APRIL 2023

CTTS TECH TALK

YOUR TECHNOLOGY PARTNER

THE SECRET TO FIGHTING RANSOMWARE: BEST DEFENSE AND OFFENSE REVEALED

Ransomware has come a long way since its simplistic beginnings in the 1980s. It's now an incredibly lucrative and sophisticated cybercrime industry, with attackers encrypting devices or networks to make files unusable until victims pay a ransom. The impact of this multi-billion dollar threat is far reaching and shows no signs of slowing down anytime soon. Ransomware is a particularly insidious form of malicious software – from its humble beginnings as an easily-spread virus on floppy discs in the 80s; it's now become embedded within a cybercrime industry worth billions. This specialized malware encrypts files, making them inaccessible until victims submit financial compensation to their attackers. Cybersecurity measures have failed to crimp the growing ransomware problem as malicious actors adapt and innovate their digital extortion tactics. As long as businesses continue paying up on ransom demands, these gangs have no incentive to stop - making attacks a seemingly unstoppable menace.

CONTINUED TO PAGE 2

WHAT'S INSIDE THIS ISSUE:

Central Texas Technology Solutions

TECH NOTES FROM CTTS CEO, JOSH WILMOTH

I hope this newsletter finds you well and enjoying the beautiful weather in Central Texas. However, today we need to discuss something less pleasant than the weather. Ransomware attacks can happen to any organization, but they are devastating for small to medium-sized businesses that may not have the resources to bounce back quickly. In this newsletter, we will discuss the potential financial and reputational costs associated with a ransomware attack and the importance of taking proactive measures to prevent these incidents from occurring.

Let's begin by discussing the financial costs of a ransomware attack. The 2021 Unit 42 Ransomware Threat Report by Palo Alto Networks states that the average ransomware payment increased by 82% from 2019 to 2020, with the average payment being $312,493. Moreover, the total cost of a ransomware attack, including downtime, lost productivity, and IT expenses can reach up to $1.85 million for small and medium-sized businesses. A cyber attack includes costs associated with ransom payments, lost revenue due to downtime, and recovery efforts. Additionally, there may be legal fees, public relations expenses, and potential lawsuits that can add to the financial burden. These costs can be catastrophic for small businesses and potentially lead to closure.

The costs of a ransomware attack go beyond just financial implications. The reputational damage that can occur can be even more devastating. When a business cannot operate due to a ransomware attack, customers may lose trust in the organization and take their business elsewhere. Worse still, the organization's name may become synonymous with a ransomware attack, causing long-term damage to the brand. This damage can be difficult, if not impossible, to overcome.

So, what can businesses do to prevent these types of attacks from occurring in the first place? The answer is straightforward: take proactive measures to protect your organization. Cybersecurity preparations include:

• Implementing robust security protocols.

• Training employees to identify and prevent attacks.

• Conducting regular security audits to identify vulnerabilities.

In addition, organizations should plan how to respond during an attack. This plan should include steps for isolating the affected systems, contacting law enforcement, and notifying customers and stakeholders.

At CTTS, we understand the importance of preventing ransomware attacks and are committed to helping our clients do just that. We offer various services, including security assessments, employee training, and security protocol implementation, to help businesses stay protected. Our team of experts is available 24/7 to provide support and assistance in the event of an attack, minimizing the potential damage to your organization.

The costs of a ransomware attack can be devastating for any organization, minimal to medium-sized businesses. While prevention may require time and resources, protecting your organization from potential financial and reputational damage is essential. By implementing robust security protocols, training employees, and having a plan, you can minimize the risk of a ransomware attack and ensure your business continues to thrive. If you have any questions about how CTTS can help protect your organization, please don't hesitate to reach out. We're here to help!

FROM PAGE 1

When it comes to ransomware, proactive protection strategies are essential. With the proper preparations and knowledge of best practices, you can rest easy knowing your business is in good hands! In this blog, we'll dive into how you can start safeguarding against an attack now so that any potential incidents will be minimized down the line.

Businesses, organizations, and individuals are responsible for staying informed of the latest cyber threats to help protect against ransomware attacks, the Cybersecurity and Infrastructure Security Agency (CISA) advises taking proactive steps such as patching systems regularly and developing disaster recovery plans in case an attack should occur. Employing **the best practices** for cyber security is essential to keeping data safe from malicious actors.

1. Stay current with the latest software updates and patches to ensure maximum system security. Keeping all components up to-date will help protect you against potential cyber threats!

You can help ensure the most robust security coverage by staying up-to-date with your systems.

CONTINUED TO PAGE 3

THE BEST DEFENSE TO RANSOMWARE IS A GOOD OFFENSE

2. Stay safe online, avoid taking risks, and never click on unknown or suspicious content.
Unsolicited emails can contain malicious links and attachments that could compromise your security, so always be wary when engaging with unexpected electronic mail. Cybercriminals are becoming more sophisticated with their tactics, and phishing emails remain a significant threat to many organizations. Employees must be extra vigilant when verifying both the sender of an email and its content before clicking on any links or downloading attachments. Remember - if you receive something that looks suspicious, delete it right away and alert your team!

3. Be aware; ensure your data is safely stored by backing up frequently and keeping it offline! Protect yourself, and stay ahead of the game.
Don't be caught off guard; ensure your data is safely stored by backing up frequently and keeping it offline! Protect yourself, and stay ahead of the game.

4. To ensure you can safely enjoy all the fantastic benefits of our connected world, adopt habits prioritizing online security.
Keeping your personal and financial information safe is essential for a worry-free internet experience.

Safe practices when using devices that connect to the internet include:
• Avoid using public Wi-Fi networks if you can.
• Do not download files from untrusted sources.
• Ensure your firewall is turned on.
To protect your device, stay one step ahead of cyber criminals by constantly installing the latest antivirus software and using a secure web browser. This practice will help safeguard against any unexpected threats to your system. To help keep your network and data safe from ransomware, you can implement several vital safeguards.

PHISHING SCAMS
Combat phishing scams and bolster email security with robust protocols and tools. Email filters serve as a critical line of defense, helping to protect your inbox from malicious emails before they can cause any damage.

SECURITY TRAINING
Keeping your staff updated with security awareness training is the key to safeguarding their data and avoiding cyberattacks. It offers an effective way of equipping them with vital tools needed for identifying malicious emails, preventing easy access by hackers, and protecting themselves from costly threats.

VULNERABILITY SCANNING
Vulnerability scanning is like a preemptive strike against potential attackers, helping you identify and secure any software weaknesses before those with malicious intent can take advantage. Proactively employing routine scans will arm your networks with the necessary fortification to fend off threats.

AUTOMATED PATCH MANAGEMENT
Despite the fast-paced environment of software/systems, automated patch management is a crucial method to remain secure and up to date. Automating these processes and removing manual checks can save time while maintaining vital security for your systems.

ENDPOINT DETECTION AND RESPONSE (EDR)
Endpoint detection and response (EDR) is a critical security solution for businesses. It helps identify potential threats before they can compromise endpoints such as desktops, laptops, digital assets, or mobile devices. EDR technology provides 24/7 monitoring of activity on business networks so any malicious behavior can be quickly identified and dealt with efficiently.

YOUR BEST DEFENSE TO RANSOMWARE CONTINUED

NETWORK MONITORING

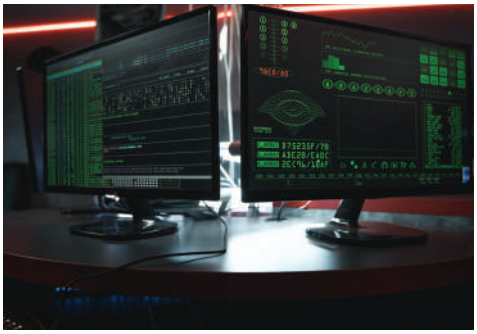
Network monitoring is a critical component of managing cyber-security. You can keep your network safe from malicious actors who would harm you through constant surveillance and quick response to potential threats. By ensuring that all activity on the system is monitored and suspicious behavior addressed immediately, companies can ensure their data remains secure at all times.

NETWORK SEGMENTATION

Network segmentation is a highly effective way to limit the devastating impact of malicious attacks on your network. By breaking up its components into specific segments, you can prevent malware spread and significantly reduce damage caused by intruders.

IDENTITY AND ACCESS MANAGEMENT

Identity and access management (IAM) is a significant tool for keeping digital environments safe, secure, and organized. It helps you monitor who has access to your applications and systems so they can do their job without unnecessary risk.



By controlling user permissions according to each person's designated role in the organization, IAM allows granular control over what users may or may not see – making sure everyone only has the right amount of information necessary for them given time.

STRONG PASSWORD POLICIES

Secure user access is crucial to protect confidential data. Establishing strong password policies and encouraging good password hygiene can help ensure users' accounts are protected with complex, regularly changed passwords. The Cybersecurity and Infrastructure Security Agency (CISA) urges an active approach to ransomware defense, including beefing up system protections with the latest security measures. They emphasize the importance of knowing your data - where it's stored and how it flows across networks - as well as regularly backing-up systems and applications critical for operations. Partner with us today to make sure you have the peace of mind that comes with having cybersecurity experts on standby, ready to help implement and maintain nothing less than best practices when it comes to safeguarding data against ransomware. So don't wait any longer; contact our team now for secure solutions tailored specifically towards protecting what matters most - your business!

COMMUNITY **UPDATES**

ST. PATRICK'S HAPPY HOUR CAME A DAY EARLY AT CTTS ON MARCH 16. THE CTTS TEAM AND THE GUESTS SHARED SOME NETWORKING FUN.
Photos by Ron Parks

With Josh Wilmoth and Sara Wilmoth are Rachel Vega (Rachel Vega Voiceover) and Jack.

Sara Wilmoth and Ken Partain welcome Jeremy Filkac (HotWorx Franchise Owner).

Ken Partain with his wife, Anne Partain.