THE DIGITAL ARCHITECTS

techBytes

DEPENDABLE TECHNOLOGY SERVICES

SPRING
2018

Welcome to Spring!

What's Inside?

5 Ways Virtualization Can Help Streamline Your Operations And Keep Your Company Safe

Wow! What a title, right? I know what you're thinking, virtualization can't possibly streamline my operations and keep things secure. This is just too much of an assumption. Well, if you think so, go ahead... flip the page. The article on page two about Baltimore's ransomware attack is definitely interesting. But, if you're truly looking to make things more accessible and secure for your company, keep reading because we might be able to change your mind about virtualization.

What is virtualization?
The term virtualization has saturated the media over the past five years. Many sources couple virtualization with terms like "reduced expenses", "performance enhancer", or even "flexible environment". However, these sales terms don't really tell you much about what virtualizing actually is. So, let's explore. Virtualization is the creation of a virtual (rather than actual) resource for computing. Virtualized resources can be anything from applications and operating systems, to entire desktops and storage. Virtualization does require physical hardware, like a host server, to house the virtual environment. However, one physical server can care for many virtualized items including software, desktops and storage.

Isn't it just like cloud computing? It is very similar, however the major difference is virtualization relies on a physical host where cloud computing just uses resources hosted by another company to conduct business.

Take a look at these five ways virtualization can help streamline your operations and keep your company safe.

1. More control over your environment. Virtualization offers more control over your IT environment. Going virtual gives your IT staff an easy path to install and maintain software, keep your network secure and push out updates. This means less downtime, quicker recovery when there is a situation, and fewer outages compared to physical computers.

2. Faster and easier backup and recovery. Businesses are always at risk for some kind of disaster. Cyber-attacks, fire, flood, or theft can strike at the most inopportune time crippling your business. Virtual environments allow you to recover your resources and data must faster and more completely with less time and manpower.

(*Continued on page 2*)

THE digital ARCHITECTS

Need Technical Help?
Contact TDA today
gethelp@tdai.net

America's Growing Cybersecurity Hub

Despite the fact that Silicon Valley gets most of the attention related to technology, New York City is positioning itself to become the center of cybersecurity in America, according to the Wall Street Journal. In recent months, the city has deployed a $30 million fund to entice new firms to plant their roots in the Big Apple as well as to allow students to attend the New York University Tandon School of Engineering's cybersecurity master's program at a total subsidized rate of $15,000.

The investment has been working so far as several Israeli firms have opened offices and at least one, Bay Dynamics, has relocated their headquarters to the area to take advantage of the incentives. Planners behind the deals are banking on the fact that New York has many creative professionals that can team with the technical expertise of foreign and domestic companies to create incredible new products and services for the market.

The Cyber NYC Requests for Proposals (RFP) released late last year, is looking for industry professionals and academia groups to partner with the city supporting a range of initiatives. This new RFP is focused on establishing a platform for New York City to connect entrepreneurs with the resources needed to strengthen partnerships, develop training and academic programs that support new technology and innovation. With this new initiative, New York City will be well positioned to become a global hub for commercial cybersecurity in the coming years.

5 Ways Virtualization Can Help...

(Continued from page 1)

3. Avoid aging hardware costs.
Virtual desktops allow you to use any type of computer to access the programs and files you need for your work.

4. Better performance.
Virtualization gives everyone the benefit of using the server's power. Regardless of the desktop, laptop or tablet you're logging in from, virtual desktops let you tap into the processing speed of your server to run your work programs.

5. An easily scalable solution.
Ready to grow? Creating new user accounts with the necessary work resources and access is a breeze. With a virtual environment technicians can have a new user up and running in just minutes.

Spin up your own private cloud.
Another great idea for your virtual environment is a private cloud. Since you own your hardware, you can house it in your office or with your IT provider in a data center. This hardware can be used as a platform to host your own private cloud resources internally. This structure offers more control and flexibility since you're managing your own systems and security.

Are you ready to virtualize?
Considering a private cloud? Wondering if this solution is a good fit? Give us a call.

THE digital ARCHITECTS

Need Technical Help?
Contact TDA today
gethelp@tdai.net

Ransomware Infects Baltimore's 911 System

It's the middle of the week, you've got your Starbucks in hand, you're ready to kick-off your workday and something out of the ordinary hits you. You smell smoke. Smoke? There is a fire! What do you do?

Call 911 of course! You're quick to tell your coworkers about the smoke, evacuate the building, and call 911 for help. However, emergency services are offline. The call just rings. The dispatch operators cannot see calls coming in, they cannot access the database to view the details they need, they are dead in the water struggling to switch over to their manual systems because a ransomware attack has compromised their network. So, your office just burns?

A little infection gums up the works. Who would have thought, that a little ransomware could gum up such an important system. Luckily, Baltimore's IT managers were able to detect the issue before it interrupted emergency services, but you can see how an attack like this could bring down a network, stop critical services, and impact more than just operations.

IT management saves the day. Baltimore's IT service department was able to detect the hackers that tried to infect the 911 computer system with ransomware and isolate the threat. They quickly made sure it couldn't spread to other servers in the city's network and worked to restore the services impacted.

How does this happen? In Baltimore's case, some routine troubleshooting on a firewall to resolve a dispatch system issue left a small vulnerability that hackers honed in on immediately. Baltimore isn't the only city in the U.S. hit with ransomware. Not long ago, Atlanta was a prime target. They experienced a ransomware outbreak that continues to plague their systems even today. Hackers demanded over $50,000 from the City of Atlanta to unlock the city's infected systems.

What can I do? Typically ransomware strikes through phishing e-mails or known vulnerabilities in software. Here are a few things you can do to help prevent an attack on your business;

1. Train your staff. Talk to everyone in your company that accesses your network, even remote employees or those who just use their own laptops. Talk about current phishing e-mail scams, discuss the variety of methods hackers use to infect your network with ransomware, review the security measures you have in place for your network and how to report suspicious activity. Security is everyone's responsibility.

2. Keep your systems updated. Known vulnerabilities in software programs like your customer management system, your firewall, or even Microsoft products in general can be very dangerous. Updates and patches give you the most current security changes closing off vulnerabilities in your network.

3. Make a plan for service. What if you do become infected? Who do you call? How can your company recover?

KnowBe4
Human error. Conquered.

If you don't have dedicated IT staff to give you answers to these three questions, give us a call. We can assess your network for any current vulnerabilities, bring your systems up-to-date, and provide you with a plan to keep your company safe. Ask us about KnowBe4 ongoing training for your entire staff!

Does Private Browsing Keep You Safer?

Have you ever browsed online and seen some advertisements for that awesome new tablet you were drooling over last week? If so, there is a very good chance your activities online are being tracked and used by market researchers to provide you with relevant content. Generally, these advertisers are harmless, however they are tracking, viewing, and using your data in order to sell you more stuff.

Clean up your browser. One of the first things you should do to clean up your browser is delete your browser's cache, cookies and history. Then move on to your extensions. Many people don't even realize how many programs they have attached to their browser. Look at the list of plug-ins and extensions in your browser and disable or delete any that you don't use regularly. You may even find it useful to delete them all and just reinstall the ones you need most as you browse the web moving forward.

What is private browsing? Now that your browser is all cleaned up, should you be using a private browsing mode? Well, this is really a personal choice. Private browsing modes like Incognito Mode in Chrome or InPrivate in Edge, are just fancy ways for you to browse the Internet in a session that is unrecorded. Essentially, the sites you visit will not be able to put tracking cookies in your browser, they cannot see passwords you've used or files you've downloaded. In fact, any and all data the websites accessed during your visit, is immediately discarded without a trace as soon as you close the browsing window. However, if you are using work computers, remember your system administrators can still see and keep track of what you're looking at regardless of your browsing mode.

Are all cookies bad? I know we mentioned cookies a few times here in this article, so here is a quick explanation of how they work. Not all cookies are bad, snickerdoodles for example are my personal favorite. Ok, I'm kidding, cookies online are basically little micro programs that gather data about your activity in order to present you with relevant advertisements and content as you continue to browse the Internet. It is almost like having a personal assistant with you to recommend things. Not everything cookies suggest will be on target, but sometimes these little trackers pop-up just what you need. Be safe online!

"Did you ever realize that we're really drinking coffee out of large sippy cups?"

Filter With The Four D's To Manage Your Inbox Effectively

The four D's are delete (or drop), defer, delegate and do it. Filter requests with the four D's to limit distractions, time-wasting tasks and interruptions.

Delete (or drop) any items in your inbox that are unsolicited or do not have value. I'm sure you can find a good dozen you can delete without even opening them.

Defer tasks that can be performed later. It may be useful to calendar time for it at a later date or flag the message with a reminder. These are items that can wait a few days or even a week for your attention.

Delegate tasks that can be handled by someone else. Send them right away with any additional instructions necessary and let it go. General filing, bookkeeping, travel arrangements, or even meetings to schedule can be delegated to a virtual assistant or in-office administrator.

Do it. Yep, this one is easy, just do what's necessary to complete the task at hand. If it takes less than 10 minutes or less and you have that time available, don't delay. Take care of that urgent or important message from a client, request more information from your colleague for your next project, or confirm this afternoon's appointment for lunch.

Inquiring Minds...

What is the TDA Staff up to this spring?

Jeannie
- Getting my yard and garden spruced up THEN enjoying a glass of wine on my porch admiring my work.
- Getting the boat ready for the summer.

Wendy
- Anything outdoors!!! Including walk or run and bike on a local trail or beach.
- Cherry blossoms in DC.
- And playoff ice hockey - go Caps!!!

Christine
- Working in my gardens with the spring flowers in bloom.
- Getting outside and enjoying the fresh spring air while biking and boating.

Ashley
- Motorcycle Rides.
- Any outdoor time with my family.

Holly
- Play softball.
- Run outside.

Jeff
- Working around the outside of the house.
- Barbecuing with friends.

Paul
- Camping.
- Working outside in my yard.

Dates to remember...

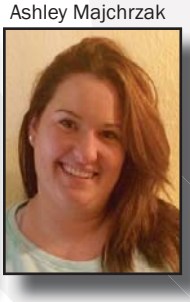
Mother's Day
Sunday, May 13

Memorial Day
Monday, May 28

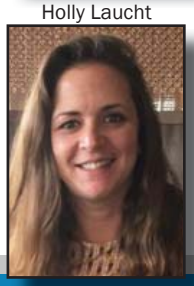
Father's Day
Sunday, June 17


Jeanmarie Richardson


Wendy Panor


Ashley Majchrzak


Christine Stephens


Holly Laucht


Jeff Christ


Paul Lucas

your TDA team