The security risks of virtualization

March 31, 2016

While virtualization security is not often talked about, it is nevertheless important. Like all technology, securing your virtualized infrastructure is vital to the success of your business. So what are some of the security risks posed by virtualization? How can you mitigate them? Here are some answers you should consider:

**Security risks of virtualization**

**Complex infrastructure** - much like the topic of virtualization itself, the infrastructure of a virtualization solution can oftentimes be confusing to small businesses. The extra layers of infrastructure complexity added by virtualization can make it more difficult to spot anomalies and unusual events happening in your virtual machines and network.

**Dynamic design** - the design of a virtualized environment is dynamic by nature and constantly changing. Unlike adding physical equipment, which is a bit of an event as you make room for it in your office and install it, the addition of virtual machines can go almost completely unnoticed as they’re created in a matter of minutes and aren’t visible in your workspace. The danger here is the age old adage, “out of sight, out of mind.” If you add too many, they can easily become difficult to manage and secure, creating security holes in the process.

**Quick moving workloads** - as your virtualized infrastructure grows, there will come a time when you need to move workloads from one machine to another. While this may sound harmless enough, the real issue is that your virtual machines will likely require different levels of security. When you’re juggling multiple workloads over multiple virtual machines, you may accidentally move mission critical workloads to a machine with a low level security, creating a security hole in the process.

**How to mitigate risks**

While these three risks may sound alarming, they can all be mitigated. The key behind effectively securing your virtual machines all comes down to process. Put some thought into your security processes and then implement them. Here are a few areas you will want to be sure to cover:

- **Organization** - decide how and where to separate your test, development and production virtual machines.
- **Audit** - develop a system to regularly audit your virtual machine security. Whenever possible, use tools to automate your security checks, balances and processes.

- **Patches** - Perform regular security patch maintenance, and create a schedule to ensure your patches are up-to-date for all virtual machines.

- **Overflow management** - When you have many virtual machines you will find they become hard to track; you need a reliable system in place to monitor them. You will also need to be aware of what each virtual machine is used for and manage it accordingly. While doing this, find ways to consolidate machines whenever possible and get rid of the ones that are under utilized.

- **Responsibility** - to ensure that the security of your virtual machines doesn’t slip through the cracks, designate one IT technician or manager to be responsible for it.

If you prioritize the security of your virtual machines and properly manage them, security can truly be a non-issue. If you’d like additional assistance with your virtualized infrastructure or would like to implement a new virtualization solution, give us a call today. *Published with permission from TechAdvisory.org*

### How to calculate your technology ROI

April 4, 2016

When purchasing new technology, how often do you consider its return on investment? For many business owners, calculating ROI is a tricky task that is sometimes skipped altogether. It shouldn’t be because if IT isn’t saving you money, it’s costing you money. Here’s how you can gain a better understanding of technology ROI and how you can calculate it in your business.

**ROI basics**

What does it mean to have a positive return on investment? It’s pretty simple. A positive ROI means the results a technology produces are greater than or equal to the amount of time and money invested. Obviously you want a positive ROI, but when is the right time to consider it? Should it be before or after you make a technology purchase? The answer is both. Before purchasing, you want to carefully consider whether a technology service or product is worth your money. Then months after you’ve implemented it, you should analyze whether or not you made a good investment. Also, don’t forget to look at your technology currently in use. Ask yourself, is your technology simply keeping the lights on? Or is it providing a solid foundation for your business to grow? If the answer is the former, there are likely better options out there worth investigating.
How to calculate ROI

When calculating ROI, it doesn’t have to be perfect. Here is a simple formula to get you started.

ROI = net gain/cost
Example: You spend $100 and make $150. Your net gain is $50
ROI = 50/100 = 50%

If you’ve yet to purchase a service or new equipment, you obviously don’t know how much profit it will generate. So you’ll have to do a bit of guesswork and estimation. It’s also important to consider some intangibles. Think about the productivity costs of staff time, disruption, and frustration (because most of us don’t work effectively when frustrated). Let’s take staff time for example. How much time will your staff save if you implement a Managed Services solution? With a Managed Service solution, your employees wouldn’t be responsible for putting out IT fires daily. The result = time that can be put towards marketing or growing your business. And that alone could make up for the costs of the technology investment itself.

Intangibles don’t just apply to saving time, frustration and disruptions, but also the costs of implementing the new technology. For example, how much time will be required to train your staff on the new technology? Also, how much time will it take to migrate from your old system to the new one? You should consider all of these when estimating your ROI.

Lastly, don’t forget to consider the unique circumstance of subscription purchases. Since you are usually paying these on a monthly basis, it can be a bit tricky to add up real costs. That’s why it’s important to use a timeline for these. For example, if you subscribe to software as a service, what’s the cost of that plan over the course of one year or five? How much money will you save over that time span?

What’s the benefit?

Besides the staffing example mentioned above, consider how a technology investment can create new revenue streams. For example, an investment in VoIP opens up an opportunity to offer video consulting to clients in parts of the country (or even world) that would normally be out of reach. This obviously leads to a new revenue stream and increased profits. So ask yourself, can the technology you’re considering create new revenue streams?
Next steps

Before making a technology purchase, it’s wise to talk with both management and end users about your decision. If you fail to consult your end users before implementation, they may disagree with your decision and therefore take longer to adapt or even rebel against it. Checking with them beforehand gives them a chance to offer valuable feedback on how it will be used in the trenches, and will get them onboard with the technology if you implement it. As for your management team, they can be a valuable resource to bounce ideas off of and gain insights about the technology you may have overlooked.

Lastly, ROI does not need to be calculated for every purchase. If you need to buy something small, like a new keyboard, just go and buy it. Save your ROI calculations for much larger investments that can have a dramatic impact on your business.

If you need help determining the ROI of a potential technology investment, feel free to give us a call for a chat. Our experts can help you determine the true benefits of a given technology and help you make a wise investment. Published with permission from TechAdvisory.org.

7 Warning signs of malware infection

March 29, 2016

As companies go to the Internet to conduct their business, their IT security becomes more vulnerable to many hackers and viruses. That’s why it’s even more important to recognize whether or not your systems are under threat from malicious software. So how do you know if your company’s IT security is under threat? Here are a few warning signs to tell if you are a victim of malware infection.

Slow computer

The most common symptom of a malware infection is a slow running computer. Are your operating systems and programs taking a while to start up? Is your data bandwidth suspiciously slow? If so, your computer may potentially have a virus.

However, before you immediately assume your computer has a virus, you should check if there are other causes to your computer slowing down. Check if you’re running out of RAM. For Windows,
open task manager (Ctrl + Shift + Esc) and go to the Performance tab and check how many gigabytes of RAM you are using under the Memory section. For Mac OS users, you can open the Activity Monitor app and under System Memory you should be able to find out your RAM usage.

Other causes of a slow system include a lack of space on your hard drive and damaged hardware. Once you’ve ruled out the other potential causes, then a virus may have infected your device.

**Blue screen of death (BSOD)**

If your PC crashes regularly, it’s usually either a technical problem with your system or a malware infection. You might not have installed the latest drivers for your device or the programs you’re running could possibly be incompatible with your hardware. If none of these problems are apparent in your PC, then the virus could be conflicting with other programs causing your crashes.

To check what caused your last BSOD go to Control Panel > System and Security > Administrative Tools > Event Viewer and select Windows Logs. Those marked with an “error” are your recorded crashes. For troubleshooting solutions, consult forums or your IT department to figure out what to do next.

**Programs opening and closing automatically**

Malware can also be present when your programs are opening and closing automatically. However, do check to see if programs are meant to behave this way or if they are simply incompatible to run with your hardware first before coming to the conclusion that your computer has a virus.

**Lack of storage space**

There are several types of malware that can manipulate the files saved on your computer. Most tend to fill up your hard drive with suspicious files. If you find unknown programs that you have never installed before, don’t open the application, search the program’s name over the Internet and use antivirus protections once you’re certain that it’s malware.

**Suspicious modem and hard drive activity**

Combined with the other warning signs, if your hard disk is working excessively while programs aren’t currently running or if you notice that your external modem is always lit, you should then scan your computer for viruses.
Pop-ups, websites, toolbars and other unwanted programs

These are irritating signs that your computer has a virus. Pop-ups come from clicking on suspicious pages, answering survey questions to access a website’s service or installing free applications. When you get pop-ups appearing out of the blue, refrain from clicking anywhere on the pop-up page and just close out of the window and use your anti-malware tool immediately.

Equally, free applications allow you to download their service for free but the installation process can be riddled with malware. When you’re installing a program from the Internet it’s easy to just skim over the terms and conditions page and repeatedly press next. This is where they get you. In the process of skipping over certain installation steps, you might have agreed to accept a new default browser, opening unwanted websites and other programs filled with viruses. Just be cautious the next time you download something for free. It’s best to try avoiding any of these practices when you can in order to protect your computer.

You’re sending out spam

If your friends are telling you that you’ve been offering them suspicious messages and links over social media or email, you might be a victim of spyware. These may be caused from setting weak passwords to your accounts or forgetting to logout of them.

In the end, it’s best to know how malicious software affects your computer so you can take steps to rectify the situation as soon as possible. Regardless of whether or not your system has experienced these symptoms, it’s always smart to perform regular malware scans to ensure your business is safe. Note: We recommend reporting any suspicious activity to your IT department or IT Company, before trying to run virus scans by yourself. To find out more about malware and IT security, contact us today. Published with permission from TechAdvisory.org

CCR Tech Tip
Spear-phishing email attacks on the rise

We’ve been getting more and more reports of data breaches resulting from email attacks. It’s important to know how to identify when you’re being targeted and how to reduce the chances of becoming a target. Please read below for some helpful tips on what you should be looking for.

The number one threat right now is “spear-phishing” attacks. The term “phishing” refers to someone posing as a trustworthy entity in attempt to acquire sensitive information. Spear-phishing is the same thing but directed towards a specific target. In a spear-phishing attack, a hacker will decide what data
they are after, then figure out who has access to that data and specifically target those people. For example, LinkedIn is a great source of information for hackers during the targeting step. Another source of useful information for hackers is public job postings. When job descriptions mention specific security systems it helps hackers to identify what they might be up against in their attack and plan around it.

**Spear-phishing scenario**
You get an email from the email address of your significant other that has in the subject line: *Honey, I had a little accident with the car*, and in the body: *I made some pictures with my smart phone, do you think this is going to be very expensive?* So, you click on what you thought was a picture of the damaged car but instead it installs a keylogger on your computer which then sends every keystroke back to the hacker every hour. Imagine the info they might collect in just one hour…usernames, passwords, credit card info, bank accounts, etc.

**Recognize email threats**
Email threats come in many forms. Here are some email characteristics to look out for:
- From an entity you are not familiar with.
- From an entity that you know but the email seems unusual or out of character.
- Email is a reply to a message that you never sent.
- Email is asking you to click on a link.
- Email contains bad grammar and spelling errors.
- You were CC’d on an email but don’t personally know the other people that it was sent to.
- Email was received at an unusual time of day, like 3 a.m.
- Email includes an attachment that isn’t related to the message.
- Email contains hyperlinks that, when hovering over them to see the URL, the URL is misspelled or is to a different website.

**Limit your exposure**
Limit your exposure online by using caution when adding your email address and/or job title to your social networking profiles. Also, remove references to any specific security systems you use in your organization.

*Brian Brimm*
**Director of Support Services**
**Center for Computer Resources, LLC***