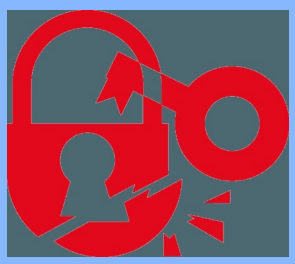
IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

APRIL 2016 SECURITY ALERT

Major vulnerability discovered in Windows!

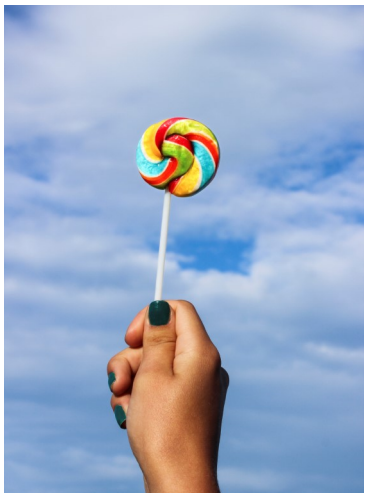
Visit www.IT-ON-DEMAND.com/BADLOCK for critical details.



APRIL 2016

This monthly publication provided courtesy of Howard Globus, Security Evangelist & Partner of **IT On Demand.**

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.



Which Flavor Of The Cloud Is Right For You?

Secure data backup, greater reliability, better resource and growth management options, and improved collaboration are just a few of the reasons to take full advantage of cloud computing today.

Yet understanding the choices you have can help you avoid some VERY costly mistakes you could wind up seriously regretting later. To help you move forward with confidence, here are some important points to consider.

Three "Flavors" Of The Cloud
Not all cloud models are the same. A cloud environment that works for a dental practice with a half dozen locations may not be entirely suitable for a new law firm with just a single office.

In determining what the best cloud model is for your organization, it's important to know how cloud services are structured. Basically, there are three types of cloud: public, private and hybrid.

Public Cloud Services Offer Flexibility And Lower Cost
A public cloud comprises a collection of data storage and software services that can be accessed on an as-needed monthly basis, somewhat like an electric utility or fitness club. It houses data facilities outside the corporate firewall that you access through an Internet browser without having to make any initial or ongoing capital investment.

Well-known examples of public cloud services include Google Drive, Microsoft Office Online, Apple iCloud and Amazon Cloud Drive. They provide data storage and, in many cases, web apps.

Public clouds are best used where a high level of privacy is not required. They can provide access to a growing pool of newer technologies that would not be affordable if developed individually.

Private Clouds Support Highly Specialized Apps
A private cloud resides within an

Continued on page 2

organization's firewall, and is typically owned, managed and supported by that business. IT resources are available to members of the organization from their own data center.

Private clouds can support highly specialized and/or privacy-restricted applications, like medical-records software for a health-care organization concerned about HIPPA requirements, for example.

"Each type of cloud has its own pros and cons."

And, while it can be more expensive to set up initially, a private cloud may deliver a higher ROI in the long run since you're not paying for ongoing shared services.

Hybrid Clouds: Balancing Complexity With Flexibility

Merging the flexibility of public cloud services with the control of a private cloud, a hybrid cloud can provide the ideal infrastructure for some organizations.

A hybrid cloud enables you to put some of your apps and data – archives and e-mail, for instance – in a public cloud, and the remainder in your private cloud. This provides the cost savings and benefits of the public cloud while retaining the customization and security advantages of a private cloud.

While it can be more complex to deploy and manage than a pure public or private cloud, a hybrid cloud may deliver the best blend of control, flexibility and cost-effectiveness for some organizations.

So Which "Flavor" Is Right For You?

There is no perfect solution – each type of cloud has its own pros and cons. That being said, here are a few key factors to consider when determining the best approach for your particular business:

Public cloud solutions are best suited to the flexibility and budget requirements of smaller businesses that want access to the kind of IT resources that bigger organizations can afford, without the cost of development and ongoing support and management.

A private cloud, managed and supported by an in-house IT team, may be ideal for your organization if control and privacy are of paramount concern.

A hybrid cloud could be the ideal solution for any enterprise that wants to manage sensitive data in-house while availing itself of third-party software and data storage for uses where the data involved isn't as sensitive.

How To Get The Best Professional Help

While hiring a cloud-computing expert can prove extremely beneficial in the long run, it's critical to work with a professional who has depth of experience in all types of cloud environments.

We've helped dozens of companies set up and run cost-effective, powerful and secure cloud networks. **For a Free Cloud Readiness Assessment, contact us at (212) 235-0260 or info@it-on-demand.com TODAY!**

Free Report Download: The Business Owner's Guide To IT Support Services And Fees

You will learn:

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim Your FREE Copy Today at www.it-on-demand.com/itbuyersguide/

Is Your Business Vulnerable To Ransomware Hackers?

Hacking for ransom is on the rise — on pace to beat out last year's figures — and hits people where it hurts, locking them out of files, photos and critical records until they pay hackers a bounty to restore their access. Hackers bait users to click on infected email links or open infected attachments, or they take advantage of outdated and vulnerable systems.

Victims see important files scrambled into encrypted gobbledygook, as an electronic ransom note warns that if they ever want to see those files again in a readable format, they must pay money in virtual currency, known as bitcoin.

Last year's 2,453 reports of ransomware hackings totaled a reported loss of $24.1 million, making up nearly one-third of the complaints over the past decade. They also represented 41 percent of the $57.6 million in reported losses since 2005. Such losses are significantly higher than any paid ransoms because companies routinely include remediation costs, lost productivity, legal fees and sometimes even the price of lost data in their estimates.

What's priceless is avoiding the hack altogether.

Here are five tips to make yourself a less likely victim:

MAKE SAFE AND SECURE BACKUPS

Once your files are encrypted, it's nearly always game over. Backups often are out of date and missing critical information.

Ransomware has become increasingly sophisticated and effective at separating users from the contents of their computers. For example, sometimes it targets backup files on an external drive. You should make multiple backups — to cloud services and using physical disk drives, at regular and frequent intervals. It's a good idea to back up files to a drive that remains entirely disconnected from your network.

UPDATE AND PATCH YOUR SYSTEMS

The recent samsam virus-like attack takes advantage of at least two security vulnerabilities on servers, including one discovered in 2007. Updating software will take care of some bad vulnerabilities. Browsers such as Chrome will automatically update behind the scenes, saving you the time and deterring hackers.

USE ANTIVIRUS SOFTWARE

It's basic but using antivirus will at least protect you from the most basic, well-known viruses by scanning your system against the known fingerprints of these viruses. Low-end criminals take advantage of less savvy users with such known viruses even though malware is constantly changing and antivirus is frequently days behind detecting it.

EDUCATE YOUR WORKFORCE

Basic cyber hygiene such as ensuring workers don't click on questionable links or open suspicious attachments can save headaches. System administrators should ensure that employees don't have unnecessary access to parts of the network that aren't critical to their work. This helps limit the spread of ransomware if hackers do get into your system.

IF HIT, DON'T WAIT AND SEE

When hackers hit MedStar Health Inc., the hospital chain shut down its network as soon as it discovered ransomware on its systems. That action prevented the continued encryption — and possible loss — of more files. Hackers will sometimes encourage you to keep your computer on and attached to the network but don't be fooled.

If you're facing a ransom demand and locked out of your files, law enforcement and cybersecurity experts discourage paying ransoms because it incentivizes hackers and pays for their future attacks. There's also no guarantee all files will be restored. Many organizations without updated backups may decide regaining access to critical files, such as customer data, and avoiding public embarrassment is worth the cost.

The hackers, of course, are counting on that.

Let IT-On-Demand guide you on the best security practices to avoid potential devastation. Contact us at (212) 235-0260 or email us at info@it-on-demand.com. We would love the opportunity to speak with you and discuss your security needs.

AP, The Associated Press, latams

Can Advances in Technology Also Cause Security Vulnerabilities?

If you are trying to run a successful business, there are many challenges standing in your way, and among the more significant issues is the threat of cyber vulnerabilities and hackers. Hackers are so advanced that they can break into anything to gather information, redistribute and alter it, and even control vehicles remotely. There's a saying that goes like this: ''There are only two types of companies. The ones that have been hacked and those that don't know they've been hacked''. This may sound like a cruel joke, but it isn't. Cyberspace is full of threats and the more we rely on technology, the more exposed we become to these kind of attacks.

Most of us by now have been faced with cyber security matters and had our devices hacked, either in our professional or personal life. One of the most significant cyber security breaks of late is the breach in 2015 by a group of security researchers who had managed to hack into a moving car, using its entertainment system to gain access into all additional systems. When the group took over the control of the car, they could control the air-conditioning, radio and windshield wiper. In addition, the car was automatically stopped by them so the passengers could have been seriously injured.

The cyber security threats are real and while the government does recognize the issue, they address it differently and with duplicity. For example, Assistant Attorney General John Carlin is promoting hack-proof super-secure cars while at the same time FBI Director James Comey is pressuring the phone manufacturers to make the phones *less* secure so that the law enforcement can access them. Recognizing how important it is to make cars hack-proof from the very beginning is an important step, however with the other story in mind, one must question if the government will request that all car manufacturers make cars less secure as well.

While it may seem legitimate for the law enforcement to be able to access this personal information, especially with the terrorist threats in mind, we also have to wonder if this would leave the gates open for the hackers as well. Hackers work either alone or in organized parties and they pose a critical threat to everything and everybody. Cyber security breaches can cause various types of damage, from unauthorized access to sensitive and personal data to financial malversations, and even further to inflicting physical damage by remotely controlling automobiles. While we are using the internet more and more to try to improve our quality of life, that very idea is causing key security concerns.

Let our security experts at IT On Demand assist you with your company's network security. Call us at (212)235-0260 or email us info@it-on-demand.com.

Sources: The Intercept, McLaughlin & Naked Security/Sophos, Zorabedian