June 2014

TechTidbit.com

brought to you by Tech Experts

Seven Smart Tips To Secure Your Business Network

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Hackers are constantly on the lookout for digital data they can use to make a profit, either by stealing money electronically or by selling the information to third parties.

Therefore, it is important to protect your precious data; here are seven tips to get you started:

Policies

Your staff is the front line of defense against hackers. Human error is one of the leading causes of data security breaches, so you need to have policies in place to ensure your employees are promoting the security of your network while working.

Strong passwords

People generally opt for simple easy-to-remember passwords that hackers can easily crack.

A simple "dictionary attack" (using an automated tool that uses a combination of dictionary words and numbers to crack passwords), is sufficient to uncover many passwords.

On the other hand, coming up with a complicated password and saving it to your computer as opposed to writing it down is a simple but very effective way to prevent hacks.

Multi-factor authentication

It is highly advisable to establish multiple layers of technology dedicated to security that you would apply to all your devices, including desktops, mobile devices, file servers, mail servers and network end points.

Multiple security blocks hacking attacks and alerts you to any problems beforehand so you can take the appropriate measures.

Data encryption

Encryption is yet another great security tool that you can use to protect your data. For instance, if your hard disk is stolen or your USB drive is lost, anyone trying to access your data would be unable to read it if it is encrypted.

Backup

Security makes up half of your data protection, while a proper backup strategy makes up for the other half. Even with great security, you need to be able to recover your data if you have a failure. Back up often, and remember to test the backup regularly.

Audit

You need to identify the vulnerable areas of your network or which data needs to be protected.

Your entire IT infrastructure, including your computers, mobile devices and network should be audited by a professional IT specialist to determine the appropriate steps to prevent hackers from accessing your data.

Managed services

Managed services are an alternative and highly-effective approach for achieving the best possible security, including backup and recovery.

Many small businesses are unable to adequately meet the daunting and expensive task of securing their data.

With a managed-service provider specialized in data security, you get the benefit of professional services and skills without having to hire an in-house security expert, thus cutting on costs. In addition, you get access to the latest security technology and support professionals.

What Happens To Stolen Data After A Breach?

Michael Menor is Vice President of Support Services for Tech Experts.

Data breaches have become so common that virtually everyone has been impacted by a breach in some way. Breaches at big retailers make the news, and replacement credit cards ominously arrive in the mail from our banks.

However, there is a lot more to most data breaches than meets the eye, as is the case with more traditional robberies, the theft of data is often just the beginning of the crime. If criminals can't use or sell stolen data without being caught, then the data quickly becomes worthless. As a result it's critical to understand what happens to data after a breach.

Understanding the Criminal Infrastructure

While "hacktivist" groups will periodically expose data to further an ideological cause, the vast majority of breaches are perpetrated by criminal groups focused on financial profit. Since very few of these attacks result in the direct theft of currency, criminals need a way to turn their stolen data into money.

Even in the simple case of stolen credit card information, criminals either need to sell the cards to other criminals or use the cards directly to commit fraud. In either case, the card data itself is a precursor to future fraud.

This may seem incidental at first, but there are important consequences. Specifically, the ability to monetize stolen data requires a very different set of skills than those needed to breach a network in the first place.

A network breach can be a relatively targeted operation perpetrated by a few attackers. However, once a breach is successful, the scale of the operation changes entirely. Whether the stolen data is personally identifiable information (PII), payment card data, or login credentials, the attackers face a challenge of scale. Millions of individual records need to be monetized either by reselling them or using the data directly for profit.

The sheer volume of data makes it impractical to do these tasks manually, and this is where cybercriminals need help. In most cases help arrives in the form of botnets that can automate the processing of individual records, and a larger ecosystem of organized crime that can consume the stolen data. Here are a few examples.

Direct Financial Fraud

Payment card breaches such as the recent attack against Target have obvious financial impacts and motivations. Yet while it is relatively simple for a criminal to derive value from an individual stolen credit card, doing the same for millions of cards is another thing entirely.

This is where the larger criminal ecosystem comes into play. The attackers behind the breach will sell the stolen card data to brokers, who in turn sell cards in batches to lower level criminals who use the data to either buy goods online or print cards to be used in physical stores.

This ecosystem shares a common problem in that stolen credit cards have a very limited shelf-life. As soon as it becomes apparent that a specific merchant has been compromised (Target for example), all of the compromised cards will be quickly deactivated.

This means that freshly stolen and active cards are highly valuable ($100 or more), while older cards can be worth pennies. This is a serious spread, and criminals need to know which sorts of cards they are buying, and the state of the cards they are holding.

To address this challenge, criminals will periodically test a subset of their cards by using them to make small online purchases. Attackers can drop a few hundred credit cards into a botnet programmed to make small purchases, and quickly determine the percentage of cards that are active and working.

Oddly enough, charities such as the Red Cross are a common recipients of these charges because they commonly receive small donations, and the purchase is unlikely to raise red flags with the consumer. Disrupting these validation steps could provide an interesting way to devalue the black-market price of stolen cards, and make the attacks less profitable for an attacker.

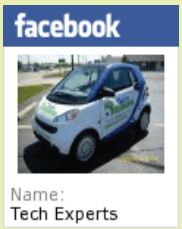
Stolen Credentials

End-user credentials (usernames and passwords) are another common target of attackers, and can provide considerable long-term value for additional attacks and fraud.

Unlike payment cards, there are no centralized authorities to deactivate compromised usernames and passwords in the event of a breach. A website that is compromised may

Continued on page 4

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

Advice For Small Business Owners Overwhelmed By Technology

Scott Blake is a Senior Network Engineer with Tech Experts.

A recent study by Brother International Corporation and SCORE found that 64 percent of small business owners feel overwhelmed when it comes to technology, because they have limited resources in information technology (IT).

Surprisingly, this isn't related to a lack of financial resources, but rather this is due to the fact that many of them do not have the proper technological guidance.

Most of them have no dedicated IT support, and 59% of the survey participants said there are insufficient resources available in small business communities to help them.

Keeping pace with tech trends

According to the study, mobile devices are the most important piece of technology for their businesses, because mobile technology allows for easy and quick reach as well as easy access to documents, regardless of where they are.

Customer Relationship Management (CRM), social media and cloud services are also among the tech tools that small business owners find necessary in running their businesses. Forty nine percent (49%) of business owners consider tech-related investments as their top priority.

However, about half of them are hesitant to invest in it too quickly without a good ROI (return on investment), while the other half are concerned that failing to invest in technology gives their competitors an advantage.

Solutions

Outsourcing IT is one alternative for small businesses to take advantage of technology without heavily investing in it.

Social media is also a convenient tool that many IT service providers use to provide tech support to their clients, while office technology products are becoming more user-friendly.

Another important step that small businesses must take as far as IT is concerned is to identify and outline their business processes.

This makes it easier to sort through the best technology to meet their business needs. It also eliminates the frustration experienced at the endless pitches small business owners get from vendors and solution providers that do not even understand their business goals.

Recommendations

When you understand your business processes, you can easily determine the technology that you need or don't need.

Take advantage of the tools available to help you understand the channels that are driving your business, including apps like Google Analytics. Finally, when using consumer apps for your business, go for the business options as they usually offer more security options and tech support.

Are You Losing Customers Because Of Your Website's Loading Time?

The amount of time a page takes to load is undoubtedly an important part of any website's user experience. The fact is that website visitors care more about speed than all the bells and whistles you add to your website.

In fact, page loading time also affects your search engine rankings. Here are a few additional facts to consider:

On average, consumers expect a web page to load within 2 seconds, with a significant portion of online shoppers abandoning a website that takes more than 3 seconds to load. Additionally, customer satisfaction is decreased by a 1-second page load delay and discourages them from buying from the same site in the future.

Measure your website speed

Page Speed Online is Google's free web-based tool that allows you to easily and accurately measure the speed of your website online.

It also provides an overview of the high, medium and low priority fixes that would help increase your page speed.

However, the suggestions may be fairly technical, and you might need professionals to let you determine which ones are feasible for your site. Some of the ways you can decrease page load time include:

•Enable GZIP compression to reduce the bandwidth of your pages and reduce HTTP response.

•Optimize your images by selecting the ideal size, format and source code.

•Enable browser caching to reduce the number of components that need to be downloaded for subsequent visits.

•Use a content delivery network (CDN) to deliver content more efficiently to users based on their location.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Google+ Basics You Need To Know

While Google+ may not boast the same popularity that Facebook enjoys, it is becoming harder to ignore. If you are just getting started on Google+, you need to wrap your head around its workings. Here are some basic features to get you going:

The Stream

This is the main home screen for Google+ where updates from people you are following show up in card-like boxes. To pull up public posts related to the same topic as that of a particular post, click the hash-tag on its upper-right corner.

Circles

These are groups that help you organize and manage your social experience. Whenever you follow someone new, you assign the person to a circle, which could be for friends, family, acquaintances or people you don't know personally.

You could also add your own customized circles. With circles, you get to focus on content from the specific group of people you want, although you can also view content from everyone. Circles are also useful for controlling who sees what you post.

Finding people

When you first sign in to Google+, the system walks you through a number of steps to locate people you know and to connect with interesting users you may not yet be acquainted with.

Notifications

Google+ uses notifications to let you know when something happens on the network that is directly relevant to you. You can access your notifications by clicking on the bell at the top-right corner of the screen.

Chats and Hangouts

Google's Hangout messaging system is integrated into Google+ so you can chat with other users and initiate video calls from within the service. Simply click the "Hangouts" link at the top-right corner of the screen and then click on any contact's name to open a chat session. Clicking the video camera icon will send the person a video chat request.

What Happens To Stolen Data After A Breach, Continued

lock out affected users so that they have to change their passwords, but there is nothing keeping an attacker from using the stolen credentials at other sites.

A 2011 study from PayPal unsurprisingly found that 60% of users reuse passwords at multiple sites, meaning that a breach at one site can easily spider out to other sites around the Internet.

In order to find sites where credentials are re-used, attackers again turn to botnets in what are called credential stuffing attacks. In these attacks, stolen credentials are fed into distributed botnets, which in turn slowly and deliberately test those credentials against high-value websites.

These attacks can afford to be patient, and will slowly test logins from many different IP addresses to avoid rate and reputation-based triggers that could expose the attack.

This strategy can transform a seemingly innocuous breach into something far more serious. If an attacker is able to take-over a victim's account on an e-commerce site, they could easily commit fraud in the victim's name.

Such fraud may take longer to identify because the attacker is using the victim's real account and from a site that the victim is known to use.

Credentials to social media sites are also highly valuable, enabling an attacker to easily impersonate the victim and infect his or her social networks.

Likewise, compromised personal webmail accounts can be a goldmine for an attacker. Such access not only provides the attacker insight into the victim's identity, but can also be key to breaking into additional online accounts.

Most sites and applications have an option to reset or resend a user's password to the email address on file. If the attacker has access to the victim's email account, he can again use a botnet to proactively find online accounts where that email is used, and then obtain or reset the victim's password.

These are just a few examples, but it serves to illustrate why it's important for security teams to consider the lifecycle of stolen data.

In order to monetize a breach, attackers often need to go through additional steps, and this provides additional opportunities to mitigate the effects of a breach.

Likewise, companies can insulate themselves from the impacts of breaches elsewhere on the Internet by knowing how criminals attempt to automatically use stolen data.

This of course won't prevent breaches from happening in the future, but it certainly is possible to mitigate the damage.