Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
December 2020

Happy Holidays

During this holiday season, we would like to take time to reflect upon the good things we have… like our partnership with you!

Thank you for giving CTTS the opportunity to work with you and assist you with all your technology needs. It is always an honor and a valuable experience for us.

We appreciate working with you and hope that the holidays and the coming year are filled with health, happiness, and spectacular success for you, your coworkers, family, and friends.

Please note that our office will be closed on Friday, December 25th in observance of Christmas Day and again on Friday, January 1st in observance of New Year's Day. If you have a technology emergency, call us at (512) 388-5559. We're always ready to give you our world class IT support and services.

Thank you from all of us at CTTS: Michelle, Kyle, Kurt, Brandon, Dominic, Ramon, Kara, Josh, Sara, Madison, and Greg.

This monthly publication provided courtesy of CTTS, Inc.

Cybersecurity's Biggest Bully Yet

Can you imagine logging into your system to access your business data and being unable to do so? Talk about your worst nightmare coming true!

Unfortunately, an increasing number of businesses around the world are living this nightmare with countless others coming in the line of fire, including yours. Ransomware is growing rapidly and crippling businesses worldwide, making up 27 percent of all malware incidents in 2020.

If you aren't already in the know, ransomware is a type of malicious software that gains access to files or systems on your network and blocks your access to them until you pay a ransom in exchange for a decryption key.

Sounds pretty serious, but why are we calling it cybersecurity's biggest bully yet? Keep reading to know all about its history, destructive impact and dangerous growth trajectory to get your answer.

Three Decades of Bullying

In 1989, ransomware claimed its first victims when a Harvard-educated biologist and AIDS researcher, Joseph Popp, distributed 20,000 floppy disks loaded with ransomware to AIDS researchers across 90 countries.

He claimed that the disks had a program that could analyze an individual's risk of acquiring AIDS via a questionnaire. The recipients were unaware of a malware program inside the disks that activated itself and locked the computers after they were powered on for the 90th time post the malware's entry into the system.

Once active, the malware displayed a message first demanding $189, and later another $378, for a software lease from a company called PC Cyborg. This attack became notoriously known as the AIDS Trojan or the PC Cyborg virus. That year, a new and formidable cybersecurity threat was born. Ransomware's emergence, however, began nearly 20 years later when 'Police Locker' attacks burst onto

the scene. These attacks used a malware that changed a user's desktop screen to depict a false note from a law enforcement agency – the police or the FBI. Interestingly, the attacks did not use encryption and could have been resolved simply by rebooting the computer, but it was the fear tactic that compelled several victims to pay hundreds of dollars in ransom.

Modern-day ransomware developers have come a long way since Joseph Popp in the late 80s, the use of RSA encryption in the mid-2000s and attacks such as Police Locker. While early ransomware developers developed the encryption code on their own, today's attackers use existing libraries, which are harder to tackle, as well as spear phishing, among other methods.

> **"In fact, a ransomware attack can grind your business to a halt and cause severe damage on multiple fronts."**

Some of the most advanced cybercriminals are making a fortune out of selling ransomware-as-a-service, which has allowed even attackers with less technical skills to carry out massive attacks. Ransomware, such as CryptoLocker, CryptoWall, Locky and TeslaCrypt, are just some of the attacks that have emerged out of this new industry.

Cryptolocker, for instance, is a malware that encrypts files on Windows devices using advanced encryption to prevent users from accessing the files on the system. To obtain a private key to access the files again, users are warned of destruction of the data should they fail to pay the ransom

The introduction and use of cryptocurrency within the ransomware industry has also made transactions more difficult to trace than conventional ones. For example, the hackers that carried out the WannaCry ransomware attacks that wreaked havoc worldwide, demanded that the ransom be paid in Bitcoin.

Through their three-decade long existence, ransomware attacks have only gone from strength to strength. While older threats reemerging is always a possibility, newer ones such as NotPetya and MAZE are constantly looking to take advantage of lapses in the cybersecurity defenses of companies worldwide.

Besides being the reason behind 41 percent of cyber insurance claims in the first half of 2020 alone, the repercussions of a ransomware attack aren't limited to just financial loss. In fact, a ransomware attack can grind your business to a halt and cause severe damage on multiple fronts.

Your company's data is the proverbial thread that strings various facets of your business together. Should your data become inaccessible, go missing or be destroyed, the damage can be catastrophic. Don't let ransomware literally choke the life out of your business' present and future.

3 Simple Steps To Earn $250!

Do you know a business or nonprofit orgnaization in need of IT Support?

When you refer any company with 10 or more users to our office, and we have completed our initial appointment with your referral, we'll give you $250! It's a win-win!

Get started here:
http://bit.ly/CTTS-Referral

Every business found in corporate land liked Christmas a lot. But the hacker, who lived just north of corporate, did NOT!

Then he got an idea! An awful idea! "All I need is an insecure password…", the Hacker looked all around. On the Dark Web, there was plenty to be found.

Did the old Hacker stop for legality…? No! The Hacker simply said, "It's a game you see, if I don't get caught, how rich I'll be!"

So, he grabbed all the passwords from the Dark Web with glee, then he researched, and he researched every employee.

"I know just what to do!" The Hacker laughed in the air. He used social engineering to bait the business with flair. And he chuckled, and chuckled, "What a great Hacker trick! The assistant gave me full access, so this malware will stick!"

It was a quarter past downtime… All the employees came in to work, to find their whole business down because of some cyber-criminal jerk! When they tried to log in, all they could do was stare. When up on their screen was a message of Ransomware.

The documents and programs needed for operation, the files and data on every workstation!

Except for one little Datto appliance tucked way in the back, its data encrypted, unaware of any attack. Its virtual backup completed hours ago, its blue light flashing, giving off a beautiful glow.

And what happened then…? Well, in corporate land they say, that the business was back to normal before midday.

Not all stories have a happy ending. Is your business prepared for the worst?

Policy of Least Privilege: Starting from Zero Trust

Did you know that two of the most infamous data breaches on record, namely the ones at Home Depot and Target, occurred due to a compromise of their network credentials? In both the cases, hackers used privileged accounts to access critical business data and private customer records.

In IT, the principle of least privilege (PoLP) refers to the concept that any process, program or user must be provided with only the bare minimum privileges (access or permissions) needed to perform a function. So, if a user account has been created for accessing database records, should that user also have admin rights?

Managing Access Levels

In some cases, the assignment of privileges is done on role-based attributes such as the business unit, time of day, seniority and other special circumstances. Some examples of role-based privileges include:

- **Least privileged user accounts** — These are standard user accounts that operate with a limited set of privileges. Most of your users should be operating under these accounts.
- **Superuser accounts** — These are essentially admin accounts that are used by specialized IT users and often come with unlimited privileges. In addition to the read/write/execute privileges, these accounts have the permission to execute systemic changes in your IT network.
- **Guest user accounts** — These accounts are created on a situational basis and often have the least number of privileges — lower than those of the standard user accounts.

What is a "Zero-Trust Framework"?

According to PoLP, organizations should avoid blindly trusting anything within or outside their network and verifying everything before granting permissions

for access. There are certain best practices that you must follow to efficiently implement PoLP in your security policies:

1 Conduct a privilege audit for all your existing programs, processes and user accounts to make sure that they have only the bare minimum permissions required to do their jobs.

2 Start all your user accounts with privileges set to the lowest possible level. Implement least privilege as the default for all your existing as well as new user accounts, applications and systems.

3 Keep track of all the activity on your network including access requests, systems changes and individual logins. Having a comprehensive understanding of who is operating on your network is critical to maintaining control over who can access what.

4 Maintain a management platform that allows flexibility to securely elevate and downgrade privileged credentials.

5 Conduct regular audits to check if there are any old accounts, users or processes that have accumulated privileges over time and analyze whether or not the elevated privileges are still relevant.

Implement PoLP across your IT environment today to strengthen your cybersecurity posture. Don't know how? Contact us now to help you understand how you can implement and leverage the powerful capabilities of PoLP.

Get Organized And Back On Track

Top Business Apps To Get You Organized

If you're struggling to stay on top of your work tasks, there are some great apps available to help out.

• **Asana** helps your business improve communication and collaboration. You can view all tasks and projects and follow progress on a communal board so you can communicate without having to rely on e-mail.

• **Proven** helps organize your hiring process by posting listings to multiple job boards with one click. You can also review and sort applicants with ease.

• **Boxmeup** organizes and tracks your packages, containers and bulk storage items to make storing and shipping a breeze.

• **Evernote** keeps all your notes organized in one place and allows you to easily share notes and lists with co-workers.

• **Trello** tracks your team's workflow. Whenever you make a change to a project or task, the app notifies each team member involved so you don't have to.

• **KanbanFlow** helps managers visualize overall workflow. It gives overviews of work status, tracks progress and assigns tasks to team members.

Nerdwallet, Apr. 21, 2020

Top 5 Ways To Overcome Setbacks And Grow

After you encounter a setback, it can be hard to start again. But simply believing in yourself is the best way to get back on track.

1 **Recognize when failure is your fault and when it isn't.** Some setbacks are entirely out of your control. Learn to recognize the difference in your faults and what you can't control, then move forward.

2 **Learn from your mistakes and don't repeat them**. Immediately letting go of the regret of making a mistake can be hard, so instead, focus on what caused the mistake, then learn from it.

3 **Focus on your new goal.** Failure often comes from going after something we don't truly want. Discover what you really want so you understand what you need to work on.

4 **Celebrate small wins.** You don't have to wait to celebrate, even if you haven't reached your end goal. Validate yourself for completing smaller tasks, and you'll empower yourself to keep going.

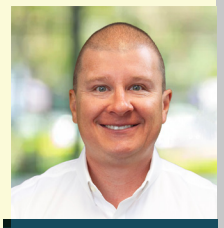
5 **Find the right mentor.** This is someone who believes in you, even when you don't believe in yourself, and who can support you in reaching your goals. Find someone with the right knowledge and experience to learn from.

Business Insider, Sept. 16, 2020

Tech Tip of the Month:

Why Your Business Needs a Data Security Policy

If you and your employees use passwords or email to access and transfer business and customer data, you are vulnerable to a cyber attack. Here are 7 ways to minimize risk and keep you, your company, and your customers safe.



By Josh Wilmoth

Read it Here: http://bit.ly/Tech-Tip-200