CELERANETWORKS
Making Technology Work For You

TECHMinutes
January 2016
Making Technology Work for You

This Issue:

Alert: Malware Locks Up Your PC and Offers Fake Tech Support Phone Number

There's an intrusive malware on the Internet that locks a user out of their PC and directs them to a fake IT support phone number. In addition to being inconvenient, it can lead to

Read the Rest Online!
http://bit.ly/1RkJRl0

About Celera Networks

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:
newsletter.celeranetworks.com

The Advantages of Image-Based Data Backup Over Traditional Backup

There's no question that data backup is absolutely critical for the success of any modern-day business, but how does your organization go about it? Just like how we rely on quick snapshots to capture moments with our smartphones or digital cameras, most backup solutions take advantage of image-based backup technology. How does this kind of data backup work, and what are the benefits it provides your business with?

How Image-Based Backups Work

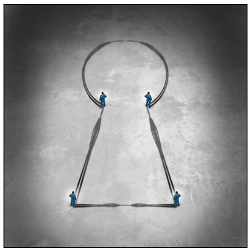
Image-based backups are widely considered the best choice for any small business's data backup needs. Just like taking a picture of something with a camera, an image of your hard drive is like a snapshot of it as it appears in that moment. Image-based backups offer great flexibility when it comes time to recover the data, like if your business experiences a data loss disaster like a fire or hardware failure. The massive benefit of images are that they can track changes that are made to a file over a period of time, and they are capable of applying changes to these files to recreate them as they were at a specific moment. Keep in mind that these changes vary by solution, so it's tricky to identify a set method.

The Benefits of Image-Based Backup

The primary benefit that snapshot backup has over other types of backup solutions is that snapshots are far less resource-intensive than tape backup processes that have to take full copies of every single file on the network. Furthermore, taking multiple tape backups of your data can lead to significant downtime, since you usually can't access the files while the backup is being processed. Additionally, tape backups require manual restoration, meaning that they must be initiated and restored manually. Due to the immense strain backups put on your server, tape backups are generally performed after hours to avoid expensive downtime. Think of it this way; traditional backup solutions look at your files. Every time the backup is run, it copies all of your files and stores them on the backup media (typically another hard drive or a tape). Image-based backups don't look at the files specifically; rather, it looks at the actual physical hard drive and copies over the 1s and 0s. This process is much faster and more effective, and the backup device can quickly determine what's new and only focus on backing up the differences.

(Continued on page 3)

It's Quite Possible for Managed IT to Coexist With Your In-House IT Service



Technology can be a fickle thing for small and medium-sized businesses, especially if they don't have a dedicated staff whose sole responsibility is handling the maintenance and management of IT. It becomes much easier to simply outsource the responsibility to a managed service provider, but even choosing this has implications that should be considered before making such an important decision.

Especially today, when the latest technology solutions can make or break your business plan, it's important to maintain a competitive advantage with your business's technology. Your infrastructure should effectively leverage its technology to improve operations and communications, and managed IT is important for this core necessity of any technology solution your business implements. Here's why outsourced IT is a commonly chosen method of technology management, as well as some potential complications that come with the territory.

Why a Business Outsources IT

One of the key reasons that a business outsources their IT management and maintenance is to save valuable time and assets that in-house employees would spend managing their technology. If your organization doesn't have dedicated IT personnel, the responsibility of maintaining technology falls on the shoulders of your staff, who likely don't have the time and skills necessary to perform the maintenance your network needs in order to remain at the top of its game. This is why remote maintenance and management services are such valuable solutions for business owners.

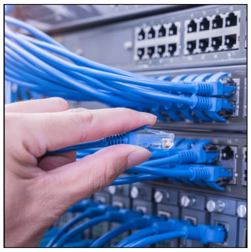
These days, businesses are capable of outsourcing much more than just tech maintenance and support. With new technologies like the cloud taking hold of the business world, the need for professional, business-orientated tech consultants grows every day. Organizations need companies that have the technical know-how to implement new solutions for all aspects of running a business, like managing a network, maintaining data backups, hosting email clients, and so much more. Basically, any aspect of your organization's technology infrastructure, from your IT maintenance to the full management and hosting of virtual infrastructures, can be outsourced to improve operations.

The Primary Challenge: Coexistence

The big issue at hand is that outsourcing IT responsibilities can potentially create a conflict with your current in-house IT services. For example, your old technology solutions that have been around since your business was founded may not be compatible with your more recent operating systems or other aspects of your technology infrastructure. This is a common problem for organizations that typically use legacy technology...

Read the Rest Online!
http://bit.ly/1TLM5HL

Reevaluate Your Network Switches Due to Increased Demand of Wireless Technology



Your computer network is only as strong as its weakest link. One of the most overlooked links is your network switch, and if your IT infrastructure is becoming more dependent upon wireless technology, then you're going to want to perhaps upgrade your network switches.

One of the most significant developments in IT networking comes from BYOD. By now, you've likely heard of BYOD (Bring Your Own Device); it's a rapidly-growing IT trend where employees are bringing their personal devices to the office and using them for work purposes. Due to the influx of BYOD devices flooding office networks in recent years, a network switch predating BYOD probably isn't up to BYOD's increased demands. Consider these common examples from NetworkComputing of how mobile devices connected to your network can increase the strain placed on your switches:

More devices mean more bandwidth requirements, and it's hard to figure out what the BYOD devices are going to be doing, whether it's just plain download bandwidth, something time critical like VoIP, or a sudden surge like Apple iOS version updates. And once end users are tied to a new way of using devices, network teams are often forced to adapt. BYOD not only means bring your own devices but "because you're overly demanding."

It's also worth noting that all of these BYOD devices are wireless and that a single employee may operate multiple wireless devices, like a laptop, smartphone, and maybe even their workstation. In a 2015 survey by ESG, it was shown that "more wireless endpoints is the foremost driver for network switch upgrades, with 44 percent of respondents rating the wireless deluge as a top factor."

The same ESG survey rated speed as the second most significant reason for enterprises upgrading their network switches (33 percent). These days, companies are looking to get the maximum speed possible out of their WiFi and they're turning to 802.11ac (gigabit wireless) in order to achieve it. If your business chooses to adopt gigabit wireless...

Read the Rest Online!
http://bit.ly/1TLMpWX

The Advantages of Image-Based Data Backup Over Traditional Backup

(Continued from page 1)

When it comes to restoring the data, you see an even greater improvement to performance. Where restoring from traditional backup devices usually means you need to restore everything all at once, slowly transferring each and every file over and writing them onto the hard drive, image-based restores allow for very rapid deployment from your backup media. The time difference could be several hours. On top of that, this gives your business the capability to virtualize from your backup solution if your main server is down, reducing downtime even more. In a worst-case scenario, a server malfunction could lead to days of downtime, but with properly implemented and managed image-based backups, the downtime could be reduced to minutes.

In comparison, image-based backups aren't nearly as large or time-consuming as the typical tape backup solution, allowing you to take multiple backups of files throughout the day that have changed since the last backup session. Naturally, this allows your business to take multiple backups daily due to your backup solution only affecting files that have changed. Plus, image-based backups are automatic, so you can take full advantage of them without worrying to remember setting up the tape backup before leaving the office in the evening.

A Backup and Disaster Recovery Solution

By now, it should be apparent that image-based backup technology should be the preferred method of data backup whenever possible. Not only is it superior to other modes of data backup, but it's also vastly more versatile and less resource and labor-intensive than the alternatives, like tape. However, image-based backup will only get your business so far if you have no way to quickly deploy your backups.

This is why Celera Networks offers a comprehensive data backup and disaster recovery solution. Our BDR device takes multiple "snapshots" of your data throughout the workday, which are stored both in an off-site data center and in the cloud for easy access. In the event of a data loss disaster, the BDR recovers your data, restoring it in minutes so you can get back to work with minimal downtime. In fact, the BDR can even replace your server in the event of a hardware failure, giving you ample time to find a suitable replacement without hampering operations.

Share this Article!
http://bit.ly/1TLLQMY

Your Business Must Think Long-term and Short-term When it Comes to IT

For your business's IT, it's important to consider both the short-term and long-term benefits of new technology solutions. However, which of these offers the greatest return-on-investment in terms of profitability and workplace efficiency? Some might argue that short-term IT (think break-fix IT) is more in line with a business's immediate needs, while long-term IT (i.e. managed IT) considers longevity and proactive thought.

A recent study performed by Tech Pro Research suggests that short-term IT is vastly more agile than long-term IT, but doesn't suggest that either are superior over the other. According to the study, 60 percent of respondents feel that short-term IT can be beneficial to their business strategy, but only 47 percent are currently taking advantage of short-term IT solutions. We suggest that short-term and long-term IT deployment are both necessary, and have different purposes and practicalities.

Benefits of Short-Term IT Investment

In a sense, short-term IT deployment can be seen as impulsive. It's designed to help your business resolve a current issue as efficiently as possible. In fact, 81 percent of respondents to Tech Pro Research's survey claim that the quicker deployment of solutions was the primary reason to be trusting in short-term IT. Other benefits include the ability to leverage IT staff more effectively, and better alignment with business objectives. These solutions are often more in line with what a business needs, as they are implemented on an as-needed basis. There is no guesswork as to whether or not they will benefit your IT infrastructure down the road.

Contrary to short-term IT deployment, long-term solutions are designed to provide a return-on-investment over a given amount of time, and to reduce overall expenditures by taking preventative measures.

Shortcomings of Short-Term IT Investment

While there are quite a few benefits of short-term IT investment, there are also quite a few shortcomings. Many respondents cited the increase in costs (35 percent) as a drawback of short-term IT deployment, while another 33 percent cited weaker problem detection as a cause for concern. These drawbacks were likely caused by planning in the short-term rather than for the long-term, proving the point that long-term IT is much better at risk management and problem detection than short-term IT investments.

Since one of the benefits of short-term IT consists of the ability to make quick decisions, it's effective for when your business needs to think on its feet. However, long-term IT investment gives your business the opportunity to be proactive against incoming threats and issues.

Read the Rest Online!
http://bit.ly/1TLMyK8

Malvertising: Hackers are Paying For Ad Space on Popular Websites

A good business practices extreme caution when using the Internet, thanks to hackers using any means possible to unleash threats against organizations of all sizes. You teach your employees how to avoid threats and to avoid suspicious websites, but what if that’s not enough to keep hackers out of your network infrastructure?

Some businesses are finding it increasingly difficult to separate the bad from the good when it comes to online security. This is thanks to a number of new and emerging threats, with the latest one being “malvertising.” This potential threat focuses on using advertising space on websites to inject malicious code into unwary users. This malware often takes advantage of zero-day exploits (problems that haven’t been patched), which means that these threats are difficult to defend against, even under the best circumstances. Take, for instance, a threat described by ComputerWorld:

[...] the source of the infection was a malicious advertisement, one that was running on a mainstream news service! The news website sells ad space served up by an advertising company, which in turn sells that ad space to anybody willing to pay for it. In this case, the bad guys were paying for it. They signed up for ad space just like any other customer, but the advertisement they created — known as “malvertising” — exploited a zero-day (unpatched) vulnerability in Adobe Flash to run commands through the browser to the victim computers’ operating systems, without any knowledge or intervention by the end users.

While taking advantage of multiple avenues of cyber security can be an effective means to combat threats that can compromise your organization’s network, what happens when threats are capable of making themselves invisible to your efforts? This is essentially what happened in the above scenario. Because the malvertisement literally needed no user interaction whatsoever, it was capable of infiltrating the system without being detected, simply because any and all training that employees might have can simply be ignored. Something like this wouldn’t be blocked by a web content filtering system because it’s on a legitimate site.

Thankfully, with the latest cybersecurity tools at your disposal, we can identify and resolve problems like these relatively quickly, should they infiltrate your defenses and set up malware on your network. The important thing to remember about cyber threats is that they will almost always leave some sort of sign that they were there. Be it a virus or piece of malware that’s detected by a firewall, or a phishing email that’s blocked by a spam filter, you’ll know that you’re getting attacked. Even in cases where administrator credentials are used for remote access to your network, you can use your access logs to determine whether or not the account activity is legitimate or not.

Malvertising is a concerning trend to watch out for, to be sure, but in the face of powerful security solutions designed to take proactive measures against online threats, you can bet that it will have some significant difficulty running amok for your business. By taking full advantage of enterprise-level security solutions, your business can detect and...

Read the Rest Online
http://bit.ly/1RkJerv

We partner with businesses in many different vertical markets throughout the New England area. The Celera team is focused on customer service and we strive to eliminate IT issues before they cause expensive downtime.

Our goal is for our clients to continue to focus on what's most important - their business.

Our dedicated staff is known for going the extra mile and doing what it takes for our clients to be successful with their technology investments.

Your firm's success is our success.

Tech Fun Fact

The backronym CAN-SPAM derives from the bill's full name: Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003.

Celera Networks

11 Elkins Street
Suite 330
Boston, Massachusetts 02127
Voice: (617) 375-9100

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

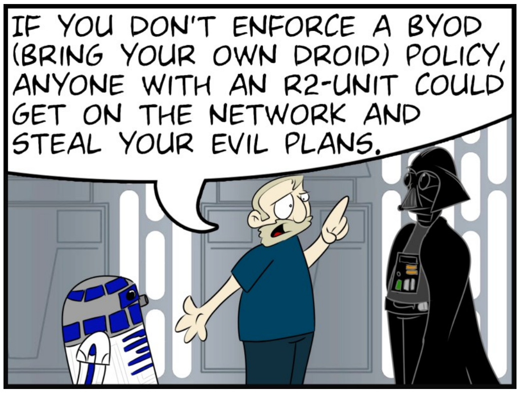
facebook.celeranetworks.com

linkedin.celeranetworks.com

twitter.celeranetworks.com

blog.celeranetworks.com

newsletter@celeranetworks.com


IF YOU DON'T ENFORCE A BYOD (BRING YOUR OWN DROID) POLICY, ANYONE WITH AN R2-UNIT COULD GET ON THE NETWORK AND STEAL YOUR EVIL PLANS.