E-NEWS

February 2018

In this issue...

Virtualization best practices for newbies

The benefits of virtualization are so significant that deciding whether to jump on board is a no-brainer. It offers centralized IT management, faster hardware resources, improved business continuity, and reduced overhead costs. But in order to experience these benefits, there are a few best practices you need to consider.

Conduct an assessment

Evaluating your IT environment is an important step in the implementation process. After all, you can't just go around virtualizing everything without a plan. An IT assessment performed by an impartial managed services provider (MSP) like us helps you understand what type of virtualization solution you need.

For example, if the report found that computers don't have enough processing power to run certain apps, desktop virtualization -- which consolidates operating systems and apps into a single powerful server -- is an ideal solution.

From there, you should be able to estimate costs and set realistic timelines for the implementation.

Don't forget about hardware

Just because virtualization frees up space in your server room, does not mean hardware is no longer an issue. No matter what type of solution you opt for, the servers you use must be strong enough to support the entire company's computing demands.

This means you must take stock of your apps and their hardware requirements and make sure your server has all the processing power, RAM, network capacity, and storage necessary to run them.

Underutilized servers are excellent candidates for virtualization, but purchasing new equipment may pay dividends in the long run. If you choose the latter option, ask your provider for recommendations. Chances are they're partnered with virtualization-optimized hardware vendors that offer top-of-the-line servers.

Prevent VM sprawl

Virtualization allows you to deliver computing resources to workstations in your network via virtual machines (VMs), which can be created on a server in just a few minutes. While this lets you scale and provision resources quickly, there are risks if you don't have someone regularly reviewing which VMs are worthwhile and which are outdated. You could be losing out on cost savings and efficiency benefits.

When too many VMs are created, they can quickly consume all server resources and complicate licensing and asset management.

To prevent sprawl, you must establish policies and restrictions for VM creation. For instance, users must have a good justification for creating a VM (e.g., testing software or provisioning apps for new users).

Prioritize business continuity

You must also protect the hardware running your virtual servers. Make sure to lock up server rooms and have secondary servers available in case the first one breaks down. While you're at it, take advantage of automated backup solutions that make copies of your VMs and their files regularly.

Work with experts

Building and maintaining a virtual infrastructure is no simple task. That's why you'll want to work with a virtualization specialist who can guarantee a seamless implementation and provide ongoing management services.

For more tips on virtualization, call our experts today!

The dangers of distributed spam distraction

Users get around 200 emails in their inbox a day, including work messages, automated payment slips, and everyone's least favorite email, spam. Spam messages are mostly harmless, but when you get more than 10,000 of them flooding your inbox, you're probably the victim of a special type of spam attack.

Understanding DSD

Distributed Spam Distraction (DSD) is designed to inundate your inbox with thousands of nonsense emails. There are no dangerous links, ads, or attachments involved, just random excerpts of text stolen from books and websites. What's more, the email and IP addresses used are all different so victims can't simply block a specific sender.

These attacks last anywhere from 12 to 24 hours and can flood inboxes with as many as 60,000 messages. While they may seem like harmless annoyances, the true purpose of DSD is to draw victims' attention away from what hackers are doing behind the scenes.

And what they're doing is exploiting your personally identifiable information (PII) to make unauthorized purchases or pilfer cash directly from your accounts. The DSD acts as a sort of smokescreen to hide payment confirmation messages behind a deluge of spam messages.

New tactics

Over the years, hackers have developed new tactics involving DSD. Several reports have shown that, instead of nonsensical emails, hackers are using automated software to have their targets sign up for thousands of free accounts and newsletters to distract them with authentic messages.

This allows DSD blasts to slip past spam filters that have been designed to weed out malicious code and gibberish text used by traditional DSD attacks.

What's even more worrying is that any ill-intentioned individual can go to the dark web and pay for DSD services. They just have to provide a hacker with their target's name, email address, and credit card numbers -- all of which can also be purchased in the dark web -- and pay as little as $40 to send 20,000 spam messages.

How to stop it

DSD is a clear sign that one of your accounts has been hijacked, so whenever you receive dozens of emails in quick succession, contact your financial institutions to cancel any unfamiliar transactions and change your login credentials as soon as possible. It's also important to update your anti-spam software (or get one if you don't have one already) to protect your inbox from future DSD attacks.

Hackers only initiate DSD attacks after they've obtained their target's email address and personal information, so make sure your accounts and identity are well protected. This means you should regularly change your passwords and pins, enable multi-factor authentication, set up text alerts for whenever online purchases are made in your name, and be careful about sharing personal information.

For more tips on how to deal with DSDs or other cyberattacks, call us today. We offer powerful tools and expert advice that will ensure your business's safety.

2018 MARCH MADNESS

MLB OPENER

Starting Line-Up
Exagrid
Barracuda
PacketViper
Veeam
Citrix
Sophos
Lenovo
Liquidware Labs

WHEN AND WHERE

THURSDAY, MARCH 29TH
HIGHMARK STADIUM
510 W STATION SQUARE DR,
PITTSBURGH, PA 15219

March is right around the corner! Join E-Safe Technologies for our annual March Madness Event:

Thursday, March 29th

8:00am – 4:00pm

Highmark Stadium, Station Square, Pittsburgh, PA.

Be sure to register and join us for the largest event of the year. Please visit

http://www.e-safetech.com/marchmadness/

Come learn from the leading industry experts about the newest tech and trends!

Don't miss out on food, beverage, entertainment, and prizes. Sign up now.

Fighting ransomware with virtualization

Ransomware takes your data hostage and demands a payment for its recovery. While it may seem like there's no other choice but to pay the ransom, you should never give in to the hacker's demands. Before the next wave of ransomware comes around, it's important to protect your business with virtual disaster recovery solutions.

Virtual DR

Virtual DR solutions allow you to create point-in-time copies, or "snapshots," of operating systems, data, and virtual machines as they appear at a given point in time. These snapshots can then be loaded onto any workstation with everything still intact. In the event of a ransomware attack, administrators can essentially roll back the system to a point before the malware hit.

What's great about point-in-time copy features is that they are automated. Just schedule the snapshots, and your virtual DR software will do the rest. And although virtual DR solutions vary, most of them have the capacity to store thousands of point-in-time copies, giving you plenty of restore points to choose from.

Why virtual DR trumps traditional DR

Traditional DR methods don't have these features. Even though most computer operating systems have a system restore functionality, modern ransomware strains are designed to disable them. On the other hand, virtual DR software isolates point-in-time copies and restore functionality from virtual machines, which means they can't be affected if one virtual machine was compromised with ransomware.

Another reason why traditional DR is not a great option is because there is a lot of manual labor involved. You have to copy all your data into a backup drive, reinstall applications, and reconfigure hardware. By the time you've recovered from the ransomware attack, the financial and reputational damage caused by downtime will have taken its toll on your business.

When recovering your system, you want as little hassle as possible. With virtual DR, you can load a clean, ransomware-free snapshot onto your system in less than 30 minutes.

However, implementing virtual DR can be complex, especially if you don't have much IT expertise. But if you partner with us, this won't be a problem! Call us today to get robust solutions that guarantee business continuity.
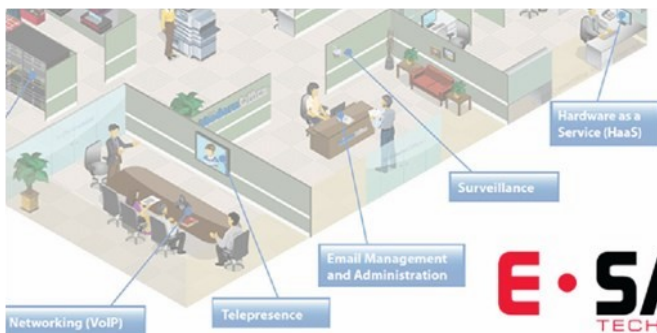
"What is Software as a Service (SaaS)?"

Software as a service is a software delivery model in which software and the associated data are centrally hosted in the cloud by software vendors or application service providers. SaaS is typically accessed by users utilizing a thin client device or via a web browser, which allows for easy access and mobility. This software distribution model is made available to customers and clients over a network infrastructure, most commonly the Internet. One of the most popular software platforms that utilizes this model is Salesforce.com where companies purchase login credentials on a monthly basis and have access to customer relationship management tools in the cloud. This model allows organizations to access their business applications at a minimal cost per month rather than paying a lump sum up-front. The software is hosted on the providers servers and equipment, which makes it easier for them to update and maintain. You don't have to keep purchasing new versions of the software. Instead, they update it and sync these changes to your already existing accounts. This is also beneficial because users don't have to invest in hardware that runs their specific software, whether it's their CRM, email, or database management tool. Corporations are beginning to build data centers that can host your applications over the web interface, which is also extremely easy to scale for prospective customers. As you grow, you don't have to purchase additional infrastructure to host users. Instead, you purchase monthly user licenses which is a much lower cost. SaaS is inspiring new operating models and when implemented correctly can benefit organizations of all sizes.

Start with a Plan, Finish with Success.

"How Can SaaS Improve My Business?"

Accessing your vital business information on the cloud can benefit companies in the following ways:

Mobility: No longer do you need to have your computer with you at all times to access vital software applications. With SaaS, you can access your information if you have a connection to the Internet with your login information on hand.

Price: By utilizing SaaS, you pay a small monthly fee to use the software. You don't have to purchase dedicated infrastructure to support your applications onsite. This also decreases the amount of taxes that you pay because there won't be that steep investment in hardware in the beginning. Also, this saves on power costs that it takes to run and maintain the infrastructure.

Manageability: There is no longer a need to run updates on your hosted software. Because the application is hosted on your provider's infrastructure, they handle the updates and streamline it to your account.

Scalability: As your business grows, there has to be an integrated solution that can grow with it. With SaaS, that is easier than ever. You don't have to purchase more faulty equipment. You are able to add to your current licenses which will increase your bill only a few dollars per month.

Next Issue:

Cloud Services

The ModernOffice™

"How Does SaaS Work?"

Companies basically rent licenses or access the software from a service provider or a managed service provider. The software runs on servers owned and maintained by the service provider, which allows the customer to utilize the software without having to run pesky updates. These software applications are typically run out of large datacenter facilities with redundant power, battery backup solutions, climate control systems, and security procedures that are financially out-of-reach for the small and medium sized business space. SaaS can allow those businesses to access the software applications on a per user basis. A large amount of SaaS solutions are based on a multi-tenant model. This means that a single version of the software application and a single configuration are used for all customers who are linked to that system. In some cases, a second version of the software is set up for a select group of users to test the pre-released versions of the software application. This enables users to increase their productivity by not having to worry about different versions of the software. The application is tested, patched, and maintained by the provider. Some other SaaS solutions utilize virtualization to manage a large number of customers instead of the multi-tenant model.

"What's My Investment In SaaS?

SaaS is extremely affordable for small to medium sized businesses. As stated before, you only have to pay for access on a per user, per month basis. Usually these are very low costs. For example, Microsoft Office 365 allows you to use the latest Office applications for around $10 per month / per user. This is an extremely low amount to pay when you take into consideration how relevant the latest Office applications stay in the mainstream business environment. It seems like every two years they come out with the latest and greatest applications. For the monthly payment, you have access to the newest software. You don't have to purchase and install the latest version in a few years and you don't have to download patches and updates. The provider maintains the application which allows you to focus on more important things. Software as a Service takes everything that's relevant in technology today and combines them to give you the stability, scalability, and manageability you need in today's fast mobile business environment. As long as you have connection to the Internet, you have access to all of your valuable business information.