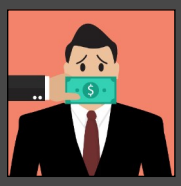
CELERANETWORKS
Making Technology Work For You

TECHMinutes
November 2015
Making Technology Work for You

This Issue:

Why Your Business Should Be Concerned About CryptoWall



Ransomware is one of the most devastating computer viruses in today's computing landscape. You may have heard of one of its most famous variations, Cryptolocker. It received a lot of attention when it dramatically hit the scene two short years ago. Thankfully, the threat from CryptoLocker...

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

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

3 Trends to Watch For in Today's Mobile Industry

Mobile devices are changing the way that businesses look at the workforce, but one of the main draws (and possibly detriments) is how the industry continues to change rapidly as new solutions are made available. In order to maximize your business's efficiency with mobile devices, it's important to consider these three trends shaping the way that organizations handle modern mobile device management.

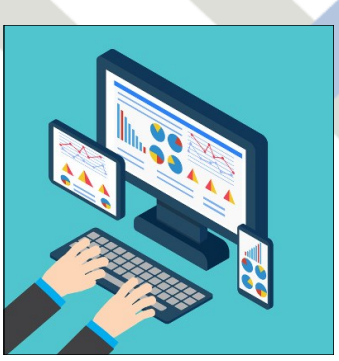
Bring Your Own Device (BYOD)

Perhaps the biggest influence that mobile devices will have on your business is the fact that employees are bringing them to the office. In fact, some employees prefer to use their own personal devices for work rather than the workstations that are provided by your organization. This practice is known for increasing employee satisfaction, and people are usually more likely to make sure their own personal devices are working properly when faced with a technology issue.

While allowing employees to use their own devices can save your organization some cash when it comes to purchasing new hardware and software (by not having to), you also have to consider the ramifications of allowing users to use their own smartphones, laptops, and tablets on your network without any semblance of restraint. It could have an effect on the security of your network, and especially the productivity of your workers.

(Continued on page 3)

It's Important to Keep a Close Eye on Software Licenses



You and your staff require certain software applications to get work done, whether it be your line of business app, your accounting software, or even Microsoft Office. This brings up a crucial question: do you know where all pieces of software you require came from, and are your licenses valid and up to date?

The Ramifications of Software Piracy

Just like any other digital product, software can be stolen, replicated, or altered to suit the needs of hackers looking to make a quick buck. For a business owner however, it's quite possible to fall prey to the tricks that these software thieves pull. These hackers might try to sell infected copies of software for "discount" prices, spreading threats across networks that might be detrimental to a business's success.

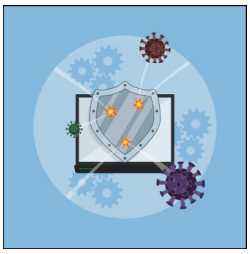
Even if you don't intentionally install copies of software without proper licenses, can you say the same for your employees? In a study performed by research firm IDC, the National University of Singapore, and Microsoft's Digital Crimes Unit, it was shown that "pirated software infected with malware was projected to cost enterprises $126.9 billion worldwide in 2014, $22 billion in North America alone." This means that your employees, thinking only to increase their own productivity, could unintentionally put your budget at risk.

What About Expired Software Licenses?

Furthermore, some software licenses are extremely sensitive to expiration dates. If they

(Continued on page 2)

Criminals Don't Even Need Malware to Hack You Anymore



One of the primary threats that business networks are trying to protect themselves from is malware. We're all aware of how much damage a stray piece of malware can inflict on a business, as they can perform functions like lock down files, steal sensitive data, and distribute crippling viruses. In recent developments, studies are showing that malware is now involved in less than half of all reported hacking attacks, and that more sophisticated measures are now being taken to exploit unwary users.

So, what are these sophisticated measures? Following a data breach, the majority of security teams will investigate the root cause of the issue, and they'll find that, more often than not, the issue has to do with either social engineering attacks or through legitimate administrator tools. What this means is that hackers are no longer relying on illegitimate means of accessing networks, and are instead taking advantage of legitimate means that don't raise a red flag for security systems.

CEO of Crowdstrike George Kurz claims that attackers are using common tools like PowerShell to infiltrate networks. Dell SecureWorks has found that most hackers are using actual legitimate Windows administration tools to access systems. Since these hackers are using real login credentials, detection systems are finding it increasingly difficult to diagnose threatening behavior, putting these organizations at risk at no fault of their own.

Thus, it's becoming aware that security shouldn't just be concerned with identifying normal threats that are easily to see. Instead, security protocol should account for problems that can't be foreseen, a task that seems like it's borderline impossible. Many hacking attacks will come in the form of spear phishing attacks that directly target users, asking them for login credentials that allow for legitimate access to an account login. Thanks to these troublesome antics, hackers often don't leave much in their wake, save for a path of destruction. *InfoWorld* states:

The fact that attackers are using legitimate tools -- FTP, RDP, PowerShell -- means they are not leaving much in the way of tracks behind them. With no easily found malware artifacts, it's harder for security teams to determine the initial penetration point. If the company has deployed breach-detection technologies that focus solely on malware and its artifacts, such as command-and-control IP addresses and domain names, then the defenders don't get the alerts when the attackers are live in the network.

This is why it's so important to pay attention to who is accessing your network, and when. Businesses often neglect to pay attention to their access logs because they feel that only authorized users will attempt to access the network through legitimate means. However, this simply isn't the case anymore. Keeping a close eye on access logs can help to ensure that nobody is accessing your network that isn't supposed to. Furthermore, businesses that haven't integrated two-factor authentication yet...

Read the Rest Online!
http://bit.ly/1jKlCi5

It's Important to Keep a Close Eye on Software Licenses

(Continued from page 1)

aren't renewed in a timely manner, what happens? Consider this scenario; your staff are being productive and are on the last leg of finishing a mission-critical initiative or project. Just when they're about to apply the finishing touches, the software prevents them from continuing their work at a decent pace. This means that your staff might be forced to finish projects late, all because of a software license expiring at the wrong moment.

One way you can avoid this is by organizing all of your software licenses so that they need to be renewed either on or around the same date. This makes it much easier to remember to do so, considering you're only remembering one date rather than several. Better yet, ask your vendors (or Celera Networks) if auto renewal or alternative licensing is available.

Whose Reputation is at Stake?

It's not just your business, but the developer's reputation as well, that will suffer if you're the victim of a hacked software scandal. Honestly though, using compromised software or even counterfeit or pirated software can incur heavy legal fees. According to CyberTrend, "Many employees in big companies believe that if they steal a program behind a firewall, they may never be found. But many developers have tracking systems that identify who their visitors are and what they're viewing."

So, regardless of whether it's intentional or not, you can expect to be held accountable if your organization ever does take advantage of software obtained through illicit means.

Besides the fact that updating your licenses and end-user agreements should always be done, some companies simply don't have the time or resources to ensure that it happens in a timely manner. We recommend that you outsource this responsibility to Celera Networks. Our dedicated IT professionals can remotely renew your software licenses...

Read the Rest Online!
http://bit.ly/1jKl4bT

3 Trends to Watch For in Today's Mobile Industry

(Continued from page 1)

Mobile Device Management

In order to resolve the issues proposed by a BYOD policy, it's important to make sure your organization has a process set up that allows for the management of all mobile devices that hold (or have access to) corporate data. Blacklisting apps is helpful in keeping certain ones that collect personal information from accessing this data, while whitelisting allows you to pick and choose which ones have this kind of access.

In particular, you want to have control over what applications have access to your business's corporate data, as well as the ability to remotely wipe mobile devices that hold this data. If a hacker were to get physical access to the device, you're making it much easier for hackers to steal this information. Therefore, you need the ability to get rid of it in an instant, should a device go missing or is lost.

Cloud Services

More businesses than ever before are turning to the cloud for the storage and deployment of their mission-critical systems, and it's easy to understand why. They want to make sure that their employees always have access to the information and applications they need to ensure productivity continues without a hitch.

The only issue is that while a cloud platform offers a significant return on investment, integrating a quality cloud solution for your business is knowledge intensive and requires the attention of a trained professional. The same can be said for all aspects of the mobile device revolution. Thus, before integrating any type of mobile device or BYOD policy, it's recommended that you contact the technicians at Celera Networks. We can walk you through the requirements of integrating mobile devices, and equip your business with the infrastructure that's most hospitable for your success. Give us a call at (617) 375-9100 to learn more.

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

4 Ways You're Unknowingly Risking Your Entire Data Infrastructure

If you don't already have a backup solution put in place, no time is better than the present to consider what it would cost your business if you were to lose everything in one fell swoop. There are plenty of ways you can back up your data, but the reality of the situation is that if you were to lose your business's information, you wouldn't be able to continue operations. It would put the entire future of your company in jeopardy, so you need to be absolutely certain that your backup and disaster recovery solution is fool-proof.

Here are four ways that you're putting the integrity of your business systems at risk.

Don't Ignore the Concept of Backup and Disaster Recovery

Obviously, the first step toward admitting that your backup and recovery solution isn't optimal is asking whether or not you have one in the first place. It's not a matter of if you experience a disaster that can wipe out all of your data; it's when it will strike. You need to be prepared for a worst-case scenario. A flood or fire isn't something that you have control over, but integrating a comprehensive disaster recovery plan is.

Don't Integrate a Backup Solution and Just "Hope it Works"

Similarly, you can integrate a backup and disaster recovery solution, but if it doesn't work when you need it most, then what's the point? You should always be testing your backups to ensure they're not corrupted and work properly. If they don't, and you have to rely on them in the event of a disaster, you'll be awfully disappointed.

Don't Have a Single Point of Failure

In other words, if a single issue with your infrastructure were to go down, would you be able to continue functioning at a normal rate? Your system should be able to survive without a single server going down that affects the entire state of operations. It's recommended that you use a combination of the cloud and on-premises solutions that allow your business access to critical systems that are necessary for everyday operations, even under the worst circumstances.

Don't Leave Your Expensive Equipment in Vulnerable Locations

One of the best things you can do for your business, especially if it's located in a region that sees a lot of rain and flooding, is to ensure that a couple inches of water won't completely ruin your critical systems. By properly elevating infrastructure hardware (or better yet, virtualizing them and moving them to the cloud), you're effectively minimizing the chances of them being ruined by a freak rainstorm or similar disaster that cause unexpected data loss.

Ultimately, the best way to prepare for the time you need to back up and restore your critical information systems is to call Celera Networks at (617) 375-9100. We'll help your organization prepare for the worst circumstances your business can face.

Share this Article!
http://bit.ly/1WIrHK3

Uber Used Technology to Break the Mold, Can Your Business?

At a September tradeshow event, Travis Kalanick, cofounder and CEO of Uber, said five words in an interview that made everyone give pause to the potential for technology to shape our world for the better, "Every car should be Uber."

In case you're unfamiliar with Uber (it's not yet available in every city), Uber is a technologies company which provides services for taxis and for-hire vehicles by allowing passengers to request trips to the closest for-hire Uber driver, through its mobile app. What makes the ride-hailing app unique is that it can turn anyone with a car and a smartphone into an Uber driver, allowing them to easily make extra income on the side by providing rides to Uber users. Plus, all transactions are handled via the app so that drivers don't have to risk carrying cash.

Founded in 2009, the popularity of Uber has skyrocketed. Uber rapidly expanded to international markets beginning in 2012, and the company is currently valued at $50 billion. It should also be noted that Uber was honored by USA Today as "Tech Company of the Year" for 2013.

Looking back at Kalanick's "Uber everywhere" comment, it's not surprising that a CEO tasked with expanding a popular company would say such a thing. While a taxi/transportation service isn't anything new, Uber's adoption of new technology is what makes them stand out. Instead of thinking about ease-of-use and integration with mobile technology as an afterthought, Uber puts that first. **Businesses that focus on consumers often sacrifice being cutting-edge so they can stick with what has always worked. Kalanick proves that it pays to think outside the norm.**

Essentially, what he is proposing is a future where transportation becomes so commonplace and accessible, that hitching a ride with Uber will make more fiscal sense and be more convenient than owning a car. Kalanick explains:

"If every car in San Francisco was Ubered there would be no traffic. If everyone in the city took an Uber instead, it would give back an hour of time every day to every person. What would you do with that time? You could give it back to your family."

It just so happens that Uber is headquartered in San Francisco, and it's also the case that San Francisco is one of the worst cities in the U.S. in terms of how much time commuters lose per year due to being stuck in traffic--78 hours per year, according to a recent traffic study by Texas A&M University. Following Kalanick's logic: more Uber cars on the road will equate to more people using the service, which means more people opting out of car ownership altogether, and that means less cars on the road and less traffic jams.

Uber has gone so far as to implement new technologies in order to make their ride-sharing service more efficient. Otherwise, an increased amount of Uber drivers would be sitting in their cars competing with each other while not having enough customers to give rides to. InformationWeek explains how this will work:

"How does Uber plan to reduce the cost of...

Read the Rest Online
http://bit.ly/1WIt9Mz

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
It has been 40 years since the world's first mobile phone call successfully took place.

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