www.hometownconnections.com
12081 W. Alameda Parkway, # 464
Lakewood, CO 80228
P — 970 682 4217

Hometown Connections

May 17, 2021

Gas Pipeline Ransomware Attack Is Wake Up Call For Public Power

Front page headlines, consumer panic, political fallout, and a $5 million ransom paid. The attack on the largest fuel pipeline in the U.S. is focusing attention on the vulnerability of our energy infrastructure like never before. With people lining up at gas stations when facing only a few days of a shortage, imagine the reaction to the local electric grid being down for who knows how long. It's beyond time for all municipalities and their utility departments to build out their cyber defenses.

The pace and scope of cyber attacks are expanding exponentially. Acting now will protect your utility and community from the grievous financial and reputational harm of a ransomware attack.

The Cybersecurity & Infrastructure Security Agency (CISA) recognizes 16 critical infrastructure sectors *"whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."*

However, it's not just the classification of these critical infrastructure sectors but the picture of how they depend on each other (see **Figure 1**) that tells the real story. Should any of these sectors suffer a major event, it could, very realistically, cascade throughout the rest. For instance, natural gas generation facilities require pipelines to deliver fuel for operations, and all sectors including national defense require electricity to function.

Figure 1: U.S. Critical Infrastructure Sectors

Figure 2 Colonial Pipeline System

On Friday, May 7, 2021, we witnessed the largest U.S. fuel pipeline (see **Figure 2**) shut down after a cybersecurity attack. While we don't yet know the full cascading effects of this event, we do know that the responsible attacker was the DarkSide group.

Looking back over the previous five years, ransomware was originally used primarily as an extortion tool for criminals to obtain a ransom in exchange for giving an individual or company access back to their encrypted data (or not). However, whether intended or unintended, ransomware has morphed into a tool that can be used to cripple critical infrastructure operations. Whether those operations belong to a shipping company, a hospital, a manufacturing facility, a chemical company, a municipality police department/911 service or a public power electric utility… it doesn't matter. All of the aforementioned examples have been operationally affected by ransomware. Sungard Availability Services (Sungard AS), a provider of IT production and recovery services, collected data for two years of ransomware attacks on municipalities (2019 and 2020). The results are staggering. More than 175 ransomware attacks occurred during this time. It's no exaggeration to say that municipalities are a major target.

The above statistics make it tempting to throw up your hands and declare defeat. However, that's not the whole picture. Gartner, a leading global research and advisory firm, determined during an analysis of clients' ransomware preparedness that *"over 90% of ransomware attacks are preventable. These attacks pose*

a threat to business data and productivity, but by following basic security fundamentals security and risk management leaders can mitigate risk against them."

Review Ransomware Prevention Checklist

In September 2020, the Multi-State Information Sharing & Analysis Center (MS-ISAC) published a ransomware guide giving a list of best practices and a ransomware response checklist. I urge you to read this short (16-pages) guide as it provides a wealth of information in a practical manner. Some of the best practices identified within the guide include:

- Joining an information sharing organization such as MS-ISAC or E-ISAC to be aware of the latest threats
- Maintain offline encrypted backups and regularly test them and maintain gold images of systems in the event they need to be rebuilt.
- Create and maintain a basic cyber incident response plan and test it regularly.
    - The American Public Power Association (APPA) has published a very good incident response playbook that provides guidance and a template for creating an incident response plan.
- Conduct regular vulnerability scanning and patch and update devices to the latest available software and operating system versions.
- Employ logical or physical network segmentation
- Ensure devices are properly configured with security features enabled and any unneeded ports and protocols disabled.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB.
- Ensure antivirus and anti-malware software and signatures are up to date and consider the use of an intrusion detection system to detect command and control activity.
- Implement a cybersecurity user awareness and training program and conduct organization wide phishing tests.
- Ensure your organization has a comprehensive asset management approach

Bring In Assessment Team

Many of the action items above are part of a comprehensive cybersecurity program, but often utilities don't know where to start or in which areas they are lacking. Hometown Connections has developed a cybersecurity assessment to provide this starting point. This assessment:

- Identifies and prioritizes vulnerabilities.
- Is based on industry standards and best practices such as the Cybersecurity Capability and Maturity Model (C2M2) and the Center For Internet Security (CIS) Controls.
- Can give leadership results they can use to gauge effectiveness and maturity of their cybersecurity program.
- Delivers detailed recommendations on how to:
    - Address deficiencies
    - Prioritize action items
    - Budget for security improvements

To gain a clear understanding of your cybersecurity posture in relation to our industry's best practices and frameworks, send an inquiry to info@hometownconnections.com for more information.

Stay Cyber Vigilant!

About the Author

Jared R. Price is the Chief Technology Officer (CTO), American Municipal Power, Inc. A co-owner of Hometown Connections, Inc., AMP is the nonprofit wholesale power supplier and services provider for 135 members in the states of Ohio, Pennsylvania, Michigan, Virginia, Kentucky, West Virginia, Indiana, Maryland, and Delaware.

Hometown Connections, Inc. is a national, non-profit utility services organization specializing in the unique challenges of community-owned utilities. Hometown Connections, AESI-US, Inc., and Marsh USA offer comprehensive cyber and physical security consulting and insurance solutions. Send your inquiry to info@hometownconnections.com for complete information.

Sources:

- https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19
- https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
- https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/
- https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks
- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
- https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook#:~:text=The%20playbook%20helps%20public%20power,coordinate%20messaging%20about%20the%20incident.