ISSUE 53 JUNE 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

The 6 Minimum Secuirty Measures Every Buisness Needs:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

SonicWall reports there were 304.7 million ransomware attacks, 51.1 million crypto-jacking attacks, and 32.2 million IoT malware attacks in 2021. The report states that attackers targeted web applications with financial and personal information for a big payday. "Even if you get your data back," says RJ2 President, Jeff Dann, "it could still be sold on the dark web. Not only do these criminals want your money, but they are also compromising your reputation. The trust of your customers, your vendors, and potential legal action could cause irreversible damages from a breach." The question is this: "How do you know if your security is up to the challenge?"

How Do Your Cybersecurity Solutions Measure Up?

With today's massive rise in cyberattacks, many more MSPs and businesses are implementing security measures to better protect their data. While they may think they are protected sufficiently, too many are woefully negligent. With the large volume of activity coming from bad actors today, companies need validation that their data assets are safe. Jeff says, "the first thing my team asks prospective clients is: "Do you feel you have the proper cybersecurity stack in place to protect your business?".Too many IT departments don't know because they've never really tested their security measures to see if they are configured properly to provide the expected protection needed to avoid attacks. Using a well-established cybersecurity framework like NIST is key because it's based on the five pillars of identification, protection, detection, response, and recovery. Focusing on these phases creates a security blanket over your IT enterprise to mitigate and respond to an attack. Ignore even one of those areas, and your business is vulnerable.

Minimum Cybersecurity Requirements to Keep Your Company Safe:

- A strict, company-wide password policy
- An enterprise-level firewall with URL filtering, IPS/IDS, and Geofencing
- Multiple instances for your data backup solution, tested daily and redundant off premise
- Multifactor authentication to access your network and cloud services
- Advanced Endpoint Protection (EDR) with a SOC
- Advanced Email SPAM filtering with Threat Protection is key, as well as an Awareness training solution for staff on how to protect against attacks.

Too many IT professionals neglect these critical measures. A lack of testing, rarely auditing their security, and neglecting routine process and procedure measures all create opportunities for the bad actors to attack.

Effective Cybersecurity Starts with Multiple Layers of Protection:

Today's criminals are always inventing new ways to steal your data or create a means to extort money from you for holding your data hostage. . Just a couple layers of protection are like having no protection at all. An overlapping umbrella strategy is currently recommendation.

Continued on page 2.

CONTINUED...

As new threats are presented, the security industry is closing those vulnerabilities, so staying up to date on the latest technology is a good practice to have. Remember it is not if you will be hacked, it is when. You must be prepared and tested to respond.

The cybersecurity stack of solutions we implement here at RJ2 Technologies is a differentiating factor in the marketplace. We bring in industry-leading cybersecurity products and require our engineers and techs to obtain training certifications with these products. The minute the solution has been vetted and the staff has become trained, those technologies become part of their cybersecurity stack.

“We want to work with business owners who truly value IT as an asset. That’s why all customers under a managed services agreement must maintain operating standards, including a full stack of cybersecurity solutions,” Jeff says. Plus, companies must have a reliable backup solution that has both an on-premises server and a primary cloud-based backup solution that’s replicated to a secondary cloud instance in a separate data center. This redundancy is important to ensure you have the means to restore data and configurations.

Here at RJ2 Technologies, we require an up-to-date and complex password policy. It is recommended that your business uses an offsite password vault that changes each password after every use. This keeps any residual reference to admin passwords on the network automatically non-actionable by hackers. It is also crucial to train your team on phishing attacks. The majority of all breaches are caused by people opening dangerous emails or clicking on links mimicking normal business communications.

No matter what solutions you put in place, you must adopt a regimen of testing your solutions, including penetration tests and vulnerability scans. An IT audit is the examination and evaluation of an organization’s information technology enterprise, including the IT infrastructure, line of business applications, policies, procedures, and operational processes against recognized standards. Normally performed by a third party and not your current IT personnel or Managed Service Provider.

However, keep in mind that security solutions provide no guarantee that your business won’t get breached. However, implementing a layered approach of solid cybersecurity solutions will mitigate the known areas of vulnerabilities hackers try to exploit. Collectively implementing a solid security umbrella over the IT infrastructure and annually auditing your security programs with a qualified third-party consultant is your best chance to avoid a breach. Developing a strong incident response plan, disaster recovery plan and business continuity plan so your business is ensured to be able to respond to threats and operate while your systems and data are being restored is the best defense against cybercriminals.

RJ2 SPOTLIGHT

Josh Stenger

Marketing Coordinator

Josh Stenger recently joined the RJ2 family, joining in January of 2022. Josh graduated from the University of Wisconsin-La Crosse in December of 2021 with a bachelor’s degree in marketing and a minor in information systems. During Josh’s time at college, he wrestled at UWL for 4 years and helped local youth wrestling programs.

Fun Fact: Josh caught a 400 lb. saw fish while deep sea fishing off the coast of Marco Island, Florida.

Where’s your favorite place in the world?

- Probably Maui, Hawaii

What do you like to do when you aren’t working?

- I like to spend my time outside either golfing, hiking, coaching, playing frisbee golf, or anything that keeps me active

What is the best career lesson you’ve learned so far?

- Don’t be afraid to ask questions

What is your favorite part of working at RJ2?

- Everyone is super friendly and willing to help you. And it’s a hybrid work environment.

If you could meet anyone in the world, dead or alive, who would it be and why?

- If I could meet anyone in the world living or dead, I’d probably want to meet Julius Caesar. I don’t have a particular reason other than it would be cool to talk to someone so old.

VoIP Quality of Service: What You Need to Know When Choosing a Provider:

More businesses have been making the switch to Voice over Internet Protocol (VoIP) because of its variety of benefits such as lower costs, scalability, and flexibility. However, there are many different VoIP providers and packages to choose from that can make it difficult to find which is the right fit for your business. One important factor to consider is the Quality of Service (QoS) offered by a provider. In this blog we will cover a quick guide to VoIP QoS and everything you will need to know about it before making a decision.

WHAT IS QOS?

QoS can be defined as the specifications and requirements that define the overall performance of a VoIP system or network. This performance is usually measured by looking at objective statistics like bandwidth usage, transmission delay, call jitter, error rates, and the like. Subjective data, like what end users think of the system's performance, is also factored in.

Featured Partner:

Sentinel One

SentinelOne is the only cybersecurity platform purpose-built for the remote workforce. Replace legacy antivirus with cybersecurity for the endpoint, cloud, and IoT.

WHY DOES QOS VARY AMONG PROVIDERS?

QoS applies not only to VoIP but also to traditional phone systems. It would not be an exaggeration to say that the quality of landline calls is near perfect. This is because all traditional phone network providers invest in physical networks and connections that offer high QoS. This means switching from one provider to another doesn't affect the quality of the calls.

However, investments in physical networks are expensive, and customers end up shouldering the costs. The high cost of maintaining the transmission network is also why there are only a couple of phone providers in most areas. In other words, it's just too costly for small companies to invest in a traditional phone network system.

In comparison, VoIP systems are considerably cheaper to set up and maintain, leading to a high number of VoIP providers. And because anyone with capital can set up their VoIP systems without having to adhere to a standard, the QoS amongst providers can vary drastically. To find the provider with the best QoS, ask them these three questions:

1. What level of quality can you guarantee?

The best providers will be able to guarantee a QoS that is comparable to or even better than traditional phone networks. This is especially important for businesses that are looking to switch to a full VoIP solution. Ask your prospective provider to run a few tests on your network and to give you a quality assurance. If the numbers are too low for your business needs, it's best to look for another provider. For more help on determining which provider and packages are best for you, check out SkyCom. Their team of experts will guide you along the process of choosing the best solution for you at an affordable cost.

2. How much of the network infrastructure do you own?

Almost every VoIP provider will rely on public infrastructure in order to transmit data. And usually, the bigger the company's share in the infrastructure, the higher its QoS is. This is because the provider will have more control over the technology. As such, one of the best options is to look for facilities-based providers. These companies own almost all of the network that carries VoIP calls and can therefore offer better services and quality.

3. How much traffic will run over public internet?

Some of the most popular solutions will use almost 100% public internet for their traffic, while other companies will use a mixture of public and private networks. The latter option allows better flexibility as these providers often use public internet for more affordable packages and private internet for high-end users. If you often use VoIP for functions that require heavy bandwidth like conference calling, then you may need to sign up for more expensive packages so the QoS doesn't drop.

Get in touch with a team of experts today if you want to know more about how VoIP can benefit your business. Contact SkyCom, a Chicago based company that provides businesses with reliable hosted phone systems through solutions like VoIP, hosted PBX, Unified Communications, and Virtual Auto Attendant & Mobile VoIP.

What Causes Slow Internet Speeds On Mobile Phones?:

Have you ever experienced days of slow internet connection where your device says you're connected to the internet, but your connection is still slow? You probably have and it can be very annoying, especially when you just need to get work done. Many people experience slow speeds on their devices, but lucky for you, we've put together five of the most common causes of slow internet on mobile devices and how these issues can be solved.

ROUTER LOCATION

The first solution we have for you tends to go overlooked in many homes/offices. Although your Wi-Fi router has a range of about 230 feet, the signal still tends to get weaker the further it is from your device. Also, large objects such as doors and walls situated between you and your device can cause a weaker connection which results in slower internet speeds.

To strengthen your connection throughout the home or office, we recommend placing your router in a centralized location, preferably away from concrete walls or large, dense objects such as fireplaces. A router radiates a signal in all directions, and if it is blocked by even just one large object, you will experience a weaker Wi-Fi connection which results in slower internet speeds on your mobile device.

WI-FI NOISE

As you may know, other electronic devices emit wireless signals as well and typically their frequency tends to be similar to that of your routers, which is 2.4 GHz. So if you have a lot of electronic devices or live in an apartment/condo, there's a good chance that other electronic devices may be causing interference with your router. The simple fix to this solution is to place your router in a centralized location away from other electronic devices.

However, sometimes it isn't possible to place your router in a centralized location away from other devices. If this is the case for you, there is another option that you might find helpful, but requires you to know if your phone supports 5 GHz. You can try changing the frequency or channel that your router is broadcasting on. To accomplish this, log in to your routers settings page, then locate a page that says "wireless settings" or "channel." For most routers this tends to be 5GHz, but you'll still want to ensure that your mobile device is capable of operating at a 5GHz frequency.

FLUCTUATING NETWORK SPEED

Another possible reason for your router's slow internet connection could be due to fluctuating network speeds. Often times, router's experience fluctuating network speeds when there are many devices connected or if some of the devices require a strong network connection such as streaming movies, downloading video games, or even some software updates.

To fix this issue, increase your router's bandwidth speed. This way, every mobile device on the network will enjoy a faster, more stable connection.

POOR VPN CONNECTION

A virtual private network is a great resource to use when you are looking to increase your security measures. However, if your VPN connection is experiencing slow/poor connection, it can affect the speed of your internet connection. To fix this issue, switch to a different VPN server or switch to a different VPN protocol.

You can also disable your VPN to increase your network speeds but this will decrease your devices security. If your are on a private network such as at home or in the office, it should be ok to disable your VPN to enjoy the faster internet speeds.

FULL BROWSER CACHE

Your mobile browser's cache stores data from previous searches you've made to faster display results of similar searches in the future. While this makes your phone more efficient, it also has makes your internet connection much slower when using the internet for other activities.

You can clear your cache manually or use a cache cleaner app to get rid of useless data and optimize your phone's internet speed. If you decide to download a cache cleaner app, make sure that it is trustworthy so you don't accidentally download a malware-infected program.

There can be a variety of different reasons why your mobile device might have slow internet connection. If your business relies heavily on having a steady, fast connection to the internet, consider reaching out to your local team of technology experts to further diagnose the issue and get it resolved as soon as possible. For more help with your internet connection speeds get in touch with us today at www.rj2t.com.

Tech Tips of the Month:

- Holding the **Windows Key + Left Arrow** will quickly snap your current window to the left portion of your screen. Holding the **Windows Key + Right Arrow** will snap your current window to the right portion of your screen as well.
- Holding **Windows Key + T** allows you to cycle through your task bar at the bottom of the screen
- Holding **Windows Key + Ctrl + D** will open a new virtual desktop, enabling you to create a new desktop that can display different open windows and apps.
- To close your virtual desktop window, hold **Windows + Ctrl + F4**

Cloud Cost-Saving Strategies for SMBs:

Over the last few years many small- and medium- sized businesses (SMBs) have made the increasingly popular transition to the cloud. However, it is important to understand what services your business will need from the cloud as the costs associated with using this type of technology can increase over time if you're not careful. In this blog, we cover some quick tips for you to follow to enjoy all the benefits of the cloud while simultaneously saving money.

NO STANDALONES

The cloud has a variety of different forms, which includes standalone platforms with rates that increase over time. If you're looking to save money, it is a good idea to select a cloud service provider that can offer you a suite of products that will work in conjunction. This is a great option for SMBs looking to save money because it offers the ability to utilize several products that would be more expensive to purchase individually. Another benefit of choosing a cloud service provider is that you'll have a team of experts at your service that will be able to quickly and effectively solve all the issues you might be experiencing.

PARTNER WITH EXPERIENCED CLOUD PROVIDERS

It is a generally a good practice to partner with experienced cloud providers as they will have a great deal of experience that will help your business smoothly transition to and integrate cloud services. This is essential as integration mishaps can lead to major downtime and also have expensive costs.

DEFINE AND PRIORITIZE BACKUPS

Unnecessary or inefficient backups waste cloud storage space. You can review your cloud storage data by asking the following questions:

- How many versions of this data need to be stored long term? The more versions you store, the more it will cost you.
- How long do you need to have access to your data? Some data may need to be stored for a few years while other types of data might be deleted after a month.
- How quickly do you need to be able to access your data backups? If you can wait a day or two, you can choose alternative backup options that are less expensive.

REGULATE USERS

Typically, cloud service providers charge on a per user basis. If you don't get in the habit of regularly managing your users, you may find yourself paying for people who are no longer part of your business. For this reason, it is important to schedule regular audits of your users and implement a process to remove them when they leave your business. This will ensure that your list is up to date.

MONITOR PROACTIVELY

Ask your cloud provider whether they can proactively monitor your account and notify you of potential issues before these escalate into major problems. This is especially important if you have a pay-as-you-go license that charges based on resource or storage consumption.

Having a strong technology framework in place is vital for your business's success, and so is implementing processes and procedures that will help prevent your business from racking up and overly expensive monthly bill. If you are thinking about partnering with a cloud service provider or are unhappy with your current provider, get in touch with our team today by calling (847) 303-1194 or visiting www.rj2t.com today.

FREE Cybersecurity Report:

"The 7 Most Critical IT Security Protections Every Business Must Have in Place to Protect Themselves From Cybercrime, Data Breaches, and Hacker Attacks"

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

Don't think you're in danger because you're "small" and not a big target like J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber attacks occurring are aimed at small business; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

Claim Your Copy Here:
https://rj2t.com/free-cybersecurity-report/