the NetWork

LeadingIT
Chicagoland CybersecurITy Support

August 2021

July Fourth Kaseya Ransomware Attack

& How To Keep Safe

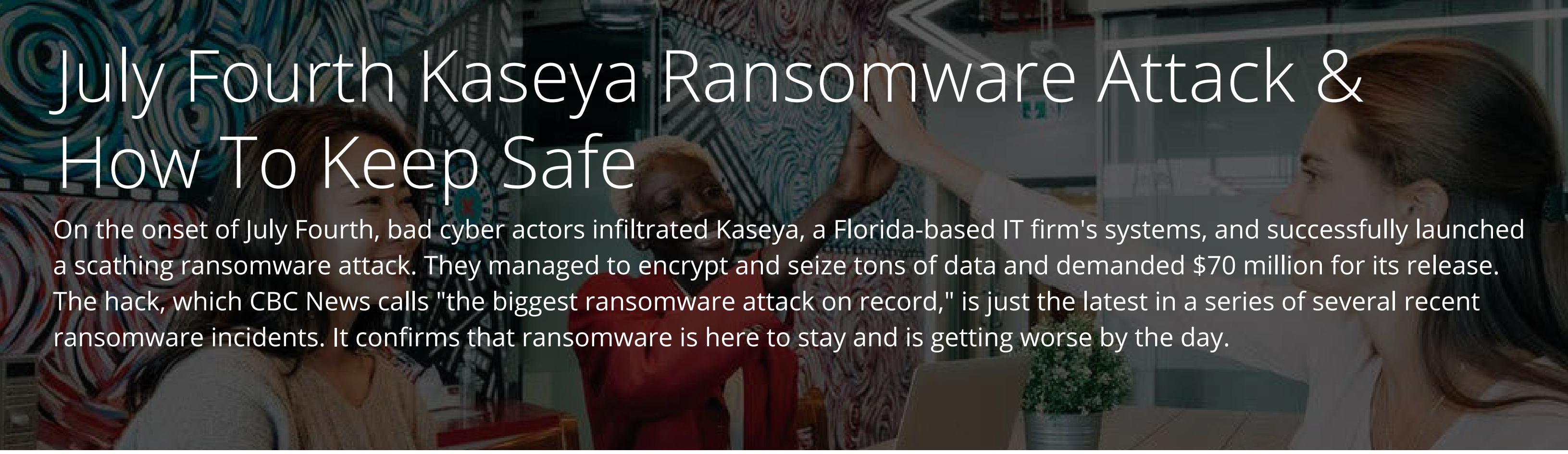
7 Cybersecurity Measures You Can Implement to Protect

Your Chicagoland Organization

Protecting Your Backups

From Next-Gen Extortion Ransomware

We Are Growing!



July Fourth Kaseya Ransomware Attack & How To Keep Safe

On the onset of July Fourth, bad cyber actors infiltrated Kaseya, a Florida-based IT firm's systems, and successfully launched a scathing ransomware attack. They managed to encrypt and seize tons of data and demanded $70 million for its release. The hack, which CBC News calls "the biggest ransomware attack on record," is just the latest in a series of several recent ransomware incidents. It confirms that ransomware is here to stay and is getting worse by the day.

Should You Be Worried About The Kaseya Ransomware Attack?
Unless you are a Kaseya client, either directly or indirectly through an MSP, there's no need for alarm. However, the attack will undoubtedly have cybersecurity experts worried. The hackers used high-level planning and sophisticated execution that bears the strains of a government-sponsored hacker group. They adopted two new tactics that bad cyber actors have never used anywhere around the world. The worst bit is that even deployed a zero-day, a software vulnerability that developers haven't noticed and therefore don't know how to fix.

How to Safeguard Your Organization Against Ransomware Attacks

1. Install automated threat detection systems

Sometimes, ransomware attackers camp in target networks for weeks, and even months, before launching an attack. With an effective threat detection system, you can pinpoint foreign patterns in your networks and thwart threats before they aggravate into serious issues.

2. Adopt multi-factor authentication

As more employees are operating remotely and carrying office gadgets home, organizations face the challenge of ensuring that these devices and logins don't land in the wrong hands. That's why you need MFA; so that even if hackers steal user credentials or gadgets, they won't be able to access your network easily. You can use MFA together with Single Sign-on to enable admins to remotely lock and wipe memories of gadgets when they get lost.

3. Install software updates in phases

As you must have noticed, hackers increasingly use software updates as backdoors to company networks. To avoid falling for this trap, only install updates to a few users in the IT department and scan them for threats before deployment to the entire organization.

4. Back up all your data

Ransomware attackers feed on the confusion and uncertainty caused by hacks to coax businesses into paying ransoms. However, with a secure and easy-to-retrieve offline backup, you can easily resume regular operations and negotiate with the hackers on your terms.

5. Train your employees on ransomware preparedness

Your networks are vulnerable if employees aren't properly trained even with the most advanced cybersecurity systems in place. Regularly train your users on how to identify threats, how to prevent attacks, and fast-response procedures. You can also occasionally launch simulated attacks to gauge their preparedness levels.

7 Cybersecurity Measures You Can Implement to Protect Your Chicagoland Organization

Businesses in all industries have become targets for cybercriminals looking to access confidential corporate and client data. Contrary to popular opinion, large corporations aren't the only businesses that have fallen victim to cyberattacks. Small-to-medium-sized businesses have also experienced their share of cyberattacks and are increasingly becoming targets for cybercriminals. According to the Verizon Business 2020 Data Breach Investigations Report (2020 DBIR), 72% of cybercrime victims were large businesses, while 28% were small businesses.

How Lucrative Is Cybercrime?

According to the Verizon 2020 report, 86% of investigated cybercrime incidences are financially driven. The most recent publicized financially-driven cyberattack occurred on May 7, 2021, with the oil pipeline company Colonial Pipeline falling victim. The company had to pay 75 Bitcoins, an equivalent of $4.4 billion, to restore their systems. The Verizon report also states that stolen account credentials accounted for 37% of cyberattacks, social engineering schemes account for 25%, human error accounts for 22%, misuse by unauthorized users accounts for 8%, and physical actions account for 4% of cyberattacks. Malware is the most common type of cyberattack. The AV-TEST Institute reported that it registers about 350,000 new malicious programs daily. If you're running an organization, it's crucial to ensure that cybersecurity is a top priority. You need to implement appropriate cybersecurity measures to protect valuable corporate and client data and mitigate cybersecurity risks.

How Can You Protect Your Organization from Cybercrime

1 Perform a Cybersecurity Assessment

Routine cybersecurity assessments should be a central element in your cybersecurity policy since they give you insights on what security controls are working effectively, which ones you need to reinforce, and what security vulnerabilities you need to patch.

2 Develop a Cybersecurity Response Plan

A thorough and well-thought-out response plan will describe all the steps to take when you experience an attack. As a result, you'll be able to take action quickly, notify equipped and trained cybercrime professionals, communicate to the relevant parties, and take control of the situation before it escalates.

3 Cybersecurity Training for Your Employees

Since cyberattacks and technology are continually evolving, your employees' cybersecurity knowledge should evolve as well. You should also conduct cybersecurity training regularly to ensure new employees don't create new security vulnerabilities.

4 Install Security Software

Security software such as antivirus, anti-malware, and anti-spyware programs will help to detect and remove malicious programs and files in your systems.

5 Keep Your Operating System and All Your Software Updated

Outdated software and programs can make your organization susceptible to multiple cybersecurity threats. New software updates often fix security flaws, remove bugs, and have new security features to ensure that your system is protected from attacks.

6 Implement Strong User Authentication

Use complex passwords that include numbers, letters, special characters, and symbols to lock out intruders. You can also implement other access and authorization methods such as biometric authentication or multi-factor authentication to lock out external parties from your systems.

7 Implement a Firewall

A firewall can be software, hardware, or a combined system that prevents unauthorized access to your network. It functions by isolating your organization's internal networks from external networks. Firewalls monitor outgoing and incoming network traffic from external sources and create a barrier blocking any malicious traffic.

Protecting Your Backups From Next-Gen Extortion Ransomware

1. Have a Data Backup Plan

Many cybersecurity professionals recommend the 3-2-1 data backup plan as an effective way to keep multiple copies of your data. This backup plan can also include these tips:

- Three copies of your data
- Two backup copies on different storage media or devices
- One backup copy offsite

2. Keep an Offline Backup

Having an offline backup copy is crucial for your cybersecurity since attackers cannot access backups that are disconnected from your system. You can store your backup copies on external hard drives, CDs, or tapes.

3. Isolate Your Backups

By using different login credentials for your backups, you make this process more difficult for the attackers.

4. Back up Regularly

Your backups should reflect the most relevant and recent information your business needs to operate. You will set up a backup frequency depending on the needs of your business.

5. Test Your Backups

You should regularly test your backups to determine the recovery time and whether you'll be able to recover all your data.

Businesses have responded to ransomware attacks by ensuring that they are backing up their data. Data backups have been a great defense against cyber threats and an effective way for organizations to recover from ransomware attacks for many years. However, ransomware writers have realized this and are modifying their threats and creating more sophisticated threats to track down and erase your data backups.

Welcome to the LeadingIT team!

We are growing and are excited to introduce the newest additions to the LeadingIT staff. Carlos and Vincent join us as Level 1 techs and Eric joins us as our new Inside Sales Pro.

WE ARE CELEBRATING!

Anniversaries	Birthdays
Jeremiah Bird - 8/24/2020	Stephen Taylor - August 11th Justin Gackowski - August 14th Jose Ledesma - August 26th Collin Saunders - August 26th Mallory Hale - August 30th

Read Our Blog For More
https://www.goleadingit.com/blog

LeadingIT