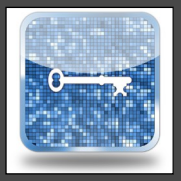
CELERANETWORKS
Making Technology Work For You

TECHMinutes
March 2016
Making Technology Work for You

This Issue:

What to Do When Passwords "Don't Cut the Mustard" Anymore



Virtually every kind of online account requires a password. Yet, due to the aggressive nature of hackers, passwords alone are no longer enough to protect your information. The best way to approach network security…

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

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

How to Leverage the Benefits of Mobile Devices While Negating the Associated Risks

Mobile devices have taken the workplace environment by storm, and you'd be hard-pressed to find anyone who doesn't use their smartphone, laptop, or other device for work purposes. This trend, called Bring Your Own Device (BYOD), helps employers spend less on new solutions, but it also presents a risk that needs to be managed: the Internet of Things (IoT).

According to a study by Tech Pro Research, 59 percent of businesses allow the use of personal devices in the workplace, while only a modest 28 percent were adamant enough to claim that they have no plans of allowing personal devices in the office. Only 13 percent plan on changing their policy over the next year.

We think it's safe to say that BYOD will continue to grow more popular as time goes on, but the businesses that are vehemently opposing BYOD have valid reasons to be concerned about employee devices. Furthermore, the use of Internet of Things devices, which are known for sharing data amongst each other, is increasing in popularity.

(Continued on page 3)

Your Network Needs a Virtual Bouncer to Keep Threats Out

Firewalls are one of the most common IT security measures on the market today, and for good reason. They act as the first line of defense against any incoming threats, and without them, your organization would have to deal with one data breach after another. Of course, that's only if you're taking advantage of a proper firewall; if not, you should seriously consider doing so as soon as possible.

In general, cyber security is an important asset to invest in, especially with the number of data breaches growing by the day. 2015 saw so many high-profile hacks that it feels like nobody is safe. When major institutions like government offices and healthcare providers have trouble keeping hackers at bay, the unanimous assumption is that hacks can, and will, happen, regardless of what industry you're in and how well you're protected. It's becoming painfully obvious that businesses that fail to utilize any security solutions are at tremendous risk of data compromisation.

Well, it turns out that any business can optimize its cybersecurity measures, and it begins by integrating a simple firewall. Here's how a firewall can benefit your organization.

The Benefits

Firewalls are absolutely critical for any business that wants to maximize its cyber security. Firewalls have the ability to detect unwanted network activity, refuse access to your network, and send notifications to a system administrator. Firewalls essentially monitor data that flows both into and out of your network, scanning for threats and preventing them from

(Continued on page 2)

The Cloud Makes Everything Easier, But Only If it's Managed Properly

As an increasingly more important component of the modern technology infrastructure, the cloud can be a daunting new addition to any organization's business strategy. Yet, many businesses still haven't made the jump to the cloud, perhaps out of fear that their use of the cloud won't significantly benefit them.

Basically, you can have an idea of how successful a cloud computing endeavor will be for your business, but you won't know for sure until you take a risk and try it out for yourself. Many of the world's top services, like Amazon and Netflix, have achieved mammoth success thanks to the advent of cloud computing. Your business can achieve a similar level of success in your chosen industry, but only if you're willing to take new and daring risks with how you use your cloud solution.

That being said, you should still approach the cloud level-headedly by doing your research and understanding what exactly you want to achieve with your cloud solution. We recommend that you thoroughly consider each of these three unique cloud computing options.

The Public Cloud

Many SMBs are turning to the public cloud for their cloud computing needs. This is usually because the public cloud has the functionality that they need, without requiring the in-depth maintenance and management that an in-house computing system would require. This is the primary benefit of the public cloud; you get all of the base functionality of a cloud solution, without all of the hassle of managing it. Where it falls short, though, is the lack of additional security features that the private cloud offers.

Simply put, public cloud solutions are reliable, but by definition, pretty cookie-cutter. They are designed to support lots of customers and get a particular type of job done. The customers don't have control over where specifically their data is hosted, what hardware it runs on, or how it's protected.

The Private Cloud

Business owners who turn to the private cloud tend to be more controlling and security-minded than those who are fine with the public cloud. A private cloud tends to be hosted in-house on company hardware or managed externally at a secure data center. Private clouds offer more control over the configurations and setup of your cloud infrastructure, making it ideal for those who want to know exactly what's going on with their cloud solution, and why. Plus, private clouds can be combined with additional security measures, like a Unified Threat Management (UTM) solution...

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

Your Network Needs a Virtual Bouncer to Keep Threats Out

(Continued from page 1)

entering your network. If any threats are detected on the inside, the firewall can prevent them from exiting the network, allowing for efficient elimination. The idea is that the firewall should be able to identify potential threats and inform the proper administrators before excessive amounts of damage accrue.

There's no reason for a business to not be using a firewall. As the most basic of cyber security measures, it's easily configurable to suit the needs of your business.

What They Don't Protect You From

Firewalls aren't perfect. While they're great for keeping threats out of your network in the first place, they aren't going to do much to eliminate threats that have already made their way into your infrastructure. This is why firewalls are often paired with other security solutions like antivirus software, that allow for the detection and elimination of potential threats within a network. Firewalls also won't do much good against social engineering hacks, like spear phishing scams, that are designed to target specific individuals by bypassing common cyber security measures.

Furthermore, the quality of the firewall will often determine what you're protected from. The normal firewall that your network router comes equipped with or a consumer-grade software firewall won't be enough to protect your business. Rather, you should invest in an enterprise-level firewall solution that's designed to protect you from advanced threats. It never hurts to be cautious, especially with your business's future on the line.

A comprehensive firewall works best alongside other forms of cyber security solutions, including antivirus, spam blocking, and content filtering. These four features combined form what's known as a Unified Threat Management (UTM) solution, which is widely considered one of the most comprehensive and efficient ways to keep a network safe. Any business that wants to take cyber security seriously should consider looking into a UTM; if offers enterprise-level protection for small and medium-sized businesses at a fraction of the cost.

For more information about how firewalls, antivirus, and even UTMs work, call Celera Networks at (617) 375-9100.

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

How to Leverage the Benefits of Mobile Devices While Negating the Associated Risks

(Continued from page 1)

Even if a significant portion of business owners have no plans to integrate the IoT with their business, they might not have a choice if employees bring them into the office unknowingly. Therefore, it should be a top priority to protect your business's network from the potential harm these devices can cause. This is why it's important to manage the benefits of BYOD alongside the risks associated with the IoT.

Benefits of BYOD

The Bring Your Own Device revolution provides several great benefits for businesses that want to improve the quality of their operations.

- **Lowered equipment costs:** If you're allowing employees to bring in their own technology for work purposes, that's less money that your business has to spend on outfitting your workers with technology needed for their jobs.
- **Greater workforce mobility and satisfaction:** If employees are using their own devices for work purposes, it means that they can take their work home with them if need be. They can put in more hours and make more time for other initiatives that create revenue opportunities for your business. Furthermore, employees using their own devices are happier, simply because they're using familiar technology instead of company-provided workstations.
- **Less reliance on IT for maintenance:** This benefit might not seem like much, but think of it this way; if employees are able to use their own devices, they're more likely to take proper care of them. This means updating them with patches and security updates, as well as keeping them in working condition, and it allows IT to spend less time resolving issues with employee devices, and more time innovating and improving operations.

Risks of IoT Devices

Despite all of the great benefits provided by BYOD, there are quite a few risks involved with implementing it. These risks are caused primarily by the Internet of Things, and all of the data-gathering devices it brings to your office. These devices are usually Internet-connected wearables, but the IoT encompasses many kinds of Internet-connected devices, including smart building components like thermostats and light fixtures, smart appliances, and even smart automobiles.

In this case, the primary risk would be the security of your network. Think of it this way: if an IoT device were to become compromised, and the employee brings it to your office, it can infect your network. This is a worst-case scenario, but a very real one. It's for this reason that it's imperative that your business should make an attempt to manage IoT devices within your organization. While a health-savvy jogger is unlikely to pose a major risk by wearing their Fitbit into the office, but business owners need to be cognizant of what's accessing the network, where data is getting stored, and who controls it...

Read the Rest Online!
http://bit.ly/1PXHX43

3 Ways Remote Technology Benefits Both Your Employees and Your Business

In an age when working remotely is a commonly accepted practice, many organizations are still skeptical about letting their employees work from home. They think that doing so will disengage them from the workplace environment and that they'll be too distracted to perform their work to specification. Yet, businesses that aren't flexible on this issue could be missing out on several significant cost savings.

Your Energy Costs Decrease

When you have an office full of workers, there are a lot of expenses that are used to help them perform their duties. Depending on the environment, you have to either heat the office in the winter, or air condition the office in the summer. All of your organization's workstations consume a significant amount of electricity, which can eat up a lot of your assets. That's not to mention lighting, the purchase of snacks, coffee, and other boons that employees might benefit from while at the office.

If you allow your employees to work from home, that's energy that's not used. Energy that's not used leads to more savings on your part, and your organization's bottom line will increase as a result. You'll see yourself spending less money on energy and earning more cash.

Your Operational Costs Decrease

When you hire new employees, unless you have workstations, laptops, and other devices on hand for them to use for their jobs, you'll have to purchase new hardware for them. You don't need us to tell you that new hardware is expensive, same goes for software solutions. Outfitting your employees with the tools they need, while your responsibility, can drain your budget.

If your employees are using their own technology to handle their day-to-day tasks, you won't run into this problem. They'll be taking advantage of their own technology, which adds a whole new level of depth to your organization's budget. Granted, you'll want to be using a mobile device management solution and a BYOD policy to ensure that these devices aren't compromising...

Read the Rest Online!
http://bit.ly/1nS9huF

Why BYOD is an Important Industry-Changing Trend

Mobile devices are challenging the traditional perception of the office environment. When employees bring their own devices to work, this is called Bring Your Own Device (BYOD), and it's an increasingly popular trend. Initially thought of as a threat, BYOD is proving to be a valuable option for businesses wanting to increase productivity, so long as it's regulated properly.

Security Issues

One of the biggest causes for concern with the BYOD market is the security of your data. Businesses that take advantage of employee-owned mobile devices will undoubtedly be taking sensitive information and other company-owned data on the road, which presents a problem for businesses that like to have full control over the deployment and distribution of their data. Businesses that want to fully leverage BYOD need to address this concern.

Take, for example, the employee who stores sensitive client or company information on their mobile device. If this device isn't properly regulated or monitored by a company policy, there's nothing stopping viruses or malware on the device from attacking sensitive information. There's also the risk of the device getting lost or stolen, putting your data in the wrong hands. The employee might have had the honorable intention of working during the off-hours, but now there's an important data leakage problem.

The most common solution to concerns over BYOD data leakage is to integrate a mobile device management (MDM) solution. An MDM is a software solution that helps businesses restrict what's capable of accessing data stored on applicable devices. Apps can be restricted or allowed access to data depending on their uses. In the event of a device being lost or stolen, or the employee leaving the company, you can revoke access to company data and even wipe company data off the device.

The Benefits of BYOD

When properly implemented, a BYOD policy for your business can be exceptionally powerful for reducing costs and increasing productivity. According to ITProPortal, there are three major reasons that BYOD is great for small businesses:

- **Greater productivity:** Letting employees use their own devices for work will yield more productivity, mainly due to employees being comfortable with their own devices. Think about it; would your employees rather use company-provided tech, or devices that they're already familiar with? It makes perfect sense. Plus, employees who use their own devices can get work done in the off-hours, which will lead to even more productivity.
- **Cost-efficiency:** There's no reason to purchase new devices for your employees to use outside of the office if they already own devices themselves. Most professionals these days own a smartphone, which makes it much more cost-effective to let employees use their own devices. The more money you save on not purchasing devices, the more you can invest in other profitable initiatives.
- **Consistent updates:** Employees that use their own devices are more likely to apply the critical patches...

Read the Rest Online!
http://bit.ly/1nSajH7

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
You cannot reverse a Bitcoin transaction, or be forced to pay.

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