9-American City and County-Ransomware

Ransomware attacks highlight need for adequate cybersecurity

Written by Andy Castillo

7th July 2021

For those not immersed in cybersecurity, the Colonial Pipeline cyberattack this past spring probably came as a shock *[Worry]*. Overnight, images depicting long lines of desperate drivers seeking fuel at gas stations that had suddenly been cut off from supply chains flooded the international newsfeed.

In May, the pipeline, which originates in Houston and supplies gasoline and jet fuel to much of the southeastern United States, was crippled by a ransomware attack issued by the criminal hacking group DarkSide. The attack impacted the pipeline's software system. With oversight by the FBI, Colonial Pipeline paid the hackers to restore its network. *[Compliance]* Sixty-three of the 75 Bitcoins paid to the hackers, worth millions of dollars, were eventually recovered by the FBI.

But not before the vulnerability of America's infrastructure had been laid bare *[Disappointment]*.

To city and county leaders, the attack highlighted an urgent need to harden digital municipal infrastructure. It's a subject that's been at the forefront of

public attention for the past few months, and one that federal leaders are tackling head on.

On Tuesday, as part of an ongoing initiative to engage with stakeholders across the country, Anne Neuberger, deputy national security advisor for cyber and emerging technology, met virtually with the U.S. Conference of Mayors, a bipartisan group of mayors based in Washington, D.C., to discuss cyber security challenges faced by local governments

According to a readout of the meeting issued by the White House's press office, Neuberger talked about the Biden Administration's ransomware strategy, "which includes several lines of effort: disruption of ransomware infrastructure and actors by working closely with the private sector; international cooperation to hold countries who harbor ransom actors accountable; expanding cryptocurrency analysis to find and pursue criminal transactions; and the federal government's review to build a cohesive and consistent approach towards ransom payments."

This cohesive approach feels particularly relevant given recent news.

Over the holiday weekend, Kaseya, a Miami-based IT and software security company, was targeted by a sweeping ransomware attack impacting between 800 and 1,500 small to medium sized businesses. The company's CEO, Fred Voccola, said in a statement issued Tuesday that the company "is working around the clock to get our customers back up and running. … We understand that every second they are shut down, it impacts their livelihood, which is why we're working feverishly to get this resolved."

The criminal group that initiated the attack, REvil, initially asked for $70 million to release the hacked accounts. In light of the breach, Keyesa is actively working with the FBI and CISA, according to the statement. Following the attack, Neuberger urged anyone who believes their system has been compromised to shut down their servers and report to the Internet Crime Complaint Center at IC3.gov.

At Tuesday's mayoral meeting, Neuberger highlighted an executive order signed into law by President Joe Biden in May, titled "Improving the Nation's Cybersecurity," which gives the administration's cybersecurity awareness efforts political teeth. The order was put forward as a step toward modernizing cybersecurity defenses "by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur," says a press release about the action.

She also discussed the Cybersecurity Industrial Control Systems Initiative, a program led by the Cybersecurity and Infrastructure Security Agency, a branch that falls under the Department of Homeland Security. The initiative includes all relevant entities—government, the private sector, academia and others—and focuses on protecting critical infrastructure (the following 16 sectors are defined by the federal government as "critical:" chemical, communications, dams, emergency services, financial services, government facilities, information technology, transportation systems, commercial facilities, critical manufacturing, defense industrial, energy, food and agriculture, health care, nuclear, water and wastewater).

Among many challenges faced by municipal leaders in the digital era, "Operational technologies are growing exponentially and migrating into domains not previously automated or connected to the internet (e.g., automobiles, medical devices, smart buildings and homes, pipelines,

aviation),” a fact sheet about the program explains. Further, 5G networks reduce the need for network routers, “limiting the ability of security providers to monitor for and prevent malicious traffic,” the sheet says.

Given the sophistication of cyberattacks these days, as exemplified by the recent Kaseya and Colonial Pipeline attacks, CISA and the FBI suggest implementing the following best practices:

Require multi-factor authentication for remote access to networks

Use strong spam filters

Train computer users about spear phishing emails so that employees don’t inadvertently click on a dangerous advertisement

Make sure that software systems are frequently updated

Program antivirus software to make regular system scans

Set up URL block-or allow-lists to prevent users from accessing malicious websites

Limit access to sensitive resources via the network

Make sure IT has well-documented standard operating procedures for resetting passwords

Regularly audit mailbox settings

Try to enforce the use of strong passwords and prevent passwords that could be easily guessed

As cyber attacks become more common, it’s vital that municipalities and businesses contracted by the government meet the threats with appropriate levels of security.

In an open letter issued last month to the private sector by Neuberger, she urged executive and business leaders to take its critical role seriously. “All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location,” Neuberger wrote. “We urge you to take ransomware crime seriously and ensure your corporate cyber defense match the threat.”