TECHNICAL UPDATE

CTSI
Serving Colorado's Counties

Volume 25 Number 21 May 25, 2021

Ransomware: A Continuing Threat

Earlier this month, a ransomware attack shut down the Colonial Pipeline, which transports 45% of the fuel consumed on the East Coast, leading to panic buying and gas shortages. The CEO of Colonial Pipeline Co. paid a 4.4-million-dollar bitcoin ransom to a Russia-based cybercriminal gain know as Darkside to regain control of the pipeline system. Every year ransomware infects thousands of computers and networks across the United States, including a statewide attack on the Colorado Department of Transportation (CDOT) in 2018 that cost $1.5 million to undo. Ransomware is a virus or type of malware that locks users out of their computers or data unless they pay a "ransom."

TEMPTING TARGETS

Ransomware attacks, especially on government systems, have become a large-scale criminal industry. In a three-year period, the two men indicted in the CDOT attack targeted more than 200 schools, government agencies, hospitals, and businesses across the U.S. and Canada. While CDOT did not pay the ransom, other victims paid more than $6 million. Ransomware attacks can be devastating and costly, often requiring the services of a data recovery specialist. Even if victims pay the ransom, something the FBI advises against, there is no guarantee that access to data or systems will be returned.

PHISHING

Most ransomware attacks happen through phishing—emails that appear to be from a trusted source designed to trick people into clicking on a link or opening an attachment. For more information about phishing, refer to Technical Update vol. 23 no. 17 Phishing: What you Need to Know.

TAKING PRECAUTIONS

The Cybersecurity and Infrastructure Security Agency (CISA), a branch of the U.S. Department of Homeland Security, recommends that organizations take the following precautions:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the targets of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Backup data regularly. Keep it on a separate device and store it offline.
- Follow safe practices (i.e., use strong passwords and two-factor authentication, be suspicious of unexpected emails, etc.) when browsing the Internet.
- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

WHAT THIS MEANS FOR COUNTIES

Ransomware attacks are a rising threat for local governments. While CAPP does provide network liability coverage of varying limits for network extortion and other network security incidents, taking steps to prevent ransomware attacks is the best defense. The CAPP Network Liability policy is available at ctsi.org. For more information, contact CTSI at (303) 861 0507.