May 2016

TechTidbit.com

brought to you by Tech Experts

Protecting Your Business From DDoS Attacks

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

A Distributed Denial of Service (DDoS) attack prohibits access to a computer resource. This kind of assault rarely happens alone but rather occurs in waves once an attacker realizes they have been successful in the first attempt.

Using the same method of attack on a business' computer system, such cyber-attackers can then overwhelm and suppress Internet facing websites and applications, which can greatly hinder the ability to conduct business as normal.

In order to safeguard against DDoS attacks, small businesses must first recognize they're potential targets, especially since there has been a recent rise of such assaults on small businesses in the past year.

While the motivation behind such an assault can be difficult to understand, they happen for a wide variety of reasons. Attackers may seek to hold systems hostage in an extortion attempt, or the attack may not be motivated by the prospect of financial gain at all.

There have been instances where DDoS attacks were launched by former employees holding grudges or by individuals disagreeing with a particular company's general policies and practices.

It is in personal attacks, such as those launched by former employees, that the gravest damage can occur because the motivation is purely to harm rather than prohibit access to websites.

In withholding, there is value in preserving the website's systems for future financial gain in the form of an extortion attempt. Personally motivated attacks, however, don't mind wreaking permanent havoc.

Cybersecurity experts suggest small businesses look into the systems already in place to protect against DDoS attacks with service providers.

Any safeguards, however, should be taken with a grain of salt because they do not guarantee your protection. If an attack on your business threatens your provider's servers, your systems may be cut off from theirs as a calculated sacrifice to protect your provider's systems and other customers.

That leaves two real solutions for small businesses to protect against DDoS attacks: (1) use cloud-based applications or (2) use a DDoS defender that guards against both application and bandwidth attacks.

Cloud-based applications are more difficult for cybercriminals to infiltrate and can also be scaled to meet small business demands.

With specific tools designed to defend against DDoS attacks, look for ones that have both detection and mitigation functions, so dealing with any perceived threats is not put off until later. It is in quick action that DDoS attacks can be thwarted.

In order to safeguard against DDoS attacks, small businesses must first recognize they're potential targets, especially since there has been a recent rise of such assaults on small businesses in the past year.

How Cloud Computing Can Benefit You

Businesses can virtualize servers, desktop infrastructures, and even entire networks for use in the cloud. Doing so eliminates the physical costs associated with operating equipment, allowing you to dodge unnecessary costs and limit the risk of hardware failure.

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

Is your business using the cloud in 2016? If not, you should know that it's a great tool that's designed to help your business better manage its data and application deployment.

However, the cloud can be used for so much more and it's quickly becoming an indispensable tool for SMBs.

Here are four ways that cloud computing is changing the way that small businesses handle their technology:

Data Storage

The cloud is a great way to share data amongst your entire organization and deploy it on a per user basis.

Businesses can store their information in a secure, off-site location, which the cloud allows them to access it through an Internet connection.

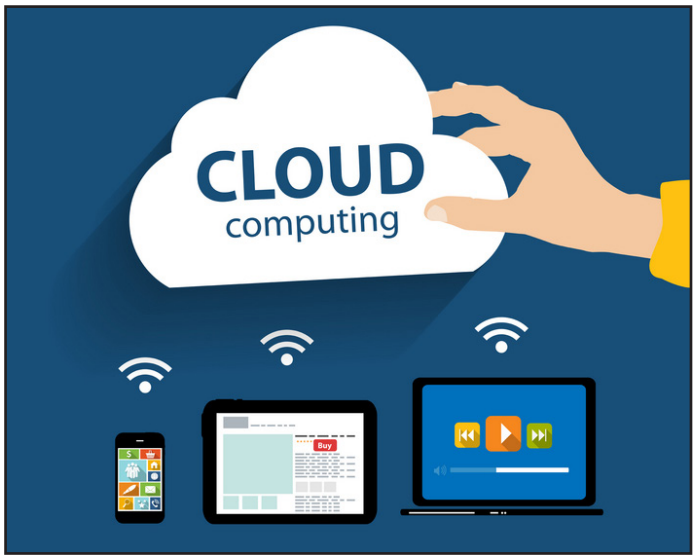
This eliminates the need to host your data internally and allows your employees to access information from any approved device through a secure connection, effectively allowing for enhanced productivity when out of the office.

Microsoft Office365

Access Office from anywhere; all you need is your computer – desktop, laptop, tablet, or phone – and an Internet connection.

Since the software is running in a data center, you just connect to the Internet to access the software.

Another benefit to this is that you have a central location for all your data. If you need to make a change to an Excel spreadsheet from your tablet and you share the file with your colleague, they will be able to view the changes that you just made.



Gone are the days of emailing files between members of your team and losing track of the most up to date file version.

Virtualization

The cloud can be an effective tool for virtualization, which is a great method for cutting costs for your business. By virtualizing physical IT components, you're abstracting them for use in the cloud. This means that you're storing them in the cloud.

Businesses can virtualize servers, desktop infrastructures, and even entire networks for use in the cloud. Doing so eliminates the physical costs associated with operating equipment, allowing you to dodge unnecessary costs and limit the risk of hardware failure. For example, you can deploy all of your users' desktops virtually from the cloud so you don't need to rely heavily on more expensive workstation technology and can instead use thin clients. Simply log into your company cloud and access all of your applications and data on virtually any Internet connected device.

Backup and Disaster Recovery (BDR)

A BDR device relies on the cloud to ensure quick and speedy recovery deployment. The BDR takes snapshots of your data, which are sent to both a secure, off-site data center and the cloud.

From there, you can access your data or set a recovery into motion. If you experience hardware failure, the BDR can temporarily take the place of your server, allowing you ample time to find a more permanent solution.

The cloud is crucial to the success of a BDR device, simply because the cloud is where the BDR stores an archive of its data.

Ransoming Your Business One Step At A Time

Brian Bronikowski is Field Network Engineer at Tech Experts.

When it comes to business security, today's climate is a careful one. It seems like every week the latest and most dangerous ransomware is coming for us.

These can come through a variety of ways, like employees, clients, and websites. The most recent threat we've seen is called Rokku. Built upon predecessors, it's only the next step in the fight against business security systems. Ransomware is a dangerous thing. The main concept is a mix of fear tactics and file encryption. After the system is infected, the virus will normally lay dormant for a time.

Once every file is found and changed to an encrypted state, a message will display, stating the worst.

All of your files are locked until you pay whatever sum the developers demand. Once in this state, you are generally given only a number of hours before your files and content are deleted permanently.

In this instant, many people will jump up to pay for their files in order to save further expense and headache. Unfortunately, doing so rarely helps the issue.

After the ransom is paid, you are supposedly granted access to the files and everything continues on unhindered. That said, there are many times you can send the money in and receive nothing in return.

Your files will still have their encrypted extensions (e.g. *filename*.rokku) and you will be in an even bigger hole than before. Some of the older encryptions have programs made by third parties to help those infected, but this is also often not the case.

In the Rokku scenario, there is no progress made in decryption. No patterns have been found and files are completely distorted in comparison to their original state.

As if it isn't already enough, there is still more to worry about. Rokku as well as other ransomwares will not stop at only the infected computer. Network shares are also subject to complete encryption.

In short order, your entire network is no longer your own. With this in mind, the question is simple. What can you do?

Ransomware is definitely a problem and is not going away anytime soon.

Continued on Page 4

After the ransom is paid, you are supposedly granted access to the files and everything continues on unhindered. That said, there are many times you can send the money in and receive nothing in return.

Do You Have A Blind Spot In Your Security?

Luke Gruden is a Help Desk Specialist at Tech Experts.

Security is only as good as its weakest link — one blind spot and a company can be compromised. It is important that each aspect of a company's security is understood and up to date.

With the following best security practices, it can be better understood what to be aware of and how to better advance a company's security.

From remote hackers, to in-person social engineering, and even your own e-mail, there are different methods of attacks and means of defense to maintain a company's integrity.

Physical Security

The basic defense that predates IT security is physical security. Locked doors, restricted access, and watch patrol are some of the oldest methods to prevent aggressive physical security breaches.

Technology has only made physical security even better with security cameras, alarm systems, RFID badges, and biometric systems that identify a person from their physical being. Having the appropriate physical security is key to preventing and deterring break-ins and stolen items.

Social Engineering

With the right words and story, some people gain access to compromising areas and information that can give a company a real bad time.

Without a physical break-in or even a computer, social engineering works against human psychology, finding the vulnerabilities of staff and workers to trick and deceive their way past security. The best way to defend from this is to have a strong and easily understood security policy that educates staff and workers not give out credentials and access to unauthorized personnel.

Phishing

Billions of emails are sent out every day — promising a vacation, warning people about their bank accounts, or asking for charity —

Continued on Page 4

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

Ransoming Your Business One Step At A Time, Continued

That said, there is more progress these days than when we first started seeing it pop up on systems. Using Rokku as an example, some newer versions are built off of older attacks.

As such, they can often follow the same patterns and can be taken care of. Anti-virus and anti-malware services are also more and more proactive against these threats.

User error can, however, still cause alarm and ruin things very quickly. Rokku and many of its predecessors are sent through email attachments. Once opened, they will start to run and everything will spiral downward from there.

It is important to know and keep others informed on basic safety practices when it comes to operating computers. Keep in mind to not trust strange sites, emails, or messages that you were not expecting or do not know the sender. Also, be aware of common spam signs.

Misspellings, exaggerated results, and poor grammar are often giveaways.

If you want to review your current computer climate, we recommend giving us a call. With preventive maintenance, business class protection, corporate antivirus, and monitors running to ensure a steady flow, we can ensure the safety and reliability of any network and the important files that it may contain.

The absolute best way to avoid a disaster such as Rokku and other ransomwares is to stop it before it happens.

Do You Have A Blind Spot In Your Security, Continued

that are entirely design to steal or compromise a person or company. Phishing targets everybody, asking for credit card numbers, asking a person to sign in to their account on a fake site, or taking something in other ways.

Do not open emails or download email attachments with suspicious or unknown origins. If an email looks odd or is too good to be true, call or check a website directly to confirm if an email is legitimate.

Clicking or falling for phishing could end with a stolen identity, stolen money, or a locked PC or network demanding ransom money. Be smart and wise about checking emails.

Hackers

There are people that spend most of their day trying to break security codes, finding software loop holes, and other abstract means to force their way through digital security to gain illegal access to computers.

There are just as many (if not more) people working together to prevent such people from ever gaining access with new security measures and patches. To protect a PC or a company from hackers, always update your security definitions on Windows and antivirus software. Knowing what software to trust and what updates are needed are important ensuring digital security. We at Tech Experts make it our business to keep digital security online and updated at all times, so that no one has to fall victim to the unseen security threat.

Being aware of these different security risk and knowing how to defend from them can give a strong basis in understanding and learning in what needs to be done to keep a company or person secure.

Security is always evolving and changing, but having a modern understanding with security in place can make the difference between a secure environment and a risky work place that could come to a grinding halt when security is breached. Be safe, be smart, and be productive with good security.

What Can I Do To Strengthen My Wifi Signal?

A weak WiFi signal in certain areas of your house could limit where you do your work and enjoy your entertainment activities, such as streaming films music or playing online games. This is actually a common issue with a couple of relatively easy fixes that will improve your wireless Internet connection throughout your house.

The first option is to replace the antenna on your router with a taller one. If your router has a built-in antenna, you can likely add an external one and see a marked increase in signal quality. There are two main types of antennae: omnidirectional and directional. An omnidirectional antenna transmits in all directions, while you can point a directional antenna where you need to strengthen the signal without making it easier for others to latch onto your WiFi. The other alternative to improve your wireless signal is to install a range extender, particularly if the area that requires the strongest signal is behind thick walls or is relatively small.