CTSI
Serving Colorado's Counties

Technical Update

Volume 24 Number 52 October 20, 2020

Protect your Organization from Ransomware

The news is full of stories about companies and organizations being targeted by ransomware, a type of malware. Ransomware infects a victim's computer, device, or network then locks or encrypts data. The cybercriminals behind the ransomware then demand the victim pay, usually within a certain time frame, or risk permanently losing their data or having it made public. According to Emsisoft's Q1 and Q2 2020, last year, ransomware attacks against U.S. government, healthcare, and educational organizations cost those organizations $7.5 billion. (For more information on ransomware, read Technical Update no. 40 - Ransomware.)

Understanding Ransomware

Ransomware falls into two general categories: crypto and locker. Crypto ransomware is a malware that encrypts valuable data on a network or device so that the user cannot access the data. Locker ransomware does not encrypt data; instead, it locks the user out of the computer or device entirely. There are numerous types of ransomware. Two common ones are listed below:

Cerber – A kind of crypto-ransomware, Cerber targets cloud-based Office 365 users and is spread via a phishing campaign. (For more information on phishing, read Technical Update no. 74 – Phishing: What you Need to Know.) Cerber comes in 12 different languages and has been deployed by large cybercrime networks across the globe. So far, it has impacted millions of people.

CryLocker – As the name suggests, CryLocker is locker ransomware. It crawls through a victim's computer and finds personal information such as their name, birthday, location, Facebook profile, IP address, etc. to generate a ransom note demanding payment within 24 hours.

Protecting your Organization

Ransomware is big business for cybercriminals and isn't going away anytime soon; however, there are steps you can take to protect your organization.

1. Backup your data – Critical network and system data should be backed up regularly. If a ransomware attack occurs, the data can be restored; however, some ransomware can infect backup servers, so backup drives should be physically disconnected from your system when not in use.
2. Use multiple layers of cybersecurity – Do not rely on only one form of cybersecurity. Use antivirus and antimalware software along with firewalls and web filtering to block attacks. Cybercriminals are more likely to target organizations with weak security.
3. Keep software and systems up-to-date – Apply vendor-provided updates to your apps, operations systems, web browsers, and plugins as soon as they are made available. Updates often patch security vulnerabilities that cybercriminals can exploit.
4. Limit access to your network – If your network has multiple users, limit global/administrative privileges to a system administrator. Most ransomware is limited to the access level of the person whose device is infected, so if a user cannot change files on the server or change security settings, the malware is more likely to stay contained on their machine.
5. Teach employees how to identify fake links and emails – Most ransomware is spread when a person clicks on an email link as part of a phishing scam. Educate employees on how to spot fake emails and links. Remember, many phishing emails are designed to mimic emails from well-known companies, so people should always check the URL of email links and be suspicious of emails with language errors or from companies they haven't done business with before.

What This Means for Counties

As many people continue to work from home, it is vital to set and maintain good network security practices. Like burglars, cybercriminals tend to go after easy targets. Implement strong network security practices to make your organization an unattractive target. For more information on ransomware, contact CTSI at (303) 861 0507.