Monthly Newsletter

The Tech Chronicle

August 2023 | www.centrend.com | Volume 5.0

Inside this Issue

PRODUCT SPOTLIGHT

BarTender® BY SEAGULL SCIENTIFIC

Create, automate and manage labels, barcodes, RFID tags and more

It's the labeling software standard for the world's most dynamic supply chains and manufacturing operations in every industry

Tech Tip of the Month

Cyber Insurance Explained: Importance and Basic Questions in Applying

In an age where technology plays an integral role in our personal and professional lives, the importance of cyber insurance cannot be overstated. With cyber threats becoming increasingly sophisticated and prevalent, businesses of all sizes risk falling victim to costly data breaches or cyber-attacks. The financial consequences can be devastating, ranging from regulatory fines to legal fees, customer notifications, loss of intellectual property, reputational damage, and even business interruption.

>>> continued on Page 2

An In-Depth Guide to Brute Force Attack

Have you ever experienced the alarming notification that someone is attempting to access your admin account? This type of incident can be incredibly unsettling, putting sensitive data and critical systems at risk. However, it also serves as a crucial reminder of the importance of robust cybersecurity measures.

In today's digital world, the threat of cyberattacks is a constant concern for individuals and businesses alike. One tactic that hackers employ is a brute force attack

> continued on Page 4

Cyber Insurance Explained: Importance and Basic Questions in Applying (continued from page 1)

Cybersecurity insurance protects against these potential risks by covering data breach response and recovery expenses. This can include costs such as computer forensics investigations, legal fees for dispute resolutions or regulatory compliance issues, public relations activities to protect the company's reputation, credit monitoring for affected individuals, and financial compensation for third-party claims resulting from the breach.

Moreover, it is not just limited to businesses. Cyber insurance coverage can also benefit individuals who store sensitive personal information online and conduct e-commerce transactions.

Having cyber insurance demonstrates a commitment to cybersecurity best practices. Insurers often require policyholders to implement specific security measures and protocols in their coverage agreement. This incentivizes businesses to invest in robust cybersecurity measures such as firewalls, encryption software, employee training programs, and regular vulnerability assessments.

Now that you know what cyber insurance is and its importance to businesses and individuals, you might wonder what questions you will likely encounter when applying. The following is a list of common questions you may expect to find on your application.

Does your company use Multi-Factor Authentication?

Multi-factor authentication (MFA) adds extra security to prevent unauthorized users from accessing accounts. MFA is used to authenticate if the identity or credentials of users are genuine. It obliges to have another authentication process on top of the traditional username and password.

Is employee Security Training provided?

Consistent security training will help keep employees your most excellent protectors instead of your weakest link. Providing and equipping your employees with training, education, and tools will bring awareness to combat cyber-attacks.

Do You Have Regular Monitoring for Unauthorized Access?

Consistent monitoring of devices with malicious activity and real-time reports can limit the impact of cyber-attacks.

Is Endpoint Security Deployed to Every Connected Device?

Endpoint Security protects your network from an entry of risky activity or any malicious attacks. Simply put, it's your anti-virus / anti-malware software and is the final line of defense that prevents cybercriminals from stealing and altering valuable company assets.

Do You Back Up Your Data and Have a Recovery Plan?

Data backup and recovery is an integral component against data loss that can seriously impact your business or individual. This ensures that user data or information is safe from damage to any data disasters. You or whoever is responsible for your IT must check the effectiveness of your backup systems to be sure they are complete and restoreable.

Do You Limit Data Access and Systems?

Limiting data access and systems to employees can protect your company and confidential information from being accessed by any unauthorized access. Setting limitations will prevent data breaches and protect against cybercrime.

Do You Use Encryption?

Encryption helps your private, confidential, and sensitive information be hidden and inaccessible to anyone without authorized access to those company assets. Using encryption enhances security throughout your systems and data.

Do You Regularly Install Updates and Patches?

Consistently installing up-to-date updates enhances security and provides new and improved functionality which helps address issues in your network which might be a weak link for cybercriminals to get access to.

Do You Have A Disaster Recovery Plan?

Insurance providers want to ensure that you are proactively protecting your network, sensitive data, and assets and not just simply relying on the coverage they will provide. Having a Disaster Recovery Plan shows your responsibility as a business entity.

Cyber Insurance Explained: Importance and Basic Questions in Applying *(continued from page 2)*

Answering any of the cybersecurity application questions wrong can result in the denial of a claim. Imagine paying for cybersecurity insurance and, after an attack, discovering that your insurance is null and void because you said you had something in place that isn't there.

Given the ever-evolving nature of cybersecurity threats businesses face today, investing in comprehensive cyber insurance is prudent and essential for long-term success. It offers financial protection against potential losses while providing access to expert support during times of crisis.

By prioritizing cyber insurance, businesses can demonstrate their commitment to cybersecurity and safeguard their operations, reputation, and customer trust.

At Centrend, our comprehensive managed IT solutions take a preventative approach. We are one step ahead of potential threats by identifying vulnerabilities and implementing strategies to mitigate risks before somebody can exploit them. If you need help bolstering your cybersecurity or simply completing your cybersecurity application accurately, contact us for a free consultation!

An In-Depth Guide to Brute Force Attack
(continued from page 1)

wherein they attempt to gain unauthorized access by systematically trying various combinations of login credentials.

Last week, a company came to us because its website was being assaulted with a brute-force attempt to gain administrative access to the backend. We also found a sudden influx of new account registrations with email notifications of users trying to register for gated content. How could we tell? The email addresses and names looked fake, and the hosting service flagged suspicious login attempt activity. I'll talk more about how we protected this client later. First, we'll cover what exactly is a Brute Force Attack.

A Bruce Force Attack, or exhaustive search, is a type of cyberattack involving successive repetitive attempts and guesses of login info, credentials, and encryption keys. Brute force attack is considered the simplest method of hacking a site or server and contributed to an estimated 5% of confirmed data breach incidents in 2017.

Brute Force Attack comes in different types depending on the complexity of the process.

Simple Brute Force Attack: This attack typically makes a hundred guesses of passwords every second and uses automation and scripts to crack the server's password. Weak login credentials, such as those using simple password combinations, are the most common victims of this attack. Generic passwords such as '123456' or 'password' can be easily cracked by cybercriminals in just a few minutes.

Dictionary Attack: An attacker tries combining common passwords and phrases based on his assumptions. Despite being considered an outdated technique of cracking a site's password and having a low probability of succeeding, you must still implement strict and timely cybersecurity measures

Hybrid Brute Force Attacks: A combination of Simple Brute Force Attack and Dictionary Attack techniques. Hackers try successive combinations of potential passwords through letters, numbers, and even characters.

Reverse Brute Force Attacks: This attack occurs when a hacker already has your old login credentials or uses a common password such as 'Password123' and tests variations to uncover the current credentials. Reverse Brute Force Attack is one of the most successful attacks among others.

Credential Stuffing: This attack is made from stolen login combinations mainly obtained from underground dark web sites or harvested from weaker security locations. The victims of these attacks are primarily users who repeatedly recycle their login credentials on multiple sites. Hackers use the same username and password that has already been discovered to access other places the user has access to.

What motivates attackers behind any Brute Force Attack?

You should not take Brute Force Attacks lightly, as they pose serious threats to the security and integrity of your online presence. The rise in cybercrimes has made it crucial for individuals and businesses to stay vigilant and take necessary precautions.

Taking proactive steps can effectively thwart potential attackers and safeguard your valuable data from falling into the wrong hands. Here are some techniques to avoid falling prey to brute force attacks.

Use a multifactor authenticator: Set up another level of security through a multifactor authenticator. Password, fingerprint, or even a one-time security token will reduce the chances that a brute force attack is successful.

Establish a more robust password: Change your admin's login credentials following the best password practices. Use a mix of upper and lowercase letters, a combination of special characters, and even numbers. Make sure to update your password regularly – preferably every three (3) months. Never, ever reuse passwords in multiple areas.

Limit Login Attempts: Limit login attempts to resources like your WordPress Admin panel. The hacker's IP address will be blocked after several failed attempts, which breaks the script that would otherwise be capable of attempting hundreds of password combinations per second.

Using captcha: Captchas will prevent automated script bots from submitting the login form hundreds of times in rapid succession. Installing a captcha plugin and applying it to the forms on your website will also save you from spam email attacks.

In conclusion, be proactive about securing your precious resources with the abovementioned techniques. Pay attention when notified about someone trying to access your systems and take immediate action to increase protection. By staying one step ahead and prioritizing cybersecurity, we can safeguard our digital assets from potential breaches.

If you need help determining whether your systems or website is secure, contact us for a free consultation, and we can advise you about implementing any of the strategies just described.

Crypto-malware 101: Everything You Need to Know

Cybercrime has become a prevalent threat in an increasingly connected and digital world. One form of cybercrime that has gained notoriety in recent years is crypto malware. This deceptive and malicious technique has caused significant financial losses and disrupted countless individuals and organizations worldwide.

As the value of cryptocurrency continues to increase and its use becomes more widespread, crypto-malware attacks are becoming more and more common among cybercriminals.

But what and how does crypto-malware work?

As the value of cryptocurrency continues to increase and its use becomes more widespread, crypto-malware attacks are becoming more and more common among cybercriminals.

Unlike other malware, crypto-malware is one of the most alarming and worrying attacks you'll think of because crypto-malware can be installed through any compromised website or app without downloading anything. Once the victim visits the infected site, a code will run at the backend independently and indefinitely – this is where crypto jacking happens.

The impact of a crypto-malware attack can be devastating. It can lead to the loss or destruction of valuable data, disrupt business operations, cause financial losses, and damage an organization's reputation. It is important to understand that anyone can fall victim to such attacks – from individual users to small businesses and large enterprises.

How to stay protected from crypto malware?

There are various ways in which crypto-malware can infiltrate a system, including phishing emails, malicious websites, infected downloads, or even vulnerabilities in outdated software. Therefore, staying vigilant and practicing good cybersecurity hygiene is paramount.

Prevention is vital when dealing with crypto-malware attacks. This includes maintaining up-to-date antivirus software on all devices, regularly updating operating systems and applications with the latest patches and security updates, and exercising caution when opening emails or clicking suspicious links or attachments.

It is also crucial to regularly back up important data and store it offline to remain unaffected by any potential attacks. Being proactive in implementing security measures such as strong passwords, two-factor authentication, network segmentation, and employee education about best practices for online safety can also help mitigate the risk of falling victim to crypto-malware attacks.

1. Know your IT infrastructure - Understanding the typical performance of the devices that make up your network infrastructure (like routers, Wi-Fi hotspots, computers, and more) can help you identify potential warning signs. For example, the sign can be as subtle as your computer overheating in situations it didn't previously. It may not even feel slower, but it's working hard in the background, unknowingly doing the cybercriminals bidding.

2. Monitor your network - One way to know what's going on with your device is to monitor your network. At Centrend and WhizkidSupport, we monitor system logs for you, along with critical metrics such as CPU and disk activity and automatically take action when things are performing out of the norm. You can do this by checking your device's syslog and router logs for any unrecognized traffic or activity. Also, visit your system's task manager and view the performance stats there.

3. Do not open attachments or links from unknown sources - If you are unsure of the destination of a link or the source of an attachment, it is best not to click on it. Even if you know the sender, if the content of the message seems off, even a little bit, or you are receiving something unexpected, check with the sender before clicking. It could save your day!

4. Pay attention to the websites you visit - Always check web links, especially when they come from text messages or emails. A quick Google search can help you distinguish genuine links from fake ones. Also, if you notice that the site has a different format, contains too many typos, or contains low-resolution images (especially with logos), you should leave immediately. At Centrend and WhizKidSupport, we use webroot which includes a web scanner to warn you if you've click on a malicious link.

5. Use strong passwords - A strong password is the first line of defense against unauthorized access to your account. Pair it with two-factor authentication for an extra layer of security. The final move on password strength is to use a password manager. The password manager can generate strong passwords, securely store them, and automatically fill them in the login screen. Centrend recommends and manages LastPass for our customers for the purpose of password management.

6. Back up data regularly - To protect against data loss, such as in the event of a ransomware attack, you should keep multiple copies of important files, ideally in various locations that you control. This way, if your computer is locked by ransomware, you can give it up instead of paying. Learn more about backing up your files and encrypting them.

7. Keep your device up to date - Denying software updates increases the chances of attackers exploiting unpatched systems. Keep your devices up to date for a basic level of security.

Greg. "What is Crypto Malware? And How to Detect It?". ExpressVPN, 2 February 2023, https://www.expressvpn.com/blog/what-is-crypto-malware/

In conclusion, understanding the nature of crypto-malware attacks and taking necessary precautions is vital for individuals and organizations in safeguarding their data from potential breaches. By remaining informed about the latest trends in cyber threats and adopting robust security measures, we can protect ourselves against this ever-growing threat landscape.

Want to know more about malware and how to protect your network from such attacks? Click here to book a FREE Cybersecurity Assessment. This assessment is simple, inexpensive, and easy to do. Still, it will give you the unbiased truth about your current security and how resistant your organization is to a cyber-attack.