ISSUE 59 ■ DECEMBER ■ 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

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

How Vulnerability Scans, Penetration Testing, and Zero Trust Security Will Help Protect Your Business

What Are Vulnerability Scans?

Vulnerability scans are used to test the security of your network. They can be done manually or automatically, and they're designed to find potential issues that could lead to security breaches.

There are two types of vulnerability scanning methods: active and passive. Active scanning involves sending probes or requests into a network in order to detect vulnerabilities. Passive scanning involves analyzing traffic on a network without sending any requests or probes, which can then be used as an indicator of weakness in the system's security. Most organizations today use both active and passive scanning methods because they each have their strengths and weaknesses: active scanning will find more problems but requires more effort on your part (and likely less accuracy), whereas passive methods can only detect issues if someone actively tries to exploit them but don't require any additional steps from you (and thus tend toward higher levels of accuracy).

What is Penetration Testing?

Penetration testing is a method of evaluating the security of a system by simulating a real-world attack on it.

Penetration tests are typically used to test the security of an information system (such as a network), but they can also be performed against physical or logical systems such as servers, routers, switches, and databases. No network is completely secure from attack; however, penetration testing is an important part of network security. A successful pen test will effectively find the weaknesses in your network and identify issues that could put your systems at risk. Penetration tests are often conducted before deployment so that any problems can be identified and fixed before users start using the system.

Why Are Penetration Tests and Vulnerability Scans Important?

Penetration tests and vulnerability scans are essential tools in maintaining the security of your network. They help you to find holes in the defenses that may allow an attacker to gain access to sensitive data or disrupt operations.

Vulnerability scans are automated processes that look for known vulnerabilities in specific systems, software, networks, and applications. Penetration tests go a step further by using actual tools used by hackers (such as malware and phishing attacks) to attempt to break into your system from outside. This allows you to see how well-protected your systems are against real-world threats rather than theoretical ones identified by vulnerability scans alone. Both types of tests are essential to maintaining a secure network.

Why is Network Testing Important?

Network testing helps you understand the vulnerability of your network, the quality of service (QoS) offered by your network speed...

Continued on page 2.

CONTINUED...

with which is processes data. This is important because:

- The more efficiently a business can process data, the better its customer service will be. If a company has slow internet speeds or unreliable servers, it may not be able to provide high-quality customer service.
- It also helps businesses identify potential threats before they become problems; this could include anything from malware attacks to brute force attacks on their firewalls.
- By knowing where there are weaknesses in their networks and how many resources, they need to properly secure them, businesses can make informed decisions about how much money they should spend on security solutions such as firewall updates or hiring IT specialists who specialize in information security management (ISM).

What is Zero Trust Security:

Zero trust security is an approach to cybersecurity that assumes unauthorized users are already present within a network. To limit their access to critical resources, it requires identity verification at every step of an employee's journey.

Examples of zero trust include (but are not limited to):

- Identity-based access control systems that use virtual tokens to authenticate users before granting them access to sensitive data or systems.
- Device identity verification using digital certificates and fingerprint readers, which requires employees to prove they possess physical devices owned by the company.

Cybercriminals have become smarter, more sophisticated, and bolder about stealing information

They're targeting individuals and companies, government agencies, healthcare providers and more. Cybercriminals are becoming better at hiding their tracks by encrypting their malware through a series of algorithms that makes it difficult for security teams to detect them. This makes it harder for organizations to stop an attack before the damage is done or limit the amount of stolen data that's leaked online. Zero Trust Security helps you prevent breaches by establishing commensurate trust levels at every stage in your network—from the endpoint through application gateways to cloud environments—to ensure compliance with regulations such as GDPR while preventing unauthorized access across all devices without slowing down productivity or performance of employees.

A simple way to think about zero trust security is "never trust, always verify."

Instead of assuming that unauthorized users aren't present within your network and making sure only authorized users are able to access resources, zero trust security assumes that unauthorized users are already present within the network.

As such, it is a proactive approach that focuses on continuous identification and access management as opposed to just providing basic perimeter security for physical or logical boundaries like firewalls and VPNs.

RJ2 SPOTLIGHT

Jeff Dann:
President

Jeff was the founding partner of RJ2 Technologies in 1998. For over 15 years, Jeff served as the President and CEO of RJ2 Technologies providing a full complement of valued technology solutions targeted towards small and mid-market customers. Jeff is fully committed to helping customers utilize technology in a manner that improves their business efficiency, deliver timely Information and allows the primary focus to be on operating and growing their business.

Prior to RJ2 Technologies, Jeff was the President and Chief Operating Officer of Pollak and Skan, Inc. overseeing twelve offices across the United States and employing over 800 employees who provided IT and technical consulting services to a variety of industry customers. Jeff was also the manager of Administration and Human Resources for an international oil and gas engineering company specializing in the design and build of oil and gas production facilities on and offshore.

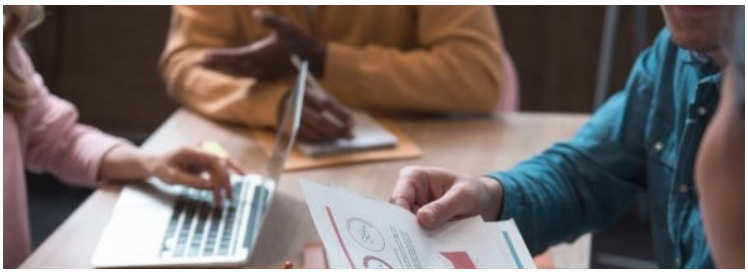
Jeff Is currently a standing member of the Board of Directors for the Better Business Bureau in Chicago. Prior to that he served multiple terms as a member of the Board of Directors for the National Technical Services Association {NTSA), Executive Board Member and President and Director of the Midwest Chapter of the NTSA.

Where is your favorite place in the world?
- I would like to go to Greece and Croatia, but of the places I have been, my favorite is Montego Bay Jamaica

What do you like to do when you are not working?
- I like watching high school sports - mostly basketball and football

If you could meet anyone in the world, dead or alive, who would it be and why?
- First would be my father who passed away too soon and would love to bring him up to date with my life experience and get some input. But from a famous perspective I would like to meet Abraham Lincoln.

How to Keep Your Business Running During a Crisis



No company is safe from disaster. For example, a ransomware attack, a fire, or an unplanned power outage can cause your small- or medium-sized business (SMB) to go offline and lose revenue. In order to protect your company from these unexpected events, it's important to have a business continuity plan (BCP) in place. This blog post will discuss what a BCP is and how you can create one for your SMB.

What is a Business Continuity Plan?

A business continuity plan, or BCP, is a document that provides detailed instructions on how to respond in the event of unexpected disruptions to normal operations. These operational disruptions can include anything from natural disasters like earthquakes and floods, to human-caused events like reputation crises and security breaches.

A comprehensive BCP will address all aspects of a business, including IT, communications, facilities, and more, enabling the company to continue providing quality products or services to its customers, even in the face of difficult circumstances.

Potential Risks to Business Continuity

SMBs face a variety of threats that could potentially disrupt operations and cause significant losses. These include:

- Natural catastrophes – storms, floods, wildfires, and earthquakes
- Man-made disasters – intentional sabotage, human negligence, and cyberattacks
- Device and utility failures – power outages, internet disruptions, and communication service issues

Creating an Effective BCP

A good BCP should not only be comprehensive, but it should also account for every possible emergency scenario your company could face. To ensure your plan is effective and covers all the bases, follow these steps:

- **Assess the risks**

Identify the hazards or potential threats that could affect your operations. Consider the likelihood that these threats could lead to actual harm, and assess any potential consequences. This will help you determine the level of risk associated with each hazard and prioritize when deciding on ways to mitigate those risks. Make sure to collaborate with all departments within your company to get a well-rounded view of the risks.

- **Conduct a business impact analysis (BIA)**

A BIA involves determining the critical functions and processes that are necessary to keep your business running smoothly. By analyzing which aspects of your operations are most important, you'll be able to make informed decisions about how to best protect those functions in the event of a disaster.

- **Determine your recovery options**

Ascertain what it would take to get your critical functions and processes up and running again after an unexpected event. This might include restoring data from backups, implementing workarounds for damaged equipment, or allowing employees to work from home. These recovery options should be feasible and achievable, so that your business can quickly resume normal operations.

- **Outline the plan**

With all of the information gathered in the previous steps, you can now start putting together your BCP. Document the steps that need to be taken in the event of a disaster, and assign specific roles and responsibilities to employees. Be sure to include contact information for key personnel, as well as any vendors or partners that might be needed to assist with recovery efforts. Keep a copy of the plan in a safe location, and make sure that all employees are aware of its existence and know how to access it.

- **Test, train, repeat**

It's not enough to just have a BCP — you need to test it frequently too. By doing so, you and your team can identify any weaknesses or gaps in the plan, and make necessary adjustments. This will ensure that your plan will work when you need it most. Additionally, you should regularly train your employees on the contents of the BCP so that everyone is aware of their responsibilities and knows how to execute the plan successfully.

If your business doesn't have a BCP, now is the time to start thinking about creating one. Our team of experts can help you develop an effective plan that will ensure your business can quickly recover from a major incident. Give us a call today.

Tech Tips of the Month

1. **Stay on top of updates and patches**
2. **Keep your hardware up to date**
3. **Make sure your data is being backed up daily and in multiple locations**
4. **Train employees to be able to identify known phishing tactics**
5. **Regularly change and update your passwords**
6. **Implement multi-factor authentication**

Making Purchases Online? Here are 4 Things You (And Your Employees) Need to Do to Keep From Becoming a Prime Target for Cybercriminals

ROI Revolution estimates that e-commerce sales will eclipse $236 billion this holiday season. While that's the most popular time for consumers to purchase online, in 2021 over $2 billion a day was made in online purchases.

Chances are you and your employees make purchases weekly personally and for your business.

And…chances are that cybercriminals are doing their best to capitalize on this to steal credit card numbers, logins and passwords and even you and your customers' banking information.

If they don't follow these four practices to stay safer (notice I didn't say safe) buying online, they could be exposing themselves and your business to identity theft, fraud, and more.

1. Don't reuse passwords from site to site. If you use the same password for multiple sites, when one company's records get breached (which happens every day) a criminal now has access to multiple accounts. So make sure you use different passwords for different sites. This does make things slightly more complicated for you, but it also makes it infinitely harder for cybercriminals.
2. Check the URL in the address bar. One indication that a website is secure is that it either has a small lock symbol to the far left of the URL or "https" in the URL. If you see a lock that's unlocked or just an "http," the site is not secure – do NOT provide any credit card information or bank account details.
3. Don't use a debit card to pay – only use a credit card. This way, if someone is able to access your account, you won't lose what's currently in your bank account. And most major credit cards have a $50 or less liability policy if unauthorized charges are made. So it's important to watch those statements. If you do feel you're the victim of fraud, make sure to contact your credit card company immediately.
4. Be wary of any texts or e-mails about package deliveries. Even if you have something you're tracking, go back to the site you originally purchased from to check notifications that way. Any links from an unknown sender could infect the device you're on, which could expose you to viruses and malicious software.
5. While there are plenty of cybercriminals happy to scam consumers, who they really want to go after are businesses because they have much deeper pockets and there are multiple ways they can cause havoc.

3 Things All Remote Employees Must Do To Prevent Your Company From Being Hacked

The last few years have seen countless companies going to a hybrid work model. According to a survey by Envoy over 77% of businesses have some full or part-time remote employees.

While this change comes with many benefits, as a business owner, there are three big things you need to make sure your employees are doing to keep your company's data secure, avoid online scams and prevent being a victim of a cyber attack.

Cyber criminals know that many of the security measures businesses have in place in their office instantly evaporate when employees work from home. Things like firewalls, secure Wi-Fi, and restricted physical access to a computer all disappear for remote workers.

According to the global security group the Institute for Security and Technology, businesses saw a 311% increase in Ransomware attacks in 2020 due to cyber criminals trying to exploit these trends. This has only increased as hybrid models have become more and more commonplace and look as though they are here to stay.

But it doesn't have to be all doom and gloom. Because these new models offer many benefits, it's just important as a business owner to know what you need in place to keep from turning a positive into a giant catastrophe through no fault of your own.

Here are three critical things you must do if you're allowing employees to work remotely:

- Always On VPN for computer, tablets and mobile devices to ensure that no matter what device employees use, or where they use it, you and your data are protected.
- Use Multi-Factor Authentication (MFA). This is where you get a text, call or need to use an authentication app to log in to programs when your account is being used.
- Set your computer screen to lock automatically. This is a simple measure that automatically logs out and locks your computer so someone can't just jump on and access your files and programs.
- Most small businesses aren't doing these three basic things to keep your data and company from becoming a victim of cyber crime. They are easy to get in place and free or inexpensive.

Want to know if your employees are putting your company at risk?

If appropriate, we can conduct a simple security assessment for free to know for sure if your network and data is safe. To get in touch about making sure all hybrid employees have all the tools