TECHMinutes

March 2017

Your Business Technology Information Source!

This Issue:

Tips for Getting the Most Out of Your IT Consultant

Budgeting accurately for your long-term IT needs requires an intimate knowledge about technology and IT trends. Compared to other department budgets that are easy to compile by making a...

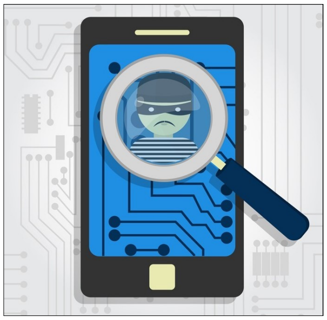
Read the Rest Online! http://bit.ly/2k3LRjp

About Pulse

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing , Enterprise-Level IT services for big businesses, small businesses, and medium-sized businesses.

Visit us **online** at:
newsletter.pulse.tech

Pulse Technology Solutions Teams Up With SecuSolutions Ltd. To Combat Cyber Attacks



Pulse Technology Solutions forms strategic alliance with SecuSolutions Ltd. to help combat cyber attacks

FORT MYERS, Fla. (Feb. 15, 2017) – James Ritter, founder and CEO of Pulse Technology Solutions (www.Pulse.Tech) (http://www.Pulse.Tech) has announced that a formal agreement has been finalized with SecuSolutions Ltd, one of North America's leading cyber security solutions for business.

The agreement positions Pulse Tech as an exclusive, full service reseller, offering support to small, medium and large businesses with an award-winning management team of IT experts. Partnering with SecuSolutions enables Pulse to provide premium security products that help companies identify and combat malicious cyber-attacks.

As a local, regional and national leader in the IT industry, Pulse Tech has more than 10 years' experience in providing IT management and support, cloud computing solutions and IT security, making the company uniquely qualified to provide SecuSolutions' products to its clients. One product in particular, the SecuScan Vulnerability Detection System, is especially relevant as it helps to minimize attacks against networks and confirms compliance. SecuScan offers high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, all in an intuitively designed user interface.

"During these uncertain times, it is more important than ever for us to protect our clients' network security," said Ritter. "Providing SecuSolutions' products will ensure our clients are

(Continued on page 4)

The 6 Most Common Technology Issues Faced By SMBs

While news sources might lead the layman to believe that most issues facing the typical SMB come from cyber criminals lurking online, the reality is far less dramatic. However, this misconception makes these issues no less serious, and still things to prepare for. Let's review some of the most common causes of technological issues in the office environment.

1. Lack of Strategy and Compatibility: When two high-ranking decision makers aren't on the same page, troubles typically ensue. Simply put, sometimes the goals set by administration don't match up with those of IT, and vice versa. This situation can often prolong the time projects can take, or throw the entire project into disarray.

2. BDR Shortcomings: The worst time to consider what to do in the face of a data disaster is after one has struck your business. However, many small businesses are neglectful in their precautionary preparations, assuming that the chances of disaster are too low to make an investment into a backup and data recovery solution. While this might save them in the short term, they jeopardize their financial future by exposing their business to the expensive repercussions of a data disaster.

3. Unknown Root Causes: In IT, it is not uncommon for a minor issue to be indicative of a much larger, more problematic concern. It is also common for these larger concerns to go

(Continued on page 2)

Why Managed IT Services are a Perfect Fit for Growing Businesses

A small business is just as susceptible to the many problems that face large enterprises, and the dangers only multiply with the more technology you implement in the office. The larger your network gets, the more difficult data distribution and storage becomes.

The more employees you work with, the more devices that will appear in the office. The more data you work with, the more likely you are to get hacked. These are all very real risks. What are you doing to protect your company from these threats?

We'd like to present one surefire way to dodge the majority of problems associated with business technology management: outsourced IT services from Pulse Technology Solutions. We can use our proactive approach to take care of your technology so that you can focus on running your business. While we offer many different types of services, here is a brief rundown of some of our popular ones.

Data Backup and Disaster Recovery

Have you taken the time to think about what your business would do if it suddenly lost all of its data? If not, do so now. It could be much more than just a couple of months' worth of leads put at risk. An untimely hardware failure could have lasting effects on the way that your business functions. You'll need to replace the hardware, which could take several days, or even weeks. During this time, your business isn't working as intended, which can severely damage your productivity. Instead of suffering from this unfortunate occurrence, you can implement a BDR to take multiple copies of your data and keep them safe for recovery at a later date. BDR is designed to eliminate downtime and take a proactive stance against data loss due to natural disasters, hacking attacks, user error, and more.

Remote Monitoring and Maintenance

Most problems with your technology can be resolved remotely, without the need for an expensive on-site visit. Managed IT services capitalize on this convenience by allowing you to get the help that you need, when you need it. This cuts out waiting for the technician to arrive on-site and keeps downtime caused by the issue to a minimum, allowing you to get the problem fixed right away and get right back to work. Furthermore, we can apply any necessary patches and security updates remotely so that you will always be protected from existing and developing threats.

Network Security

Hacking attacks and security threats will always be one of the most dangerous parts of running a business. Some of the scariest threats currently on the Internet include ransomware and botnets that enslave Internet of Things devices. Only a cybersecurity professional knows how to identify and prevent infections from known threats. We can equip your business with a comprehensive Unified...

Read the Rest Online!
http://bit.ly/2jZk7MD

The 6 Most Common Technology Issues Faced By SMBs

(Continued from page 1)

unnoticed as the minor side effect is repeatedly resolved without any further digging. As a result, the larger concern may be more difficult to resolve when it eventually is noticed, causing a much larger drain on a company's resources.

4. Waiting for an Issue to Occur: While there is wisdom in the motto, "if it ain't broke, don't fix it," it simply doesn't apply to a business's technology. Proper care and maintenance can help prevent critical issues. Many issues of this type demand total attention from your staff and prevent productivity until they are resolved, most likely at a much higher cost than it would be to simply prevent them.

5. Legitimate Security Issues: Even though there are far more ways for things to go wrong due to internal complications, no business can disregard the threats that are lying in wait to snatch sensitive information once the opportunity presents itself. Yet many small businesses are lax in their security solutions, assuming that their size will prevent them from being targeted. However, their lack of adequate protections allows viruses and malware to do their worst with ease, as cyber criminals have no problem with snagging low-hanging fruit.

6. Troubles for Users: If the technology that employees use to complete their work can no longer provide the operability that their responsibilities require, a business will feel the results. These results usually take the form of decreased employee productivity, morale, and time well spent.

Clearly, while the threats posed by malicious entities online shouldn't be underestimated, these common issues can not be ignored if a business wants to stay in business. However, by setting a standard for your daily operations to follow, you can keep your company from being tripped up in these issues.

Pulse Technology Solutions can help. We have considerable experience in helping businesses take the necessary steps to circumvent these issues, preventing downtime and lost productivity.

Give us a call at 239-362-9902 to learn more.

Share this Article!
http://bit.ly/2jYL6bg

4 New Technologies that Can Revolutionize Your Business

New technology paves the way for businesses to leverage their resources in exciting ways. Of course, it's impossible to take advantage of these benefits if you don't even know these new technologies exist. Therefore, to help you achieve an edge over your competition, consider how these four new technologies can enhance your business model.

Smart Virtual Personal Assistants (SVPAs)

Think of SVPAs as virtual executive assistants. These "predictive intelligence" apps use voice recognition to sort through personal data from email messages, address books, calendars, and task lists in order to anticipate the next logical step and drastically boost daily efficiency. Apple, Google, and Yahoo all recently acquired SVPA apps to integrate into predictive products, from mobile apps to smart speakers, helping users get tasks done even before they would remember to do it otherwise.

Security and Privacy Solutions

A perennial on Webbmedia's list, privacy concerns remain top-of-mind for wired Americans. According to a Pew Internet and Society poll, 91 percent agree that consumers have lost control of their personal data. Adobe, Dropbox, and Snapchat have experienced major password breaches, and Target and Home Depot had credit card data from millions of customers stolen by hackers. To address these system breaches and reduce the widespread public mistrust, companies are looking to spend more resources on password security and encryption management. To assist with this, Twitter released Digits, a two-way authentication service that sends one-time confirmation codes via texts, which will be offered to mobile apps.

Internet of Things

Thanks to the Internet of Things, the world we live in is now surrounded by an unprecedented number of devices with the ability to communicate directly with one another, similar to how the Nike FuelBand connects to the coffee maker. These devices will become a vital part of our day-to-day home, work, travel, and shopping experience. The implications on how IoT devices can enhance the productivity and connectivity of businesses as only limited by imagination and the ways that these vast networks can be secured...

Read the Rest Online!
http://bit.ly/2jYU1JQ

The Most Popular Domains Make the Biggest Targets for Email Spoofing

Let's say that you receive an email from a software vendor, say, Microsoft. When you are contacted by a major company like this, do you automatically assume that it's secure, or are you skeptical that it's a scam? Ordinarily, it might not seem like a big issue, but all it takes is one click on an infected attachment or malicious link to infect your business's infrastructure.

According to a Swedish cybersecurity firm called Detectify, there are major online domains that are at risk of email spoofing due to misconfigured server settings. Email spoofing is the act of sending a message, while masking the true email address that it comes from. This allows hackers to forge the sender address to suit their needs. Generally speaking, email messages don't have automatic authentication built into them. This is something that must be configured on the server side of things.

Thankfully, there are ways to properly configure your email server, but unless you're a hardcore techie, you run the risk of either configuring the system incorrectly, or changing settings that may compromise your security. Yet, it's still important to keep in mind how the solutions that prevent email spoofing, work. Here's a breakdown of the details:

- **Sender Policy Framework (SPF):** This is a record that's checked alongside the DNS (Domain Name System) record, in order to decide whether or not the server is allowed to send email using the specific domain. SPF uses three identifiers for its messages: softfail (accept the message, but mark it as spam), hardfail (reject the message entirely), and neutral (do nothing and let the message through unhindered).
- **DomainKeys Identified Mail (DKIM):** DKIM hashes the body and the header of the email separately, and creates a private key that gets sent with the message. Once the message is received, the key will perform a DNS request to see where the email originated. If everything adds up properly, the message is received.
- **Domain-based Message Authentication Reporting and Conformance (DMARC):** DMARC is considered the ideal solution, as it makes use of both SPF and DKIM to identify an email. DMARC's functions split into three: reject (a full rejection, and the end-user never sees the message), quarantine (the message is stored for your review), and none (allow the message through). The idea is to either identify messages as fraudulent, or provide the system administrators with the ability to review them and make the...

Read the Rest Online!
http://bit.ly/2lPp6BO

You Know Who's Looking Forward to Tax Season? Identity Thieves

One of the most high-profile hacking attacks in the United States struck last year when the Internal Revenue Service (IRS) was breached. 464,000 Social Security numbers were swiped; enough to file 101,000 tax returns using false personal identification numbers. Every organization can learn how to better protect themselves during tax return season, especially since you have so much on the line every year.

In response to the aforementioned threat, the IRS has made several improvements that allow the organization to (hopefully) better protect taxpayers as they perform their financial obligations. Specifically, these improvements are effective "before, during, and after a tax return is filed." On the IRS's official website, "This is highlighted by the number of new people reporting stolen identities on federal tax returns falling by more than 50 percent, with nearly 275,000 fewer victims compared to a year ago."

One of the best tools that the IRS has used to cut down on these concerning identity theft numbers is an annual security summit. In part, the following results have been attributed to the summit:

- Fraudulent returns are being stopped more frequently before processing: The IRS accounted for almost 50 percent fewer fraudulent returns, which amounts to about 787,000 identity theft returns from January 2016 to September 2016. These returns would have totaled well over $4 billion.
- A significant decrease in fraudulent refunds: 106 new institutions became bank partners since 2015, and this played a role in cutting fraudulent refunds. The number of refunds...

Read the Rest Online!
http://bit.ly/2jZf9zP

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

James Ritter
Founder & CEO

Pulse Technology Solutions Teams Up With SecuSolutions Ltd. To Combat Cyber Attacks

(Continued from page 1)

equipped with the latest technology to keep them safe from online predators."

For more information, visit Pulse.Tech or call us at 239-676-6679.

More about Pulse Technology Solutions Headquartered in Fort Myers, Fla. since 2006, Pulse Technology Solutions (www.Pulse.Tech) is a managed technology firm owned and managed by James Ritter. The firm has provided outsource technology for hundreds of clients, large and small throughout the state of Florida, regionally and nationally. Pulse Tech offers innovative technology combined with solid business solutions, preventing problems before they happen and optimizing clients' businesses. Services include IT management and support, cloud computing solutions, IT security and business continuity.

Contact us for more information!

Share this Article!
http://bit.ly/2lMrjOD

Tech Trivia

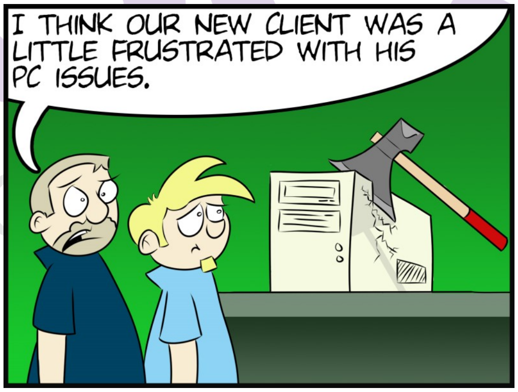
Gerald A. Lawson - created the first cartridge-based video game system.

Pulse

12611 New Brittany Blvd.
Bldg# 18 Fort Myers,
Florida 33907
Voice: 239-362-9902

Visit us **online** at:
newsletter.pulse.tech

newsletter@pulse.tech
facebook.pulse.tech
linkedin.pulse.tech
twitter.pulse.tech
blog.pulse.tech


I THINK OUR NEW CLIENT WAS A LITTLE FRUSTRATED WITH HIS PC ISSUES.