

Official Part of

Global Leaders Summit Series
EXCLUSIVE. INNOVATIVE. CONTENT DRIVEN.

www.cybersecurity-leaders.com

Is Your Workforce the Weakest Link in Your Security Policy?

By John Brenberg, Information Security & Compliance Manager, 3M and member of the 3M-sponsored Visual Privacy Advisory Council.

Just like thieves roam bustling tourist areas, hackers look for easy opportunities to gather valuable data.

Companies are spending record amounts to protect themselves from cybersecurity threats – reaching $75 billion last year – which means attackers may seek new weaknesses to exploit.

The sad reality is that employees may be that new weakness. Many don't apply the same vigilance to protecting corporate information as they do their own personal information.

An employee carefully shielding an ATM keypad while entering their PIN may not think twice about leaving network log-in information taped to their computer monitor at work.

So how can you get employees to break bad habits and protect corporate information with the same diligence they do their own personal information?

Conduct a Risk Assessment

A risk assessment of employee habits can help identify the risks – both inside and outside your company's walls.

A growing number of companies have open-office floorplans, which reduce privacy and may be more susceptible to visual hacking. Or perhaps employees have formed a habit of propping open security doors, or letting in visitors without proper authentication.

Going beyond your building's footprint, employees also risk falling prey to hackers while accessing company information on their daily train commute, working remotely from an airport or coffee shop, or attending a conference.

Apply Changes

After a risk assessment, the proper policies, tools and training can be put in place. For example, when traveling, workers should use loaner computers, which may help limit the information available to hackers if a device is compromised.

Workers should also avoid public Wi-Fi hotspots, as hackers can use those to intercept unencrypted data .

One basic tool that every employer should supply is a privacy filter. They are easy to use and apply over a device screen helping prevent visual hacking by blackening out the angled views of potential onlookers.

Workers should also receive annual training on proper handling and protecting of company information.

Don't forget about third-party agencies and consultants; their privacy policies should align with your expectations as well.

Empower your employees with the tools and training needed to be vigilant guardians of your company's most closely held ideas and information; don't let them fall victim to visual hackers and be a weak link in your company's security policy.

About the Author

John Brenberg has over 30 years of experience spanning new product introduction, system development, infrastructure management and information security and compliance across multiple business segments and processes.

He is responsible for leading the IT programs for information security, compliance and risk, all for the protection of company and customer information and critical business processes.

Brenberg credits his success to his many strong internal partnerships across intellectual property, privacy, compliance and systems management. He is also a member of the Visual Privacy Advisory Council.

THE MEANS TO PREVENT FINANCIAL CYBERTHEFT IS AVAILABLE

NOBODY IN THE U.S. HAS AUTHORITY OR CAPABILITY TO STOP THE CRIME

Harold Chanin, President Cyber-Theft Prevention Associates

There are two aspects of identity theft (IT).

To stop the crime of stealing another's identity without seeking financial gain is basically a mission impossible, not at-issue here. The financial side of this criminal coin is the issue.

Electronic financial theft (EFT).

The U.S. membership-credit card design could not serve EFT due to reliance on *human*s. But a few decades later EFT emerged. The electromagnetic reel-to-reel audio tape was embedded on the plastic card to enhance productivity and increase profits by reliance on *electrons*.

The accidental gift.

Shortly thereafter EFT quickly spread globally after the U.S. gave ownership of the card design to the International Organization for Standardization (ISO) and operations to the International Electrotechnical Commission (IEC) in Geneva, Switzerland.

The American National Standards Institute (ANSI) in Washington, D.C. is the U.S. representative.

This unintended consequence expanded and extended this online crime syndicate's reach and capability, especially cyber hacking and breaching centralized government, business and personal financial data and information repositories.

In response, ISO/IEC embedded the European microprocessor chip, thereby adding a layer of electronic theft protection at points-of-sale to reduce processing fraudulent chip cards.

Business is business.

For decades thereafter few bought the chip's costly, limited protection capability. But others saw this new business opportunity. Still there was little acceptance of the chip card - most noteworthy in the U.S. Fortunately for the entrepreneurs, the recent rash of vast, global EFT resulted in several major marketing accomplishments within the U.S.

In 2014 President Obama signed the executive order those seeking federal contracts must be using chip cards (such as the government's SmartPay Card variant).

And in 2015 American banks and lenders proclaimed merchants not accepting the chip card (such as the EMV Card variant) may then be held accountable for this loss.

EFT has not been stopped, just wounded.

The ISO/IEC is an extremely vast and complex international technical organization setting specs and standards. But due to intellectual property agreement ISO/IEC may not assess a nation's patent without obtaining formal permission from that nation (in this case the ANSI).

From investment perspectives, the basic payment card must be redesigned (by the ISO) and the system software then redesigned (by the IEC) to prevent EFT, not just protect from, throughout the financial cyber process (at the front-end, the middle and the back-end).

Business-wise, far more people make their legitimate living due to the existence of EFT (studies and reports, education, selling protective goods and services, investigating and chasing) than these criminals, their cohorts (e.g., human money mules) and victims combined.

Nobody in the U.S. has authority or capability to stop the crime.

Nobody until the ANSI grants ISO/IEC permission to assess for adopting the U.S. financial cybertheft prevention technology (follows). Until then American federal and states taxpayers, merchants and consumers will continue to pay around $1 billion/day due to the global EFT.

THE ELECTROMECHANICAL "CYBER CARD" FINANCIAL SYSTEM

Utility Patent: Chanin No. US 7,991,695 B2 August 2, 2011: Interactive Financial Card System Uniquely Suited For Conducting Financial Transactions On The Internet.

THE VULNERABLE INTERNET MARKETPLACE.

- Electronic financial theft (EFT) cannot be stopped by legislation, nor by blaming these thieves and their many victims.
- The crime enabler is the archaic engineering of the identity-based card design.
- According to the U.S. Government (e.g., the President, GAO and CBO) around a $1 trillion per year is stolen and wasted worldwide due to EFT (a third from the U.S.).
- As global economies continue expanding into online 'cashless-commerce' so does EFT.

PAYMENT CARDS LEGACY.

- The original paper membership-credit card design (Diners Club circa 1920) was based on accountable human-to-human processing and thereby security gatekeeping.

- The magnetic-strip (IBM 1950) also permits theft since net-neutral electrons not humans conduct identity confirmation and authorize transfer of money ownership. (Ownership because Internet “tubes” and telephone “lines” cannot transfer cash.)
- The 1970s European micro-chip card was standardized by ISO/IEC (circa 1980) to help protect from EFT at points-of-sale when utilizing fraudulent chip cards.
- The low-cost, disposable, non-identity, U.S. electromechanical Cyber Card system was engineered to stop EFT by replacing electrons with humans – back to the secure future.

EFT PREVENTION CONCEPT.

- Standard payment cards (e.g.; Credit, Debit and ATM) can be visualized as if house keys which provide each owner’s identity, address and security attributes.
- The electromechanical Cyber Card design can be visualized also as if house keys which do not provide theft-enabling data, information or security attributes.

EFT PREVENTION PRINCIPLE.

- Security risk with standard and chip payment cards can be compared to the limited, statistical protection provided by bullet-proof vests, while Cyber Cards can be compared to offensive weapons which cannot function.
- Cyber Cards provide no identity nor financial value to others by possession, duplication or knowledge of their inherent data and information baseline.
- Cyber Cards do not employ identity, nor embossed or printed numerics including no card number, no account number, and no security or check digits.
- Cyber Cards do not need the owner’s name, dates, photo, signature, face-recognition, fingerprint, micro-chip, security hologram or the like.
- Cyber Cards can provide openly available information regarding card type, bank, issuer, service disclaimers, phone numbers, legal warning, etc.
- Cyber Card identification is based on a scene selected by the owner from among many thousands; space is provided to write a personal identity code to protect from rare cases of same scene cards used at the same place at the same time by the same person(s).
- Each Cyber Card by design can only serve the legitimate owner, not the card possessor nor due to such data and information as gained.

SECURED INTERNET CYBER CARD SYSTEM.

- Employs proved, off-the-shelf mag-strip, hardware and firmware.
- Each cyber device requires integration with an off-the-shelf mag-strip reader.
- Software is segregated and encrypted.
- Cyber Cards cannot serve skimming, hacking or breaching, such as with malware and/or botnet malware.
- Cyber Cards security systems are de-centralized into several encrypted repositories, each repository requiring knowledge of the issuer's encrypted platform for integrating identity confirmation, for financial authorization and money ownership transfer.

SECURED CYBER CARD PROCESS.

- Upon receipt of the Cyber Card the owner is provided with the issuer's initial, encrypted cyber-encoding by which to enter the de-centralized, on-line Internet financial system.
- Ensuing security is established solely by the card owner who alone can change encodings; the issuer's encrypted, decentralized system then assures nobody else can, including employees or thieves.
- The Cyber Card owner can encrypt security encodings in their personal cyber devices for secured in-house purchases on the Internet.
- The system cannot be entered without the Cyber Card, the device's e-reader requiring and accepting the unknown owner's security encodings per the unknown owner's encryption (PINs and Passwords are basic examples).
- Others cannot operate this Internet system by possessing or duplicating another's Cyber Card since the Cyber card provides no intrinsic identity, thereby no financial value.
- The new cyber system also permits the simplicity of owning a singular government and/or commercial Cyber Card which requires its possessor to decide which top-tier encrypted Internet system to enter based on the non-identifiable owner's encoding.

OTHER APPLICATIONS OF CYBER CARD TECHNOLOGY.

- Governments can issue variants of the Cyber Card to secure electronic voting.
- Can be the first step to enter security-soft infrastructures and facilities.
- Can secure federal and state financial programs including Social Security, Medicare, Medicaid and Tax Reimbursement.
- Converts the high-value U.S. Social Security Card to a no-value membership card.

- Due to the unique electromechanical Internet entry, Cyber Card variants can prevent hacking some non-financial government and private data and information repositories (not unlike the electromechanical system securing U.S. nuclear weapons).

INVENTOR AND PATENT OWNER.

- Has a BS (1962) in Mechanical Engineering and MS (1968) in Industrial Engineering from the New Jersey Institute of Technology (Newark College of Engineering).
- Worked 10 years in industry as engineer and organizational management consultant.
- Worked 36 years in the Department of Defense as weapons systems engineer, projects manager and senior RDT&E laboratory executive (e.g., the M4 Carbine used by the U.S. Navy's Seals-T6 to put Osama Bin Laden out of our misery).

About the Author

Harold Chanin

President, Cyber-Theft Prevention Associates

7811 Lando Avenue, *Boynton Beach, Florida 33437*

Latin CIO Summit

November 17-18, 2016, Trump Ocean Club, Panama City, Panama

Industry leaders from around the globe are confirming their places on the line-up for the Latin Chief Information Officer Summit. Join them in a two day event offering Latin America's leading decision makers of the industry a devoted environment for **unparalleled business and networking opportunities in a stimulating environment.**

Grow your business & sales in just 2 days
Network with high level executives during formal and informal time such as cocktails and dinner hours!
Target qualified buyers through our pre-scheduled one-on-one meetings format

EXPERT SPEAKERS ALREADY CONFIRMED ON THE LINE-UP INCLUDE

- EVP & Chief Information Officer, **Costco Wholesale Corporation**
- Chief Information Officer, **Xerox Corporation**
- Global Product Security & Services Officer, **Philips Healthcare**
- Chief Information Officer, **Georgia-Pacific LLC**
- VP, Global Technology Services, **U.S. Bank**
- Senior Vice President, Head of North America, **Syntel, Inc.**
- Chief Technology Officer – Americas, **HCL Technologies**

SOME TOPICS TO BE DISCUSSED ARE:

- The Role of the CIO
- Data Security
- Mobility and Network Connectivity
- Trends and Uses of The Cloud
- Big Data
- IT Working Together with Sales and Marketing
- Adapting to the Fast Forward Digital World
- Investing in Talent
- The future of Technology in Latin America

For more information please contact **alejandrad@marcusevansmx.com** or visit
http://events.marcusevans-events.com/latinciocdm

marcusevans

NSA Spying Concerns? Learn Counterveillance

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

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

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

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

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

Course Overview:

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

Your Enrollment includes :

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

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

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

You have built a great app with an amazing team.

Let us help you secure it.

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

KEY FEATURES

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

GET IN TOUCH

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

SW-GEN-2015-0205

AppSHIELD™ SDK

MOBILE APP FIREWALL & CLOAKING TECHNOLOGY

Firewalls are essential for security

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

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

DO IT YOURSELF TO BUILD A MOBILE APP FIREWALL

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

VS.

LICENSE OUR AppSHIELD SDK

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

GET IN TOUCH

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

Top Twenty INFOSEC Open Sources

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

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

Here they are:

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

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

(Source: CDM)

National Information Security Group Offers FREE Techtips

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

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

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

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

Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

So use it by going here:

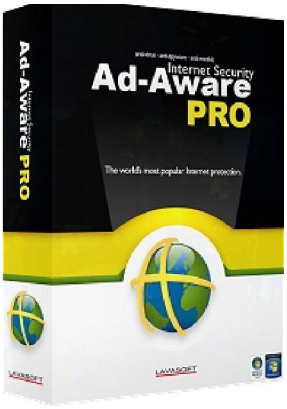
http://www.naisg.org/techtips.asp

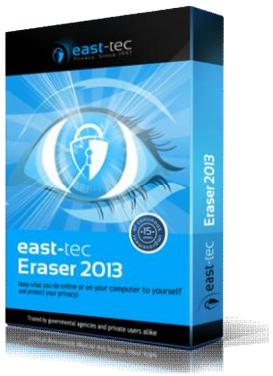
SOURCES: CDM and NAISG.ORG

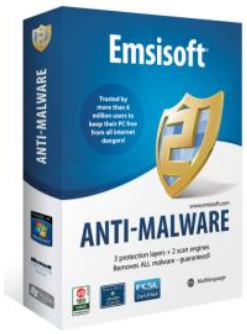
SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

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.







Job Opportunities

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

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Warnings e-Magazines will also keep you up to speed on what's happening in the cyber crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy.

You get all of this for FREE, always, for our electronic editions.

Click here to signup today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

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

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine September 2016

Sample Sponsors:

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

Cyber Warnings Newsflash for September 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…

Tech Q&A: Spotting malware on your phone, buying lottery tickets with an app

http://www.foxnews.com/tech/2016/09/25/tech-q-spotting-malware-on-your-phone-buying-lottery-tickets-with-app.html

Malware-infected USB sticks posted to Australian homes

http://www.bbc.com/news/technology-37431335

Street Fighter V Update Pulled Because It Made PCs Vulnerable To Malware

http://kotaku.com/street-fighter-v-update-pulled-because-it-made-pcs-vuln-1787038586

Employees download new malware every four seconds, Check Point finds

http://www.healthcareitnews.com/news/employees-download-new-malware-every-four-seconds-check-point-finds

IoT devices increasingly being used for malware attacks: Symantec

http://zeenews.india.com/internet-social-media/iot-devices-increasingly-being-used-for-malware-attacks-symantec_1933746.html

Malware figures out it's running on VMs and refuses to execute

http://www.theregister.co.uk/2016/09/23/new_antivirus_trick_dont_write_reports/

Malware Evades Detection with Novel Technique

https://threatpost.com/malware-evades-detection-with-novel-technique/120787/

New PonyForx Infostealer Malware Sold on Russian Hacking Forums

http://news.softpedia.com/news/new-ponyforx-infostealer-malware-sold-on-russian-hacking-forums-508661.shtml

Raum turns the most popular torrents on the web into malware spreading weapons

http://www.zdnet.com/article/raum-tool-spreads-malware-through-popular-torrents/

Data-stealing Qadars Trojan malware takes aim at 18 UK banks

http://www.zdnet.com/article/data-stealing-qadars-trojan-malware-takes-aim-at-18-uk-banks/

A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack

http://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952

Smart Anti-Detection Tricks Added by Clever Malware

http://virusguides.com/smart-anti-detection-tricks-added-clever-malware/

Malware attacks are declining but getting cleverer

http://betanews.com/2016/09/21/malware-declining-but-cleverer/

Growing Malware, Ransomware Risks Highlight Opportunity For Partners

http://www.channelpartnersonline.com/news/2016/09/growing-malware-ransomware-risks-highlight-opport.aspx

Fake Pokémon Go apps are crammed full of malware

http://thenextweb.com/apps/2016/09/15/fake-pokemon-go-apps-malware/#gref

Suspected Russia-based stealth banking malware Qadars Trojan sets sights on 18 UK banks

http://www.ibtimes.co.uk/suspected-russia-based-stealth-banking-malware-qadars-trojan-sets-sights-18-uk-banks-1582497

Just For Men Website Caught Distributing Malware

http://www.vocativ.com/360855/just-for-men-malware/

Thousands of Seagate NAS boxes host cryptocurrency mining malware

http://www.pcworld.com/article/3118717/security/thousands-of-seagate-nas-boxes-host-cryptocurrency-mining-malware.html

Generic OS X Malware Detection Method Explained

https://threatpost.com/generic-os-x-malware-detection-method-explained/120503/

Smartphone Infections Rise 96% In H1-2016: Malware Study

http://www.darkreading.com/vulnerabilities---threats/smartphone-infections-rise-96--in-h1-2016-malware-study/d/d-id/1326949

RAA ransomware now targets businesses, installs data stealing 'Pony' malware

http://www.zdnet.com/article/raa-ransomware-now-targets-businesses-installs-data-stealing-pony-malware/

New Malware Targets Android Banking Apps, Cybersecurity Group Says

http://www.wsj.com/articles/new-malware-targets-android-banking-apps-cybersecurity-group-says-1473198676

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

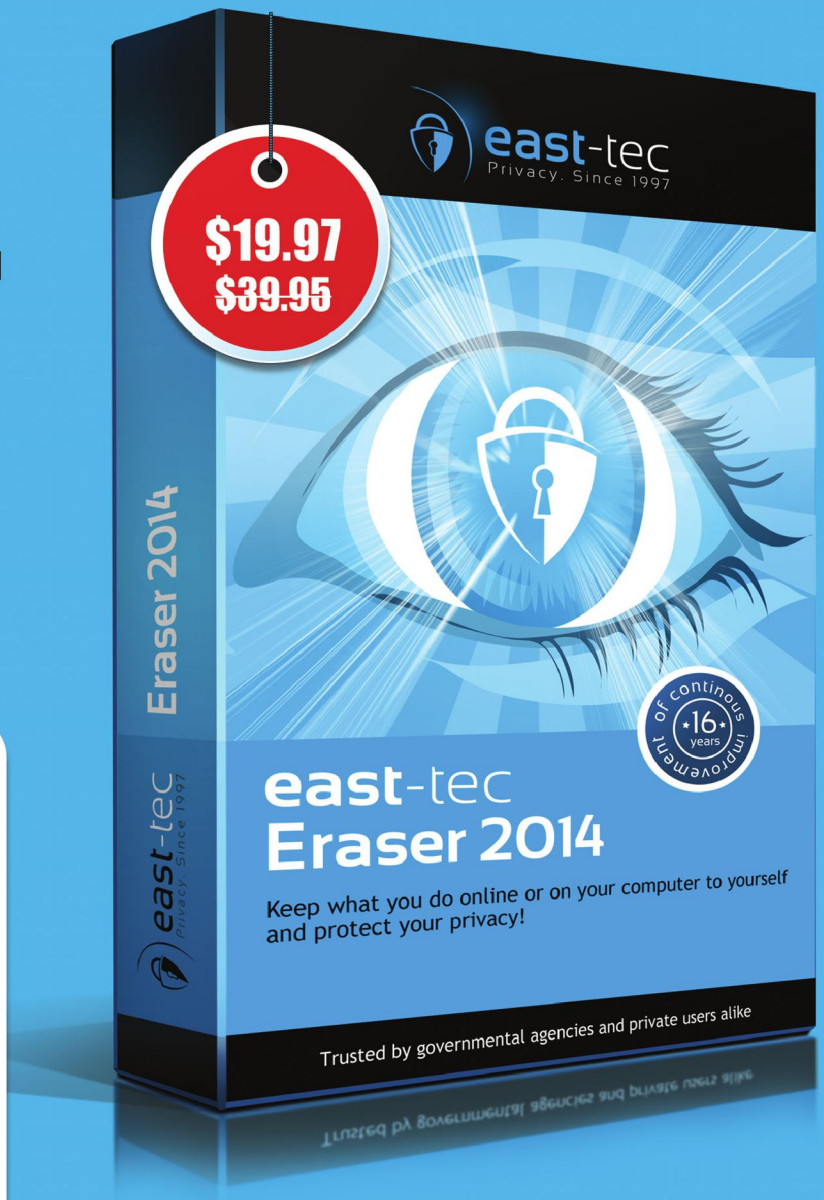
Cyber Defense Magazine - Cyber Warnings rev. date: 09/28/2016

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 pictures pages online privacy secure search cookies security emails