MAY 2023

CTTS TECH TALK

YOUR TECHNOLOGY PARTNER

PROTECT YOUR BUSINESS: CYBERSECURITY MEASURES YOU CAN'T IGNORE

Protecting your business against cyber threats is crucial in today's digital landscape. No matter the size or industry, every company is vulnerable to cyberattacks. Therefore, it's essential to take proactive measures to safeguard your organization's sensitive data and assets.

One cybersecurity approach that can help businesses is the zero-trust framework. This model assumes that every aspect of your system, including human, machine, or application, poses a risk to your network. As a result, verification, and authentication are necessary at every point of access to prevent hackers from infiltrating your data through compromised accounts or devices. To begin your zero-trust journey, read on.

CONTINUED TO PAGE 2

WHAT'S INSIDE THIS ISSUE:

Central Texas
Technology Solutions

TECH NOTES FROM CTTS CEO, JOSH WILMOTH

As we move into May here in Central Texas, it’s a time of change and growth. The weather is warming up, and businesses are looking to grow and improve. However, one area that cannot be overlooked is cybersecurity. With cyberattacks becoming more frequent and sophisticated, it's crucial to implement robust cybersecurity measures to safeguard your organization's sensitive data and assets.

One strategy that can help your organization minimize the damage caused by cyberattacks is implementing a Zero Trust framework. Unlike traditional security models that rely on perimeter-based security, Zero Trust assumes that every device, user, and application is a potential threat and requires verification before granting access to any resources. In other words, Zero Trust cybersecurity involves a "never trust, always verify" approach to securing your digital assets.

A recent study found that 76% of organizations reported being a victim of a cyberattack in the last 12 months. Furthermore, the average cost of a data breach is $3.86 million, with an average of 280 days to identify and contain the breach.

These statistics highlight the importance of implementing a Zero Trust framework in your organization.

At CTTS, we understand the need for robust cybersecurity measures to safeguard your business's sensitive data and assets. Our team of experts can help you implement a Zero Trust framework that ensures your network is secure, your data is protected, and your business is safe from cyber threats.

The Zero Trust approach may seem daunting at first, but it involves a simple three-step process: continuous verification, access limitation, and breach assumption. By following these steps, your organization can protect itself from cyber threats and keep its sensitive information safe.

Continuous verification involves constantly verifying the identity of users and devices accessing your network, regardless of their location or device type. Access limitation involves restricting access to sensitive data and resources to only authorized users and devices. Finally, breach assumption involves assuming that a breach has already occurred and proactively taking steps to contain and mitigate the damage caused by the breach. Implementing a Zero Trust framework requires a strategic approach, and it's important to work with an experienced IT service provider who can help you find and implement solutions that fit your unique needs. At CTTS, we take a holistic approach to cybersecurity, ensuring that every aspect of your system is protected from potential threats.

Implementing a Zero Trust framework is an essential step in safeguarding your organization's sensitive data and assets. With the increasing frequency and sophistication of cyberattacks, it's crucial to take proactive measures to protect your business. Our team of experts can help you implement a Zero Trust framework that ensures your network is secure, your data is protected, and your business is safe from cyber threats.

Don't wait until it's too late – take action today and protect your business from cyber threats. Contact us today to learn more about how we can help you implement a Zero Trust framework and safeguard your business from potential cyber threats.

THE TRUTH ABOUT ZERO-TRUST CYBERSECURITY

Despite its effectiveness, zero trust has been plagued by misunderstandings and misinformation. Therefore, it's crucial to debunk the top zero-trust myths to ensure businesses can implement this security model effectively.

Myth #1: Installing just one zero-trust product will fully secure your business.

Fact: Implementing zero trust requires a strategic approach. While there are tools to assist, only some products can do it alone. Therefore, working with an experienced IT security provider is the best way to find and implement solutions that fit your unique needs.

Myth #2: Zero trust is complicated to implement.

Fact: Implementing a zero-trust security framework can be daunting for businesses with limited knowledge or resources. Therefore, it is crucial to partner with a trusted IT service provider who can help you understand your business's risk profile and develop a practical road map to implement a comprehensive and effective zero-trust security strategy.

Myth #3: Zero Trust hinders employees from being productive and diminishes morale.

Contrary to popular belief, implementing a zero-trust model does not hinder employees' productivity or dampen their morale. It promotes increased collaboration and efficiency.

Our IT service provider can suggest user-friendly policies and easy-to-use solutions that balance security with convenience, allowing your employees to work seamlessly and harmoniously.

Myth #4: Zero Trust is too expensive.

Fact: Though implementing a zero-trust model may require additional resources, partnering with an IT service provider can help increase efficiency and control costs. The cost of not implementing it can be way higher in case of a significant cybersecurity breach.

In conclusion, zero-trust cybersecurity is essential in protecting businesses from cyber threats. It assumes every aspect of your system poses a risk to your network and requires verification and authentication at every point of access. Implementing zero trust may seem challenging, but working with an experienced IT security provider can simplify the process and ensure that you find solutions that fit your unique needs. Protect your business against cyberattacks and ensure continuity during a breach.

Secure your business's future now with zero-trust security. Take the first step towards a more fortified business today!

WHY ZERO-TRUST CYBERSECURITY IS IMPORTANT FOR BUSINESSES

In today's digital world, cybersecurity is more important than ever. With businesses relying more and more on technology and digital tools, they become more vulnerable to cyber threats. Small and medium-sized businesses (SMBs) are particularly at risk since they may not have the resources to implement comprehensive cybersecurity measures. One strategy that can help SMBs protect their digital assets is Zero Trust cybersecurity.

Zero Trust is a cybersecurity approach that assumes that every device, user, and application is a potential threat and requires verification before granting access to any resources. In a Zero Trust model, all devices and users must be authenticated and authorized before access to sensitive data or resources. This approach is essential for SMBs, which may need more resources to implement comprehensive cybersecurity measures. Zero Trust can help SMBs protect their digital assets without breaking the bank.

There are several reasons why Zero Trust is essential for SMBs:

Protecting sensitive data: SMBs often handle sensitive customer data such as financial information, addresses, and personal data. A Zero Trust model ensures that only authorized users can access this data, protecting it from unauthorized access.

Limiting the impact of cyberattacks: In a Zero Trust model, even if a hacker gains access to one device, they still cannot access all of the resources in the network. The impact of a cyberattack can be limited, preventing it from spreading to other devices or causing extensive damage.

Securing remote work: With more employees working remotely, SMBs must ensure their digital assets are secure from outside threats. A Zero Trust model can help SMBs verify the identities of remote workers before granting access to sensitive data or resources.

Meeting compliance requirements: Many SMBs must comply with industry-specific regulations that require them to protect sensitive data. A Zero Trust model can help SMBs meet these requirements and avoid costly fines. Implementing Zero Trust cybersecurity may seem daunting for SMBs, There are several steps they can take to get started:

Identify critical assets: Determine which assets are most valuable to the business and prioritize protecting them.

Monitor network activity: Use monitoring tools to track and identify potential threats.

Continuously review and update security policies: Regularly review and update security policies to ensure they remain effective against new threats. While implementing Zero Trust may seem daunting, SMBs can take concrete steps to get started and protect their business from cyberthreats. By assuming that every device, user, and application is a potential threat, SMBs can better protect themselves from cyberattacks, limit the impact of breaches, and meet compliance requirements.
In conclusion, SMBs cannot afford to ignore cybersecurity measures. Zero-Trust cybersecurity is critical for SMBs looking to protect their digital assets. By following the steps outlined above, SMBs can begin their Zero Trust journey and improve their cybersecurity posture. Remember, it's better to be safe than sorry, so don't wait until it's too late to take action!