Risky Business Aging critical infrastructure networks and advanced attacks

May 13, 2021

Jennifer Dean | Product Marketing Manager

The most recent attack on a top U.S. fuel pipeline operator offered an unwelcome illustration of just how vulnerable key supply lines can be. Operating the country's largest refined products pipeline, Colonial Pipeline was brought to its knees over the weekend by a ransomware attack by cybercriminal gang, DarkSide. The Colonial artery is 5,000 miles long and transports 100 million gallons of fuel per day, so if the ransom is not paid or an agreement is not reached quickly, disruption could be significant. So far Colonial has been tight lipped about how the hackers gained accessed, but that's not important. Ransomware is the outcome of the overarching problem of underlying network security shortcomings and unauthorized access to critical infrastructure leaving it vulnerable to cyberattacks.

The Ugly Truth

We live in a more connected world today than many of our critical infrastructure environments were originally designed to support, and as we try to bring our critical infrastructure up to speed, the legacy systems are often patched instead of updated, or repaired instead of replaced. So a water treatment plant, or an electrical grid is most likely a patchwork of new and old, as software and hardware is replaced piecemeal. And unfortunately, security is often an afterthought. Making sure the environment is up and running and providing the service intended is top of mind.

The ugly truth is much of our critical infrastructure relies on networks with access controls, security flaws, and weaknesses that haven't updated over the years. When a network is breached and the data is not protected in transit, it leaves not just the data plane vulnerable, but the control plane and the management plane, essentially handing over access to the entire system.

Data Manipulation

Many breaches are all about data collection, which appears to be what happened in the case of Colonial Pipeline. According to BBC reporting, the hackers stole approximately 100 GB of data and locked access to it, threatening to leak the data if their ransom is not paid. But remember, there would be no data theft without unauthorized access to the underlying network.

Gaining entry to the network of a water treatment plant or an electrical grid can lead to much more sinister activity—data manipulation. Data manipulation happens when the attackers don't steal any data, but instead make tweaks to the data to upset the environment, which relies on real-time, accurate information. When the data coming in is slowed down, altered, or flooded (like with a denial of service attack), the results can cripple a critical resource.

Although scary to imagine, shutting down transportation hubs, taking controls of a nuclear plant, or creating widespread blackouts can all be done by gaining access to the networks of our most critical infrastructure. In fact, an event straight out of our nightmares happened in February when a hacker accessed a vulnerable network of a water treatment facility in the city of Oldsmar, Florida, and modified chemical levels.

Oldsmar Sheriff Bob Gualtieri said,

"Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners. It's also used to control water acidity and remove metals from drinking water in the water treatment plant," said.

"The hacker changed the sodium hydroxide from about 100 parts per million to 11,100 parts per million. This is obviously a significant and potentially dangerous increase."

WHAT? Luckily no tainted water reached residents' taps, but it is incredibly scary.

Modernizing Critical Infrastructure

Security experts are counting on the Colonial attack to be a wake up call for operators of critical infrastructure, including electrical and water utilities and energy and transportation companies. The same experts warn by not investing in updating security, critical infrastructure operators are flirting with catastrophe.

The rapid growth of virtualization, data center and cloud computing technologies means we are becoming increasingly reliant on high speed/high-availability data networks to deliver information when and where we need it. Cybercrime in the form of hacking, corporate espionage and even cyber terrorism, is on the rise.

The only fail-safe solution to ensure your data is secure as it travels across the network is encryption.

Network Encryption is Key

Information security threats remain commonplace and there is an increasing emphasis on organizations of all types to ensure the integrity and security of their data, both at rest and in motion.

We cannot rely on the assumption that our data remains secure within the perimeter of the office environment. All organizations share systems and information that rely upon common network access and most modern businesses comprise multiple offices, some separated by a few yards, others by thousands of miles.