TECHNOLOGY TIMES

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

By Computer Networks of Roanoke, Inc.

Serving Roanoke and surrounding areas since 2006

Volume 8, Issue 9 September 2015

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Hank Wagner, Owner/Founder
Computer Networks of Roanoke

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

Cybercriminals Now Have A Bull's-Eye On Small Business… Is Your Company's Data At Risk?

In a December 2014 survey by the National Small Business Association, 61% of small businesses reported being victims of a cybercrime within the past 12 months.

The average cost to recover from a cyber-attack skyrocketed from $8,699 per attack in 2013 to $20,752 per attack in 2014. And, of the businesses targeted, 68% said they'd been hacked more than once.

See Security Audit Page 2

INSIDE THIS ISSUE

Chinese Manufacturer of PCs Installing Unwanted Software

August 12 & 13, 2015
SANS Institute

Lenovo has been using code in the firmware of some devices to make unwanted software persist even after users reinstall operating systems.

Lenovo is exploiting Microsoft's Windows Platform Binary Table feature, which is built into Windows machines.

http://www.zdnet.com/article/lenovo-rootkit-ensured-its-software-could-not-be-deleted/

[Editor's Note (Ullrich): While nothing new, this level of "vendor root kit" puts Lenovo in its own class of creepiness. Not only does the system come pre-installed with a set of vendor supplied tools, but it will also actively intercept attempts to install the operating system from scratch, a common practice among more security conscious users.

Also note that a pre-owned system like this could easily be weaponized later by installing additional software.]

About Lenovo

While the Lenovo brand came into existence only in 2004, the company has a much longer history. In 1984, Legend Holdings was formed with 200,000 RMB (US$25,000) in a guard house in China. The company was incorporated in Hong Kong in 1988 and would grow to be the largest PC

See Lenovo Page 3

Security Audit continued from Page 1

Experts agree, as cyber-crooks become ever more sophisticated, the threat to small businesses is going to get worse before it gets better…

So what can you do to beat the bad guys?

Here are three common ploys used by hackers – and how you can fend them off:

Phishing – A really legitimate-looking e-mail urges you to click a link or open a file that triggers a malware installation on your computer.

> **Best Defense:** Don't let anyone in your company open files or click links in an e-mail unless they're certain who it came from.

Cracking Your Password – Hackers can run programs 24/7 testing password combinations. The easier your password is to guess, the more likely it is they'll crack it.

> **Best Defense:** Consider using a password manager that generates and stores tough-to-crack passwords. For extra security, use unique passphrases for financial accounts in case the manager gets hacked.

Drive-By Download – You visit what appears to be an innocent site; yet when you click, your device gets hacked – and you may never know it, until it's too late.

> **Best Defense:** Make sure your browser is up-to-date, or use one that updates automatically, such as Firefox or Chrome. Internet Explorer users have been found to be most vulnerable to these attacks.

Unfortunately, these three examples are just a small sampling of the dozens of ever more ingenious ways cybercriminals are breaking down the doors and destroying unprepared businesses.

Let us help! Call our office and receive a FREE Cyber-Security Audit to uncover gaps in your company's online security.

Our highly trained team of IT pros will come to your office and conduct this comprehensive audit. We'll then prepare a customized "Report of Findings" that reveals specific vulnerabilities and a prioritized Plan of Attack for getting any problems addressed fast. ❖

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

Do You Accept Credit Cards? Watch Out For These 5 Pitfalls That Could Lead To Lawsuits

If your company is not fully compliant with Payment Card Industry (PCI) Security Standards, you could be at risk of a serious tangle with attorneys. Technically, PCI guidelines are not a hard-and-fast set of laws. However, merchants can still face hefty liabilities for not meeting them.

Avoid these mistakes to keep your company out of hot water:

1. Storing Cardholder Data in Noncompliant Programs

Many states have laws regarding data breaches and, depending on where you accept cards, you may be subject to many of them. For example, Massachusetts has 201 CMR 17.00, which requires companies keeping any personal data from Massachusetts residents to prepare a PCI-compliant plan to protect that data. If a company then fails to maintain that plan, the business may face state prosecution.

2. Fibbing on the Self-Assessment Questionnaire

If you have considered tampering with the reports from your company's Approved Scanning Vendor, think again. Time invested now to fix any holes in your data security system could save you big-time from the penalties your company could suffer if there's ever a data breach.

The same thing applies to simply "fudging the truth" on self-prepared compliance reports. Even if you think it's a harmless stretch of the truth, don't do it.

3. Not Using the Right Qualified Security Assessor

Many companies use Qualified Security Assessors to help them maintain their PCI compliance. Every QSA does not necessarily know as much as another, however. It's important to select someone who both understands your business and stays up-to-date on the latest version of PCI Security Standards.

4. Trying to Resolve Data Compromises Under the Radar

You may be tempted to fix a customer's complaint yourself if they inform you of a data compromise. Not informing credit card companies of data breaches, however small, can lead to you no longer having access to their services. Those credit card companies can then file suit against your company, costing you big bucks in the end.

5. Not Checking ID for Point-of-Sale Credit Card Use

Sometimes it seems like no one checks IDs against the credit cards being used, so merchants tend to be lax about doing so. Unfortunately, running just one unauthorized credit card could cost you a lot in the long run.

Even if the state in which you do business does not have specific laws regarding PCI compliance, a civil suit may come against your company for any data breaches. The court will not favor you if you have not been PCI-compliant. ❖

Business Email Addresses Matter

By Karen Vujnovic,
Manta Staff Writer - August 21, 2015

Most of us have multiple email addresses, from Yahoo! to Gmail. There are even a few AOL addresses lingering in the shadows. But are these generic email addresses what a small business owner should be using? According to a Manta online poll, 41% of respondents use Gmail for their business, with 39% stating that a customized domain isn't necessary.

But even if you're a one-person show, your email address is part of your branding, and branding matters—and the poll reflects that. Over 89% of small business owners with customized email domains use them to showcase professionalism and branding.

Other reasons to consider a personalized business email address:

- Marketing emails are less likely to end up in someone's spam folder.
- Effectively manage email lists.
- Track opens and click-throughs. (Otherwise, you're sending emails willy-nilly and won't know who is engaged.)

In the end, having a customized email address give you a more polished and professional appearance and makes you far more credible to potential customers. ❖

Mobile Devices Pose Biggest Cybersecurity Threat To The Enterprise, Report Says

Network World | Aug 24, 2015 8:14 AM PT
http://www.networkworld.com/author/Zeus-Kerravala/

Earlier this month, Check Point Software released its 2015 security report which found that mobile devices have become the biggest threat for today's enterprises. I like the fact that more vendors are doing their own studies and sharing the findings. Cybersecurity has so many facets that it's very challenging for IT departments to understand where to focus their energy, so surveys like this help.

The survey revealed something that I think many businesses have turned a bit of a blind eye to, and that's the impact of mobile devices, primarily due to the wide acceptance of BYOD (Bring Your Own Device to work). The last Network Purchase Intention Study by ZK Research (disclosure: I'm an employee of ZK Research) showed that 82% of businesses now have some kind of BYOD plan in place. Even heavily regulated industries like healthcare and financial services are putting BYOD programs in place because of pressure from the lines of business. Years ago, CEOs and managers didn't want consumer devices in the workplace as they were considered a distraction. Today, businesses that do not allow workers to use mobile devices are putting themselves at a competitive disadvantage.

In actuality, it's not "BYOD" that's the real problem. It's the fact that these devices are mobile and can be connected from virtually anywhere. Whether the company or the individual owns the device, workers are still able to take it to an uncontrolled area, connect and do what they need to do to be productive. If the company owns the device, it's certainly easier to keep the device in compliance with corporate policy, but both individually owned and company-owned mobile devices pose a risk.

The Check Point survey found that organizations with more than 2,000 devices on the network have a 50% chance that at least six of them are infected. The survey also showed that almost three-quarters of respondents felt that the top mobile security challenge is protecting corporate information on mobile devices. This makes sense considering that workers will access company data from almost everywhere.

Think about the fact that workers will connect a mobile device to a public access point without knowing anything about it, particularly when cellular service is poor or when roaming and connecting over cellular is cost-prohibitive. We all want to work from anywhere and we'll use whatever means necessary to connect. Now, what if a worker is in a restaurant and, when browsing the list of available wireless networks, they find one called "Free City WiFi"? Most people would connect to this without thought. What if that happens to be a cleverly named access point in some cybercriminal's apartment above the restaurant, and they're capturing all of the information going to and from the mobile device? Corporate data is at risk when workers are off the company network, and it's critical that the proper steps are taken to secure the mobile devices.

The other risk that mobile devices create is that they could get infected when off the network and then spread that malware around when it reattaches to the business network. Typically, user connections don't need to connect by going through a next-generation firewall or an IPS system, so the only way to understand if the device is causing harm is to look at the flow information going to and from the device and quarantine it on anything anomalous.

I'm certainly not saying that businesses should ditch the BYOD efforts or stop supporting mobile devices. That would be business suicide, as workers would revolt. The important thing to understand is that an increase in mobile devices increases the chances of a breach, to the point where all companies should accept the fact that it's probably going to happen. There needs to be a focus on understanding what to do when the breach occurs and how to mitigate against it before serious damage is done. ❖

Lenovo continued from Page 1

Company in China. Legend Holdings changed its name to Lenovo in 2004 and, in 2005, acquired the former Personal Computer Division of IBM, the company that invented the PC industry in 1981.

Editorial Comment

So, you know:

- The US Government blames the recent Office of Personnel Management data breach on the Chinese, right?
- And, it appears that some Chinese PC manufacturer (Lenovo) is installing "back-doors" on the PCs they sell.
- And, that the Chinese are blamed for hacking into UCONN and the NY Times?
- And, the Anthem Healthcare data breach has been blamed on the Chinese?

Maybe we should not be buying Lenovo PCs and Servers. Just sayin'…

Mobile Devices from previous page

The Lighter Side:

Technology has forever changed our lives and our world more than you know. Here are some numbers to put that fact into perspective:

1. About 4 billion people worldwide own a mobile phone, but only 3.5 billion people own a toothbrush.

2. Computers and other electronics account for 220,000 tons of annual trash in the U.S. alone.

3. About 300 hours of video are uploaded to YouTube every minute.

4. Around 100 billion e-mails traverse the Internet every day, and about 95% of those messages go straight to spam folders.

5. The annual amount of electricity it takes for Google to handle a billion search queries every day is around 15 billion kWh, which is more than most countries consume.

6. About 500 new mobile games appear on the Apple App Store each day.

7. The "father of information theory," Claude Shannon, invented the digital circuit at age 21 while he was in college.

8. Regular computer users blink only half as often as non-users.

9. Over 1 million children can say their parents met on Match.com ❖

Predictable Results For a Predictable Fee

We do it all…HIPAA Security Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, IT Consulting.

And, we do that for businesses with as few as 10 PCs.

We are looking for a select number of new clients in the medical and professional services fields.

If you are dissatisfied with the level of service you are getting from your current IT Vendor, pick up the phone, call me, Hank Wagner, at 757-333-3299 x232, or email me: hank.wagner@computernetworksinc.com and we can chat a bit about your needs. ❖

David Rourk of Rourk Public Relations has rebranded his business to better describe his current work with web sites. We use them for Search Engine Optimization (SEO) which helps get our website on Page 1 of Google's search results.

Visit them at http://www.businesswebsiteexperts.com/ to see more about their services, and how they may help your business.