AN INDEPENDENT SUPPLEMENT BY MEDIAPLANET TO CHICAGO TRIBUNE

No.3/December 2011

MEDIA PLANET

CYBER SECURITY

3 STEPS TO CREATING A WELL-PROTECTED BUSINESS

Advanced Persistent Threats
Do you know how they affect your company?

Kevin Johnson
How smartphones and tablets leave businesses vulnerable to hackers

SMART HACKING
Kevin Johnson, SANS Institute Instructor, Senior Security Analyst, Secure Ideas

SECURE YOUR BUSINESS FROM CYBER THREATS

Learn how to effectively combat increasingly sophisticated hacking attacks

The technological innovations leveraged by businesses continuously reveal new cyber threats that can be combatted through training, education, and awareness.

STEP 1
EDUCATE YOUR WORKFORCE

You are the greatest weapon against cyber crime

Technology has become an extremely powerful tool, allowing us to do just about anything we want, anytime we want, anywhere we want. In addition new developments are only accelerating this trend. For example cloud technology enables you to access your data, games, music, email or movies regardless of where you are and when you need it. With the development of mobile devices such as smartphones and tablets, you now have a universal device to view, modify and share that very same data. Technologies such as these have not only made our personal lives much simpler, but also made organizations more efficient. They can quickly create and develop new products, analyze huge amounts of information, and help coordinate the activities of employees globally. However all these amazing advances have made it only simpler for cyber attackers to commit fraud, identity theft, extortion and corporate espionage.

The growing human vulnerability

We in the security community have strived to keep up with both these advancing threats and technology. We have made tremendous progress; operating systems are more secure, web filtering has become widespread, and enterprise solutions such intrusion detection and firewalls have become far more effective. However, as technological solutions continue to improve, one key weakness continues to stand out, the human element. While organizations have poured billions of dollars into technology, very little has been done to secure their people. This is why the human has become the primary attack vector, as reported by Microsoft in their most recent Security Intelligence Report and recent incidents at Google, Oak Ridge National labs and hundreds of other organization.

> "Organizations need to deploy active security awareness programs that are engaging and training their people."

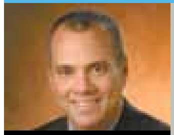
Lance Spitzner
Training Director, SANS Securing The Human Training Program

Education is the key

The key solution here is not technology but education and awareness. By changing employee behaviors, people can not only become a primary control for preventing attacks, but they can also be leveraged for helping detect and respond to them. Organizations need to deploy active security awareness programs that are engaging and training their people on a continual basis. Awareness, not just technology, is the key in today's rapidly changing world in securing your organization.

LANCE SPITZNER
editorial@mediaplanet.com

WE RECOMMEND



PAGE 7

Tom Heiser
Urges businesses to create security systems that recognize the enemy within quickly

MEDIA PLANET

CYBER SECURITY,
3RD EDITION, DECEMBER 2011

Publisher: Mark Dinglasan
mark.dinglasan@mediaplanet.com
Designer: MIssy Kayko
missy.kayko@mediaplanet.com
Managing Director: Geraldine Delacuesta
geraldine.delacuesta@mediaplanet.com

Contributors: Doug Chansky, Alan Dabbiere, Tom Heiser, Kevin Johnson, Ron Knode, Gary Mullen, Lance Spitzner, Stan Stahl, Ph.D; Michael Sutton

Distributed within:
Chicago Tribune, December 2011
This section was created by Mediaplanet and did not involve the Chicago Tribune or its Editorial Departments.

FOLLOW US ON FACEBOOK & TWITTER!
facebook.com/MediaplanetUSA
twitter.com/MediaplanetUSA

Mediaplanet's business is to create new customers for our advertisers by providing readers with high-quality editorial content that motivates them to act.

A personal guide to staying safe online

Cybercriminals steal your sensitive personal information by taking control of your computer.

This also lets criminals install rogue programs on your computer, turning it into a zombie under their control—the cyber-equivalent of Night of the Living Dead. These control programs make money for the cybercriminals by sending spam, displaying pop-up ads, and committing sophisticated computer crime. How do they do it? Cybercriminals take control of your computer by exploiting four weaknesses:

- Every program running on your computer has subtle programming errors (vulnerabilities) that cybercriminals exploit to take control of your computer.
- Legitimate internet web sites often fail to prevent cybercriminals from installing malicious programs on their websites. When you visit these sites, these malicious programs silently install Trojan horses and other malware on your computer.
- Default settings for many computer programs make it easy for cyber criminals to take control of your computer.
- Users often don't know what they need to do to minimize the dangers and risks of cyber crime, particularly the need for defense-in-depth.

In order to keep cybercriminals off your computer, here are some defense strategies:

Limit exposure: Create separate accounts for all family members. This will make it harder for cybercriminals to install malware on your computer.

SECURE YOUR WIFI. **If you have a wireless network, encrypt it with WPA2 encryption.** PHOTO: SXC.HU

Protect your desktop: Install a reputable antivirus/antispyware product and keep it up-to-date. Sophisticated cybercriminals can get past basic antivirus/antispyware software. Antivirus is necessary but not sufficient.

Secure your WiFi: If you have a wireless network, encrypt it with WPA2 encryption. Otherwise anyone near you can eavesdrop on your communications and piggy-back on your connection.

Defense strategy: Be careful with your financial information online. Use a credit card rather than a debit card when shopping on-line. Link PayPal to your credit card, not your bank account. Federal law limits your credit card exposure to $50. There is no corresponding limit if you use a debit card (even though many banks cover debit card fraud).

Remember, always think about the information you are giving out and when in doubt, don't.

STAN STAHL, PH.D
editorial@mediaplanet.com

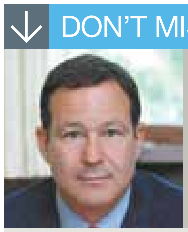
PROTECT THE "E-ME"

The Internet is today's home away from home; it is the playground for our imaginations; it is the new community we live in. So the same as we lock our cars and houses, we need to safe guard the 'e-ME' or electronic version of our individual information. Neglecting this or failing to take the topic seriously is just as crazy as pinning up our debit card with PIN number to the tack board at the local community shop with a note saying, "if needed use this, it's on me, you're welcome."

It is our personal responsibility to protect ourselves—understanding that concept, understanding our own Internet presence, and wanting to take steps to secure it is the first line of defense.

DOUG CHANSKY,
CONTOUR DATA SOLUTION
editorial@mediaplanet.com

DON'T MISS



Alan Dabbiere, Chairman, AirWatch

Why MDM? Enterprise mobility: Death by a thousand cuts

Enterprise mobility can be "death by a thousand cuts." There are currently an estimated 5.3 billion mobile subscribers, which equates to 77 percent of the world population. In addition, the widespread deployment of corporate and employee-liable devices for business use is on the rise. However, as the mobile landscape continues to grow in leaps and bounds, how can enterprises tame the beast by deploying, monitoring, managing and supporting mobile devices securely and effectively?

Mobile device management (MDM) solutions allow enterprises to efficiently and securely extend corporate resources to mobile workers. In addition, MDM solutions enable organizations to securely deploy, monitor and manage devices and applications across of broad range of device platforms. This allows IT to not worry about tactical day-to-day management of devices and apps.

ALAN DABBIERE
editorial@mediaplanet.com

Question: How do smartphones and tablets leave businesses and individuals vulnerable to hackers?
Answer: Kevin Johnson explains that mobile platforms are easily hacked but awareness and effective consulting can secure mobile devices and protect enterprises.

STEP 2
SECURE YOUR COMPANY MOBILE DEVICES

Execs hire security experts to keep data out of the wrong hands

Smartphones and Ipads may be the way of the future, but for a growing number of businesses, they're proving to be a major security risk. Many companies are turning to security firms to "ethically" hack into their networks, to determine if data from their tablets and phones is being compromised. The results often leave corporate leaders at a loss for words.

"They're stunned most of the time, and there's a sense of panic," says **Kevin Johnson,** a Senior Security Analyst with Secure Ideas. "When I present them with a list of their email addresses and text messages I was able to obtain, they start to freak out."

"Mobile devices are one of the biggest risks around," says Johnson. "Sure, there's always computer malware to deal with, but when you're dealing with smartphones and tablets, it's a widely unexplored area. They've become ridiculously common and have the ability now to rival laptops. Companies hire us to get a realistic assessment of the risks they're exposed to. They want us to find the flaws."

Understand the risk

Johnson, who has a background in development and system administration, has years of experience performing security services for Fortune 100 companies. He says companies must understand what can happen when their systems are compromised.

"If they don't know how vulnerable they are, how can they expect to correct the problem? It comes down to awareness—understanding what you're opening and what you may be exposing yourself to. That's why hiring a firm specializing in security, or at least becoming educated about risks, is key. Companies need to know whether hackers can steal their data and their clients."

An instructor who's been tinkering with computers since high school, Johnson says mobile device platform flaws expose users to attacks.

> "It comes down to awareness—understanding what you're opening and what you may be exposing yourself to. That's why hiring a firm specializing in security, or at least becoming educated about risks, is key."

Kevin Johnson
SANS Institute Instructor, Senior Security Analyst, Secure Ideas

Check for vulnerabilities

"One of my favorite ways to get data out of an organization is by creating a mobile application. It can be a game or an application that's related to their business. For a retail store it could be an app that pretends to be a price checker. I send an email saying we're about to release a new app but want to test it, so they'll need to install it on their Android, for example. Once they install it, I use a geo-locator to determine if they're in the corporate office. If so, there's a good chance the mobile devices are connected."

According to Johnson, "We're seeing the exact same flaws that we used to see in desktops in the 1990's now in the mobile space. The developers have this mindset that mobile is brand new and they are forging new trails."

CINDY RILEY
editorial@mediaplanet.com

INSIGHT

Michael Sutton

Vice President of Security Research, Zscaler

Cloud solutions for real-time defense

Today, attackers are leveraging legitimate resources to target unsuspecting victims. Whether poisoning Google's search results, infecting legitimate sites or hosting malicious content on social networks, hackers are manipulating resources that users already trust. Attacks are also increasingly intelligent, triggering only when a victim's machine is likely to be vulnerable and laying dormant.This creates a challenging environment for end-users and those tasked with defending them. Today, companies need to seek security solutions capable of inspecting all web traffic in real-time—regardless of the device being used or where the employee is working from. Today's ever-increasing mobile workforce is leading enterprises to consider flexible, cloud-delivered security solutions—those that empower enterprises by protecting every user, on every device, everywhere they are.

> "Today, companies need to seek security solutions capable of inspecting all web traffic in real-time."

MICHAEL SUTTON

editorial@mediaplanet.com

DON'T MISS!

Creating trust in the cloud adds value to the cloud

Ron Knode
Co-Director, Cloud Trust Protocol Initiative, CSA Steering Committee

The realization of enterprise benefits from the elastic nature of cloud processing is perhaps the biggest (potential) digital trust payoff ever. Can we capture the elastic payoff by putting trust in the cloud? Can we "trust in the cloud?"

- Secure cloud processing must offer more than just economy. Consequently, "security" in the cloud is not enough. "Trust in the cloud" is necessary to create new enterprise value.
- There is no shortage of research efforts, study programs, and consortia of all kinds trying to provide advice, structure, and clarity to the discipline of cloud processing, and in particular the security and privacy issues surrounding cloud processing.

For the full report: http://assets1.csc.com/cloud/downloads/wp_cloudtrustprotocolprecis_073010.pdf

41%

- **By the year 2016,** the job outlook for all professional and related occupations in the Information Technology field is expected to grow 41 percent.

SOURCE: U.S. BUREAU OF LABOR.

NEWS

BEST TIPS FOR BUSINESS & DATA

Educate your workforce

Make sure your employees know a simple fact: no business is 'too small' to be targeted by cyber crime.

Loose clicks sink ships

It's a sad truth, the majority of cyber-incidents can be traced back to a single mistake made by an unsuspecting person.

Close vulnerabilities

Make sure your workforce is equipped with current software,and convey the importance of accepting software updates when prompted.

Make sure to backup

The time you spend setting up a data backup system is a pittance compared to the monumental hassle of retrieving data from a broken hard-drive on an employee laptop.

GARY MULLEN
editorial@mediaplanet.com

Information Technology plays a crucial role as companies look to the future

Demand increases for IT professionals with graduate degrees

The numbers tell the story. By the year 2016, the job outlook for all professional and related occupations in the Information Technology field is expected to grow 41 percent ,according to projections by the U.S. Bureau of Labor. Gurvirender Tejay, Ph.D., Associate Professor of Information Security with the Graduate School of Computer and Information Sciences at Nova Southeastern University, says cyber security is emerging to be a discipline in itself.

Gurvirender Tejay, Ph.D. Associate Professor of Information Security, Nova Southeastern University

”This field is very demanding and constantly changing. Most of the hacker groups now operate as an organization with well-defined structure and roles.They also employ malware development teams. These groups encourage young hackers through apprenticeship programs. In contrast, we do not see many organizations coming forward with mentorship programs to nurture Cyber Security students.”

Advancing in your field

Tejay adds, ”Pursuing graduate education can assist individuals to advance in their fields to become senior executives.A successful information security executive needs to have good grasp of technical security issues balanced with sound understanding of organizational challenges. In my opinion, we now need a Professional Doctorate in Information Security—an intermediary degree between Masters and traditional doctoral degree.”

Tejay explains, “We offer both Masters and Doctoral programs in Information Security. For students interested in organizational cyber security,we offer MS in Management Information Systems with concentration in Information Security Management. We also offer a degree in Computer Science with emphasis on technical cyber security.”

Beginning in the fall of 2012, Carnegie Mellon University's Information Networking Institute will offer an Executive Master of Science in Information Assurance (ExecMSIA) for mid-career and information technology executives who want to advance their careers in the area of information assurance. The ExecMSIA offers a concentration in Cyber Forensics and Incident Response or Resilience Management.

Nicolas Christin, Ph.D., Associate Director of CMU's Information Networking Institute, explains, “The amount of security training IT professionals undergo has not kept up, so we're now in a situation where people face a greater danger,without having the expertise needed to make rational, informed decisions. Information security is not something you can purchase and just tack on to a product -- it's an entire process that has to become part of a company's culture.

“ You can find fairly easily toolkits that make it a snap to attack a target. You don't need to be an expert to actually inflict damage to a victim, but the potential victims have to be expert to deflect these attacks. Today's and tomorrow's IT top-level managers need to understand IT security as much as they understand business processes.

CINDY RILEY
editorial@mediaplanet.com

INSIGHT

Question: What can companies do to protect the most vulnerable areas that hackers target?
Answer: Organizations must take the necessary steps to educate employees, secure IT infrastructures, and share intelligence to improve security for the public and private sectors.

STEP 3
TAKE A RISK-BASED APPROACH TO SECURITY

Protecting your organization: Security in the face of advanced threats

Organizations around the world today are facing the challenge of managing vast amounts of data even while they are trying to take on new initiatives.

New initiatives such as migrating IT services to the cloud, taking advantage of new productivity-enhancing web applications or embracing innovative tools like mobile devices, smartphones and social media are now being embraced by companies.

This growth of digital information and new openness of computing is creating incredible new opportunities for collaboration, communication and innovation, but it's also creating new vulnerabilities that cyber criminals, hacktivist groups and nation states have learned to exploit.

Attacks are getting more sophisticated and targeted—moving way beyond identity and credit card theft. Today we're seeing nation states stealing intellectual property from enterprises in order to gain economic advantage.The defense establishment has been experiencing these types of attacks for many years, but it now seems that any organization with high-value assets is on the hit list.

What can organizations do?

The good news is that there are measures organizations can take that can ensure that the benefits of our increasingly-digital business world are not overshadowed by the threats. Organizations can start by taking a risk-based approach to security. They need to determine who would most likely want to attack them, why they might be targeted and take the necessary security measures to protect the "crown jewels" of their organization. Organizations must realize that their employees WILL make mistakes. They will click on links that they shouldn't. Education is very important, as cyber criminals are now targeting the employee to gain access to an organization's critical information. But now that people are the new security perimeter, organizations must assume that some attackers will get into their IT infrastructures. Therefore, organizations must create security systems that will recognize the enemy within quickly, protect their information assets, and render attacks harmless. Intelligence gathering should also continue as a primary core competency for any organization's security team. To that end, being effective in combating advanced threats will require government agencies and corporations to share intelligence to build trust to benefit organizations as well as improve security on the whole for both public and private sectors.

"Attacks are getting more sophisticated and targeted—moving way beyond identity and credit card theft."

Tom Heiser
President, RSA, The Security Division of EMC

Share insights

To help organizations address escalating threats, RSA enlisted the help of the Security for Business Innovation Council (SBIC), which consists of global information-security officers from Fortune 1000 companies, to share insight into these increasingly menacing attacks. Their recommendations are compiled into a report entitled "When Advanced Persistent Threats Go Mainstream: Building Information Security Strategies to Combat Escalating Threats". The report offers seven concrete recommendations for evaluating advanced persistent threats and implementing appropriate security strategies. To read the guidance and the how-to strategies, please download the full report at: www.rsa.com/APT.

TOM HEISER
editorial@mediaplanet.com

DON'T MISS!

David Pack, Manager of LogRhythm Labs

The maturing cyber crime economy and supply chain—It's "When" not "If"

Hacking is as old as computing itself. For years there have been online communities where black hats (i.e., the bad guys) exchange ideas, share tools and exploits, and brag about their latest achievements. But a mature cyber crime economy and supply chain have emerged virtually overnight in a way that's forcing organizations of all shapes and sizes—from Fortune 500 companies and large federal agencies to community banks and local hospitals—to think very differently about information security.

Today, cyber criminals have ready-access to for-sale malware, exploits and for-hire resources necessary to perpetrate virtually any online crime or cyber attack. This ever-expanding supply chain acts as a force multiplier for online crime, hactivism and cyber terrorism. Most organizations, even those with the most sophisticated information security arsenals, realize that it's no longer a matter of "if" they'll be breached but "when."

Best practices dictate continuous monitoring of all activity across the enterprise, ongoing situational awareness and an ability to respond swiftly and effectively when events arise. Next generation security information and event management (SIEM 2.0) offers the most comprehensive platform for defense, detection and response amidst the mutating security landscape.

DAVID PACK
editorial@mediaplanet.com

ADVANCED STRATEGIES AGAINST ADVANCED THREATS

RSA®

EMC²®