TECHMinutes

October 2012

Your Small Business Technology Information Source!

This Issue:

Discover new ways to protect your company from disaster and data loss at our Lunch & Learn Seminar

Ditch the lunch bag because lunch is on us.
October 18th 12:00pm—2:00 pm
330 Pony Farm Road, Oneonta NY 13820

Register NOW!
http://bit.ly/SFuRuj

About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Read past newsletters at:
newsletter.directive.com

6 Security Questions to Ask Your Pentesting Company

Prominent companies falling victim to hacker has become all too common in the news. Some of the larger breaches in security involve the compromise of thousands of customers' information. Definitely not the kind of press you want, not to mention the irreparable damage to your business. This can be a little scary for a small business owner, especially if you consider that these large companies have the best cyber security money can buy.

There are companies that test cyber security. This service is called Penetration Testing (or pentesting). Most hacking victims, both large and small, fail to utilize this service. Choosing a company to PenTest your system is important, not only for your security, but also for your company's reputation, and the safety of the customers' personal data. You do not want to just give anybody access to your system and have them prod around at it, you want a company you can trust. If you are looking for a reputable company to test your security, there are six questions you need to consider.

Are they experienced? How long has the security testing company been in business? What sort of clients do they work with? What type of training has the technicians received? Ask several questions about the capabilities of the company, it is also acceptable to obtain client refer-

(Continued on page 4)

Anatomy of a Hacker

If you have ever been the victim of a computer virus or cyber attack you know how bad it can hurt. You know the pain of having your data compromised or even your business operation completely shut down. You feel violated, and to add insult to injury, you have no idea who did this dirty deed.

Cyber criminals are always anonymous and clearly the bad guys, which would make us at Directive the sheriff in town, we are here to serve and protect you. Today, we want to pull back the curtain of anonymity, tack up a big wanted poster, and show you their ugly mugs.

These perpetrators have no regard for the law, or may even rationalize how the law does not apply to them. They obviously have technical knowledge and enjoy using their skills to manipulate and outsmart others. Some cyber criminals do it simply for the thrills and enjoy the risk and chaos they create, while others have more specific intentions like monetary gain. Additional cyber criminal motivations include: emotional reasons like revenge, political and religious loyalties, and even reasons that are sexual in nature.

We might picture cyber criminals huddled in groups, working in a dark warehouse, but a majority of the crimes would be classified as "petty" and are carried out by normal individuals acting alone. Part of the problem of cyber crimes is found in the variety of criminals it draws. Within

(Continued on page 3)

Connecting Home and Office

In a 2012 Wrike.com surveyed 1,074 workers, 83% of respondents reported working at home for at least part of the workday. Chances are, you have employees working at home, and they are loving it! In fact, employees enjoy working at home so much 78% would forgo free meals, and 25% would accept a reduction in salary, just for the opportunity to work at home!

Working at home is a great way to boost employee morale and productivity, and to make a good thing better, there are several policies and tools available to increase communication, provide better security, and take the productivity of your pajama-wearing employee to the max.

Giving your employee the ability to remote into your computer network from home is the key to their success. This enables the employee to save their work on a remote server, ensuring the data is protected, backed up, and accessible. The alternative comes with risk, if the employee saves their work on the hard drive of their local PC, not only can you not access the files, but you are also increasing the risk of data loss, especially now that kids and pets are added to the scenario.

The Cloud at Home and the Office

Making use of cloud computing to do work remotely is the ideal solution when working from home, the office, and everywhere else in between. With the cloud you can rest assured knowing that all data, from all connected workstations and devices, is backed up continuously. The cloud also adds another level of protection by allowing IT to directly connect and service any problems the employee may be experiencing.

Keeping in Touch and in Control

Worried about working from home causing productivity issues or giving access to your network to strange devices? Using both terminal servers and clouds to regulate remote access keeps all the controls, policies, permissions, and protections you have in place at your office also in place when the employee logs on from home.

Additionally, there are applications available that allow you to track employee access and monitor their time usage so you know they are not wasting time. There are also several available tools like instant messaging, teleconferencing, voip, and mobile smartphones that make communicating with your homebound employee so easy that you might even forget they are not in the office!
If you want to get the most from your telecommuting policies and technology, give us a call at 607.433.2200 and we will be happy to discuss the options available to you.

Share this Article!
http://bit.ly/SFraoi

Travel With Free Wi-Fi

Everybody likes the free goodies in a hotel room, tiny shampoo bottles, coupons to nearby restaurants, and HBO top the list. Wi-Fi however, our favorite goodie, sometimes fails to make the complimentary goodie list. It seems a little messed up to us, that hotels (the place you work and sleep) charge you for Wi-Fi while Burger King gives it away for free, but we have found a Wi-Fi loophole to help you out.

The loophole gives you free Wi-Fi in your hotel room, which is a great way to save on travel expenses. HotelChatter.com, a website that keeps tabs on hotel pricing, averaged the price of Wi-Fi usage per room at almost $14 per day.

Fourteen dollars may sound reasonable if your stay is only one night, but turn the trip into a five nighter and you just dropped $70 for Wi-Fi service. This sets up our loophole, you can buy and use a quality wireless router for under $70.

BYOR (bring your own router) works in any hotel room that has free internet access available through an ethernet port. Although, always remember this safety tip, an internet connection can be like a hotel room bedspread, you may want to think twice before instinctively hopping on. We highly recommend the router is configured before plugging in for maximum protection. Other safety measures, like using WPA security instead of WEP, and choosing a complex password, will keep the people from the room next to you, above you, and below you, from accessing your data. And when configuring your router, remember that network security is our forte at Directive and we would be happy to look over your router before your trip.

If you lack the luggage space to bring a router and you own a smartphone, you have an even easier option to get free Wi-Fi in your hotel room. This loophole is called tethering and involves hooking up your smartphone to your laptop and using the phone as a router. This is extra safe because you own the internet con-

(Continued on page 4)

Anatomy of a Hacker

(Continued from page 1)
the hacker community a class system exists based on an individual's technical expertise and the potential damage one can cause.

- **Toolkit Newbies**. Technical novices who generally download illegally from the internet.
- **Cyber Punks.** Capable of writing programs able to deface websites. Spamming and phishing for identify theft also falls within their skill set. They are usually boastful of their hacking success.
- **Coders.** Write code solely for the purpose of damaging other systems. Their motives are ulterior and spyware and Trojans are primarily used.
- **Old-guard hackers.** Hacking is a sport for the old guard, they treat it as a mental exercise. They are highly skilled and do not cross the criminal line.
- **Hacktivist.** This group is the fastest growing and they can cause big damage. They are politically or socially motivated and receive funding from other groups who share their agenda.

Due to the complexity of computer networks, cyber criminals are particularly hard to catch, the crimetrail usually ends at a computer. In fact, only five percent of cyber criminals are actually caught and prosecuted. This leaves them with a 95% chance of getting away with it, which only goes to embolden their actions.

Simply because a cyber criminal is hard to catch, does not mean it has to be easy for them to succeed. You can protect yourself by keeping your antivirus software up-to-date and training everyone who uses your network to know what to look for with email phishing scams and scareware popups. Having a sheriff on your side to watch your back is the best defense against attacks from these cyber creeps, at Directive we want to be your sherriff. We can manage your antivirus software, identify weaknesses in your firewall, as well as provide you with other defensive techniques. Give us a call at 607.433.2200 and let us serve and protect you.

Share this Article!
http://bit.ly/SFqJKO

5 Tips to Make Yourself a Better Presenter

Speaking to a crowd, especially one comprised of your peers or potential clients, is a nerve wracking experience. All too often, a speaker will put all his/her effort into a PowerPoint with graphics worthy of James Cameron or distracting animations that spin, sparkle, and pop. As the speaker, you're the focus. Here's a few tips to keep your audience captivated:

Your PowerPoint is Just a Guideline

When speaking in public there is always the temptation to plan a script. One of the biggest mistakes that a speaker can make is worrying about following the script, when they should focus on being engaging and informative. If you know your material and know your major talking points, then just let the visuals be secondary.

Location, Location, Location.

Consider the venue that you're giving your presentation. Even when you're speaking somewhere for the first time, try to get an idea of the room layout. This should affect how you prepare for the speech by adjusting your volume, projection, and eye contact to fit the type of room. In some cases, you may even want to tweak your presentation to suit the audience size.

Practice Makes Perfect

Once you're comfortable with the material you've outlined, it's time to bring your game to a friendly audience that will offer constructive criticism. Speaking in front of your peers will help you transition from talking to yourself to talking to an audience. It'll help you figure out which lines work and which don't and will help you retain the audience's attention.

Only YOU Can Make a Presentation Interesting

It's nice to have a PowerPoint with graphics to help convey your point, but you need to be the focus. In fact, when preparing a presentation, consider the chance that the projector will blow a bulb and you'll have to fly solo. If you know your topic that well, and you can address all the points to convey everything you intended to without the PowerPoint, then you'll capture the room's attention.

Q&A: Save Time for Questions

After you finish your presentation, open the room up for questions and interaction. Obviously, don't give a presentation on a topic you don't know much about - audience members like to come up with challenging questions. If you don't know an answer, it's best to say "That's a great question, meet me after the presentation and get me your email, I need to run that by my team." Then, of course, be sure to follow up.

Share this Article!
http://bit.ly/SFsw2z

6 Security Questions to Ask Your Pentesting Company

(Continued from page 1)

ences and ask them about the quality of service they have received.

Do the testers belong to a standardizing organization? Ask the security company about the background checks they perform on their employees. These are the people to whom you are handing over the keys to your castle. It's important to make sure they are not hired hackers in disguise. Good Penetration Testing companies have layers of background checks in place, and partner with organizations that certify technicians. A trustworthy PT company will share this information with you.

What certificates and degrees have the testers obtained? In the same way you would call the college and double check the education of an applicant applying for a high level job. You can also check with the standardization agencies that certifies the pentesting company. Be sure to also check with the agency, what is the current level of certification for the prospective company?

Are they equipped to handle the testing of an organization such as mine? Within the different companies that offer Penetration Testing, there are various schools of thought in regards to different methods of security testing. Talk to the PT company about your specific security needs, and get a feel if their methods will work for your organization.

Does the contract protect your company's network and hardware? Before you let someone else tinker with your networks and systems, be sure to cover liability. Just like you would make sure a contractor is fully insured before giving him access to your home, so it is with Penetration Testing. It is best practice to draw up a contract making the PT company liable if they damage your system.

Get to know your Penetration Testing Partner, it is important that you are comfortable with the team you give access to your information too. Double check their credentials and make sure they have the skills to make your network impervious to hackers, because 'once you've been hacked, there ain't no goin' back'. Contact us at Directive at 607.433.2200, we will be happy to discuss with you different solutions for your security needs.

Share this Article!
http://bit.ly/SFq8sr

Travel With Free Wi-Fi

(Continued from page 2)

nection. Tethering is not without a few drawbacks, phone connection speeds determine internet speed, and phone data is usually capped, so remember to check how much data you have left in your plan, before you leave the router at home and hop on a plane.

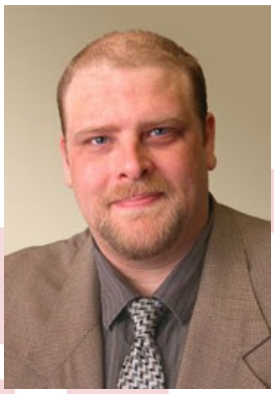
There is a positive trend developing in the hotel industry, in the spirit of competition, more and more hotels are giving away Wi-Fi. Other hotels are shifting to a tiered pricing plan for different speeds of Wi-Fi. . . .

Read the rest Online!
http://bit.ly/SFrLGH

???? NEED HELP ????

Live Chat Support is available for all your account, technical support or billing questions or concerns.

To use the service go to www.directive.com and click the Live Chat Support link at the top of the page.



Chris Chase
Solutions Integrator

Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
newsletter@directive.com