TotalTechCare
TOTAL TECHNOLOGY SUPPORT

TECHMinutes

August 2016

Your Small Business Technology Information Source!

This Issue:

The Internet Dramatically Changed the Publishing Industry. What About Your Field of Expertise?

It's well-known that publishers are a major component of an author sharing their work with the world, but recent innovations threaten to disrupt the status quo of the industry. Like many industries, the publishing industry has been...

Read the Rest Online!
http://bit.ly/29tpR10

About Total Tech Care

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.

Visit us **online** at:
totaltechcare.com

Business Continuity and Disaster Recovery Go Hand in Hand

Businesses are volatile entities that can change drastically at any given moment. All it takes to eliminate data and cause disaster is an unexpected natural disaster, like a flood or fire, or a hardware failure that wipes out mission-critical data. The fact remains that your organization could face significant downtime from data loss, and the future of your business could hang precariously in the mix.

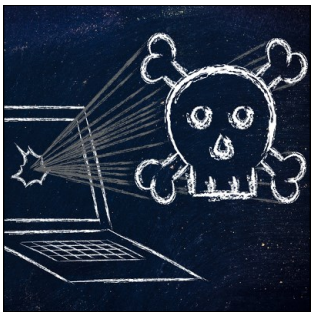
Why Backup and Disaster Recovery is Necessary

If your business doesn't have a reliable way of recovering from a data loss incident, you need to implement one as soon as possible. It's been proven time and again that businesses that fail to recover their data within seven days of the incident, will likely go out of business within one year. Here are some of the most common reasons why data loss disaster is so prevalent in the business world.

- **Natural disasters:** Floods, fires, electrical storms, tornadoes, hailstorms, and more, all have the potential to wipe out your physical infrastructure, and in turn, your digital assets. Therefore, you need to take steps to implement backup and disaster recovery tools, especially if you live in an area that's prone to weather hazards.
- **Cyber attacks:** Data breaches are known to cause data loss, either due to the destruction of data, or the theft of it. Furthermore, due to the unpredictability of what a virus or malware can do to your infrastructure, it's recommended that you try to avoid cyber attacks as often as possible. In particular, ransomware can lock your data away and

(Continued on page 3)

Threat Spotlight: How to Stop Brute Force Attacks



Hackers of all shapes and sizes use brute force attacks to gain access into accounts and infrastructures, but do you know how they work and what your business can do to protect against them? Failing to understand brute force attacks could put sensitive information in the crosshairs of hackers, and leave it vulnerable to ongoing attacks.

What Are Brute Force Attacks?

A brute force attack consists of a hacker repeatedly assaulting a login form with credentials at an incredible rate, hoping to crack the code and gain access without knowing the password to the account or system login. Most brute force attacks are performed by an algorithm that's designed to rapidly input thousands upon thousands of credentials every second, hence the term "brute force." Since it takes a more deliberate and frontal assault, rather than using a discrete or intellectual path, it's considered more straightforward and forceful. Though there are many types of brute force attacks, one of the most common is called a dictionary attack, where password attempts are systematically generated with popular words pulled from the dictionary in order to access the system.

Why They're a Problem

McAfee Security reports that in 2015, brute force attacks accounted for about 25 percent of all online hacks, second only to Denial of Service attacks. Perhaps this is due to how

(Continued on page 2)

Threat Spotlight: How to Stop Brute Force Attacks

(Continued from page 1)

straightforward these attacks are, since they are deliberate attacks that don't require skirting around security measures. Those behind brute force attacks know that they will be caught, which makes them particularly dangerous, since all caution is thrown to the wind and forgotten. These types of attacks are used to access accounts or system infrastructures in order to steal credentials like credit card numbers, Social Security numbers, and other data.

Plus, brute force attacks can be used to install a rootkit on a device, or turn a PC into a zombie bot. It's not uncommon for brute force attacks to be used as a jumping-off point for other major threats.

What to Do

A security solution that can lock out users based on IP location or failed login attempts is one way to protect your business from brute force attacks, but if the attacker is executing the campaign with a botnet, these measures will be limited in their ability to protect you. Botnets consist of several infected computers with various IP addresses, acting as individual users, thus rendering your security measures useless.

One other technology that can be effective at eliminating brute force attacks is two-factor authentication. In addition to your password, two-factor authentication provides an extra layer of security. Basically, if hackers don't have access to your physical device or a secondary email account, they won't be able to get the second code required to access your account or infrastructure. Two-factor authentication is a great asset in general, so it's worth taking into consideration regardless of what type of business you're running.

Your business should be equipped to handle all types of online threats, particularly those which are dangerous and present a significant threat. Total Tech Care can help your business integrate solutions designed to maximize your organization's security and continuity. To learn more, give us a call at 866-348-2602.

Share this Article!
http://bit.ly/29tn0Fo

Do You Agree with BYOD? 72 Percent of Businesses Do

Mobile devices have grown extraordinarily popular in the workplace. Organizations find them to be of considerable value for staying connected and getting work done while outside the office. This trend has presented a serious risk in the form of network and data security. How can businesses support mobile devices in the workplace, without compromising on the security of the device and the data it holds?

Data leakage is one of the major pain points of businesses that allow employee-owned mobile devices in the workplace. Every business has sensitive information that needs to be secured from malicious entities, no matter how benign it seems. As the business owner, it's your responsibility to ensure that you have a policy put into place to protect your data. In the case of mobile devices, you need a Bring Your Own Device (BYOD) policy that dictates how an employee uses their mobile devices for work purposes.

A recent study by Bitglass shows that 72 percent of various organizations, including financial, technology, healthcare, government, and education, feel that BYOD should be supported for at least some of their employees. As for mobile device management, which is an organization's control over devices used by employees, only 14 percent of organizations used solutions that protect data with device encryption. This is a significant difference that reveals a tricky situation: company's like the idea of BYOD, but don't (or aren't able to) implement a mobile device management solution.

Naturally, you can't let your business be the next to lose information due to mobile security threats. Implementing a mobile device management solution from Total Tech Care can help your business retain complete control over the data that's stored on your employees' mobile devices. You can restrict access to data based on work role, whitelist and blacklist app data, and even remotely wipe devices:

- **Whitelisting and blacklisting apps:** Some applications will request access to information stored on a mobile device, but some won't have any real reason to have access. For example, a flashlight app has no business accessing your phone's contacts or geographical location. By whitelisting and blacklisting apps, you can minimize your data's exposure to threats.
- **Role-based user access**: One of the easiest ways to minimize danger to your organization's data is to limit who has access to it. By integrating role-based user access, you can allow your team to access data that they need to do their jobs properly, and keep them from accessing that which they don't.
- **Remote wiping:** Sometimes the best way to prevent a data breach Is by remotely wiping data from a lost or stolen device. You shouldn't rely on a lost device showing back up, especially if it were left in a public place like a bus or subway station. You should always be prepared for a worst-case scenario like this...

Read the Rest Online!
http://bit.ly/29to1No

Business Continuity and Disaster Recovery Go Hand in Hand

(Continued from page 1)

force you to pay a ransom. More often than not, having a data backup solution is the only way to get your data back without shelling out the big bucks.

- **User error:** One of the most common causes of data loss is user error. People make mistakes, and even those who have access to data for the purpose of fulfilling their day-to-day duties could accidentally delete a file or move it somewhere it's not supposed to be. Also of note, users may accidentally hand over credentials to hackers performing phishing scams, which can be a major problem.
- **Hardware failure:** It's inevitable that your technology will grow old and be rendered obsolete. It's your responsibility to notice the warning signs and to replace your technology before it fails. If a critical server component were to go down, you would experience not just downtime, but massive data loss.

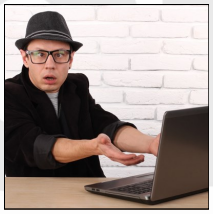
What You Need to Look For

Depending on your business's specific needs, you'll require a data backup and disaster recovery solution that's designed to take regular backups and rapidly recover data, among other things. Here are three topics to consider when determining which kind of BDR solution that you want for your business.

- **Cloud and off-site backup:** You don't want to store your data backups on in-house tapes. Rather, you want them secure in an off-site location, like the cloud or a data center. This way, you can know that your data is stored in a compliant location that can't be damaged by natural disasters.
- **Quick recovery time:** You want to be able to rapidly deploy your business's data to your infrastructure in order to minimize downtime. Tape backup can make this part of the recovery process long-winded and...

Read the Rest Online!
http://bit.ly/29tksXN

If Your Network is in the Cloud, What Do You Do with No Internet?



Thanks to the advancements of virtualization and cloud computing, many businesses are hosting key parts of their IT infrastructure off-site. While this move is great for mobility and productivity, it makes operations extremely dependant upon a working Internet connection. If this scenario describes your organization, what's your plan to stay productive should your Internet connection fail?

Whether you host just some of your mission-critical data in the cloud or your entire IT infrastructure, a failed Internet connection translates to costly downtime; even those annoying Internet "hiccups" can add up over the course of the workday. Even the best ISPs can't promise 100 percent uptime, making it very likely that you've experienced this pain point before.

Also, what about a worst-case scenario? Imagine for a moment Florida getting slammed with a natural disaster that takes your ISP offline for days. This is more likely to happen than you would think. Here are three solutions to overcome this inconvenience.

Have a Backup IT Infrastructure On-Site

One solution is to have a backup of your infrastructure stored locally on your in-house network. Taking a precaution like this certainly is prudent, although, while locally backing up your infrastructure is a great move, not every business will have the ability or funds needed to enact this proactive measure.

Access a Mobile Network

Another idea to give your office Internet access when your ISP fails is to equip your staff with 4G-enabled laptops and smartphones that can act as temporary hotspots. This will provide your team with the ability to access the files they need over the 4G network, allowing operations to continue humming along. However, before you put a lot of stock into a strategy like this, you'll first want to check the terms and conditions of your mobile data plan. Having the entire office access your carrier's 4G network could result in some hefty fees that may or may not be offset by the profits made while working on your mobile network.

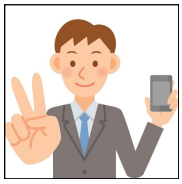
Have Your Team Work Remotely

Another approach is to simply take advantage of other working Internet connections that can be found elsewhere. This is one clear advantage to having a mobile workforce. If your office is experiencing Internet troubles, then your staff can take their mobile devices with them to the nearest coffee shop with working Wi-Fi connection, or even work from their homes. A move like this will keep operations going in an emergency situation, and depending on the likes and dislikes of your staff, you may even find such an arrangement to be more productive for your company overall.

According to ZDNet, this option may actually be the best option in terms of overcoming downtime, and it's worth implementing as a contingency plan: "It's true that businesses are increasingly allowing for remote work and disaster planning is a good argument for it. It may even be worthwhile as an exercise. Require employees to have a plan for working off-site and schedule a day for everyone, or perhaps one department at a time, to do so. You might learn something about productivity while...

Read the Rest Online!
http://bit.ly/29tmjeV

How to Easily Add a Second Phone Number to Your Mobile Device



As the smartphone takes over many of our daily tasks, it can be annoying if we have to use a separate device to accomplish what we need to, like making calls on a different phone. Did you know that it's easy to add a second phone number to your smartphone?

There are plenty of reasons why you would want to do this. Maybe you would like a second phone number that you can use to sign up for promotions so that your primary number doesn't end up on a telemarketing list. Or, perhaps you want to take calls for your business on your personal smartphone. Whatever your reason, the technology that allows you to do this is very accessible.

Call Transfer

A solution that has been around for quite some time (even before smartphones) and comes with most phone plans is Call Transfer. If your current phone system supports it, you can forward calls from it to your personal cell phone, allowing you to take business calls while on the go.

Using Call Transfer is an easy way to receive calls on your smartphone from another line, but this feature traditionally doesn't allow you to make calls from your second device using the transferred phone number. Although, there are phone solutions specifically designed for business, like Voice over Internet Protocol, that will give you the option to both make and receive calls using the transferred phone number with minimal hoops to jump through.

Second Phone Number Apps

If your goal is to get a second phone number for your smartphone that operates entirely as a fully functioning phone line, then there are several apps that allow you to do this. Here are a few of the most popular options.

Google Voice/Hangouts

Using your Google account, you can sign up for a second Google Voice phone number and then use Google Hangouts on your smartphone to both make and receive phone calls. This is a convenient option for those already getting a lot of use out of their Google account, and the best part is that it's free.

Sideline

Sideline provides your phone with a second phone number, although it just provides the basics. With Sideline, you have the ability to make and receive calls and have voicemail with your second phone number, but that's about it. At $3 per month, Sideline is an inexpensive option, but you'll have to suffer through advertisements while using it.

Line 2

Line 2 has more features than the previous examples, making it a better option if you want to use your second phone number for business purposes. These features are reflected in Line 2's two plans; $10 per month for a personal number and $15 per month for a business line. For many smartphone users, the mobile app and the online dashboard may make Line 2 a desirable product.

Skype Number

Skype makes getting a second phone number relatively easy, and if you're already using Skype as your go-to video chat solution, then getting a second phone number through Skype will make a lot of sense. A Skype Number offers users a fairly robust package of features, and at $6 per month, it's an…

Read the Rest Online!
http://bit.ly/29toUWt

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Robert St. Germain
CEO

Tech Fun Fact
Facebook purchased Instagram in 2012 for $1 billion in cash and stock.

Total Tech Care

600 W Prospect RD
STE 2G
Oakland Park, Florida 33309
Voice: 866-348-2602

facebook.totaltechcare.com
twitter.com/totaltechcare
newsletter@totaltechcare.com

Visit us **online** at:
totaltechcare.com