hAPPenings

March 2019

PIONEERING PROGRAMMERS

Hello and welcome to March's hAPPening's. This month we're focusing solely on security – cyber security in particular. You can never be too careful when it comes to securing your network – whether at home or at work. As the developments in technology continue to improve at an exceptional rate, so do the threats from cyber criminals.

FOLLOW BEST PRACTICE WHEN IT COMES TO MSO CYBER SECURITY

Keeping your organization safe and far away from cyber security related issues is becoming increasingly difficult for businesses around the United States. The time between attacks and massive data leaks over the last decade hasn't been much. It seems like businesses are at the mercy of hackers most of the time and can only pour more and more money into adopting the latest cybersecurity technology and hiring the most expensive consultants.

Good news is that regardless of the size of your organization, there are certain steps that you can take as head of the company or even the IT department which will ensure the best possible protection.

Most of the time, it isn't the amount you invest into cybersecurity, it is the preventive measures adopted by an organization which really make the difference.

Here are some of the best practices which can be adopted early and save any business from a potentially unrecoverable situation.

Regular Backups and Disaster Recovery Plans

The need to be prepared for the worst should be done during the best times. There is no telling when the tables can turn and hackers do not do the deed with prior warning. Ensuring that all sensitive data is

backed up and kept in secure locations is the first and foremost solution to a good disaster recovery plan. Without having certain protocols in place may result in losing data forever and even being unable to recover it. Do not depend on default and basic systems to do the work. Make sure that you are backing up systems for yourself and your client by going the extra mile on certain servers and in the cloud, which are completely off limits and inaccessible.

Cyber Security Starts from Within

The easiest way for an outsider to get into the realms of your business is from a minor mistake made from someone on the inside. The proven way to ensure that employees know what is right and wrong when it comes to cyber security is by educating and spreading the knowledge of how to stay safe.

A deadly virus, malware infected software or even weak passwords can all be exploited by something as simple and unthreatening as a USB drive which someone in marketing or sales may put into one of their systems. You may expect everyone in IT to have it down and understood, but in realty, it may come as a shock as to how many employees in the tech sector fail to underestimate the consequences of their minor mistakes.

Cyber security has become one of those monstrosities which companies are unwilling to take on head first and would just rather outsource. The reality is that the smallest precautionary measures end up playing the biggest and strongest defense. By keeping software and hardware updated to the latest versions, along with knowing which aspects of business are most at risk, businesses can stay one step ahead of perpetrators before it is too late. Go ahead and assess your company's situation and see how much is at risk as of right now. You may be surprised to see that a hacker could have gotten in without any real effort at all.

Pioneering Newsbytes

Samsung and Huawei Battle for Foldable Smartphone Greatness

Samsung has already released its new Samsung Galaxy Fold and Huawei is yet to officially release the Mate X, but both smartphone giants are looking to battel it out for foldable phone greatness. It is a new generation in smartphone technology as devices are getting larger and increasing in their functionalities. Both devices have large screens and fold into much larger, sharper looking tablet sized phones. Dual batteries on each device make it all that much more attractive, but with price tags even crossing the $2,000 mark, it could a tech revolution only a few will be able to afford in the start.

DATA PROTECTION – VITAL FOR EVERY MSP

Being an MSP is stressful business, we all know that. You are probably wondering if there is something new in this post that you already haven't heard before. That is unfortunately the situation of today. The risk to data has never been greater than it is now and MSPs have to be constantly on their feet with eyes open to ensure customers are being protected at all costs.

This could mean changing policies and procedures regarding client data protection based on how hackers are behaving in the market today. It may seem like a warranted aspect of having a business, but keeping data safe is just one part of the job of being an MSP that their customers can rely on.

If 2019 is the year you plan to focus on data protection for your clients, then the following points are vital for that plan to succeed:

Build Awareness Among Clients

With your clients knowing just even the basics of how they can better protect their data and presence in the online world, half of the headache of providing data security is slashed right then and there. This is why it's a popular saying. Better safe than sorry.

There are a hundred things that can go wrong and as many techniques available to combat a breach of data, but knowing how to avoid such situations altogether makes doing business that much easier. The way to do this is to hold regular training sessions for clients, especially new ones which are being onboarded. Let them know of the basics and how they can protect themselves first before the experts need to come in. Showing monetary and reputational benefits of doing the needed can add that needed incentive to take things seriously.

You could also introduce plans to cut some of their extra charges which you may be included for added data security if they follow the rules. This is what insurance companies are doing. An example of this is where one auto insurance company reduces deductibles by 10% every year a claim isn't made. This is a small incentive, but one which really gets car owners thinking about their driving habits, resulting in longer term profits for the insurance provider.

Demonstrate What a Security Breach Would Result In

Everyone thinks that a breach of security and a serious hack could never happen to their organization. It is easy and even childish to imagine that hackers would never consider getting into your company's servers and exploiting whatever they can find. Clients are even known to question the sensitivity of their data in the first place. This is why even demonstrating a simulation of what a catastrophe it could be for them, if a breach of data was to ever happen, could set them straight.

Cyber security is ultimately a game of being one step ahead of the offensive by playing a good defence. Know the weaknesses and address the issues before things potentially get out of hand. The better aware your clients are, the more they will trust you with their data protection requirements.

COMMON CYBER THREATS IT PROVIDERS SHOULD PROTECT AGAINST

The world of cyber security has become a scary place to be in the modern business environment. Why? Because essentially every business is now completely online and relies on being connected to the cloud or remote storage devices to have access to important information virtually round the clock. Businesses are expanding to the point where there are people all around the globe in various locations accessing that information and need to be able to do so as they please.

Not having the proper security measures in place could result in everything going down in an instant. This is why it is expected that cybercrime related damages could be in the trillions of dollars in the next few years if companies continue to resort to saving money on costs associated to having tough cyber security policies in place. What are the biggest cyber threats to businesses today? Keep yourself updated and protected. This is the first step in being a better MSP for years to come.

Phishing is Way Too Common for Comfort

That email which seems like your bank account statement, asking for private information in order to unlock the attached file or clicking on a link to recover lost data may seem harmless. Unfortunately, phishing has become the choice of hackers globally to get into the personal lives of employees in an instant.

In that very moment, a hacker will be able to access everything associated with that account they are trying to access if people do not recognize the common signs of an email being a phishing scam. This is popular amongst Apple users who continue to regularly receive seemingly real bill statements by a fake address of Apple. Not paying attention could result in a loss of everything you have worked so hard for in the blink of an eye.

MSPs need to ensure that their clients are aware of emails which may seem legitimate, but are actually not from a trusted source. It is important to never give out sensitive information over an email or to even someone calling you over the phone. If there is even a one percent of a doubt, it should not be followed through with.

Ransomware is Highly Damaging

Remember hearing about several companies around the world which were infected with ransomware and a demand of money was made in order for their private data to be restored? This sort of attack spread like wildfire and millions of dollars were lost, plus a lot more worth in terms of data as well. Businesses were just completely unprepared for anything of that sort to ever happen to them and it certainly is not going to be the last time either.

Operating systems and even the hardware being used by a client needs to be regularly monitored and updated. This can be done by using quality endpoint protection software on all devices and training employees to be more aware of their tactics.

Hackers will always be coming up with new and innovative ways of trying to get past your firewall. Are you ensuring everything that can be done is so that you don't end up losing everything?

HOW TO PROTECT YOUR CLIENTS FROM RANSOMWARE

Hearing about companies losing sensitive data and hundreds of thousands and even millions of dollars to hackers' demands is becoming too common of a story. This is leading us to become more desensitized to just how monumental of an issue it is. Protecting your own business, as an MSP, is the first step in ensuring that you will be able to protect your clients from the most destructive of situations.

As technology rapidly advances and being on the cloud just becomes second nature, it is vital to understand just how desperate cyber criminals are really becoming. Protecting clients from ransomware needs to be a top priority for MSPs now and while it may seem like an impossible task at first, there are reasonably simple ways of ensuring it is done the right way.

Do a Thorough Assessment

It is ideal to know what the current situation is and where the security risk level can be placed on a variety of your clients. Develop an emergency situation standard which is regularly conveyed to clients based on an assessment your security team is able to do on a set basis.

When onboarding new clients, a security assessment should be done right at the start of things to know better what they and you also can expect moving forward. Without the right steps taken to ensure cyber security is at the optimal level, it could be a dire situation not to far down the road.

Build Client Resilience

The methodology of teaching a man to fish, rather than to give him a fish each time is of immense value in this modern cyber security climate. Let clients be the first and strongest line of defence against any attacks in the form of phishing emails, ransomware or malware getting into their systems. In reality, they are

the first line of defense and always will be.

It is not possible to hold their hands throughout normal day to day business operations, but building the resilience of clients to be able to identify and stay safe from potential risks can make everyone's life that much easier.

Since emails hold such a great value for every business, these are usually the first entry points hackers use to get vulnerable people to allow them inside. One an attacker has gained access, it is hard to assess the level of damage done or even if they are completely out of the system yet or not.
Always Prepare for the Worst

A good MSP makes sure the preventive measures are taken, a great MSP ensures that there are regularly taken backups which can come into play at any moment. The greatest loss a business, more specifically a client of yours could face, is that of losing sensitive data. Having those recovery systems working as soon as something goes wrong will keep clients from reaching the edge of their seats. How could they not want to continue doing business with an MSP like that?

There isn't always the need to invest a large amount of money to make things a success. Simple steps taken can make doing business more effective and sustainable in the long run.

Pioneering Newsbytes

Apple Watch Series 5 Hitting the Market in March

People are still getting used to the idea of having a smart watch on their recent, literally monitoring their every statement, but Apple is already getting set to release the 5th generation of its popular Apple Watch series. With a highly anticipated exclusive to the United States ECG feature, people are looking forward to getting better insight into their health without having to undergo complex, and at times, expensive procedures. Experts regard this as a breakthrough in tech bringing health to home and is only the first step to a future of healthier, happier people. The Apple Watch Series 5 is expected to release in the last week of March 2019.

PIONEERING
PROGRAMMERS

www.devs4msps.com
www.pioneeringprogrammers.com

1059 S Sherman Street
#140 Richardson, Texas, TX 75081

info@devs4msps.com

972-895-3100