BRACEWELL

INSIGHTS

Florida Water System Hack Highlights Challenges for Public Utility Cybersecurity

February 23, 2021

By: ***Vincent E. Morgan***

Earlier this month, fears usually confined to dystopian novels and Hollywood movies were ***realized*** in Oldsmar, Florida when an unknown hacker breached the city's water treatment system by successfully accessing its control systems and increasing sodium hydroxide to deadly levels. Fortunately, the employee whose desktop was accessed quickly noticed the intrusion. Immediately after the mysterious intruder left, the employee re-adjusted the controls to safe levels before any contaminated water reached the community.

The hacker gained access though a widely-used commercial application that allows team members to access each other's desktops. These types of applications give users wide-ranging access to internal networks from the internet, making them useful for remote troubleshooting but ripe for abuse. Oldsmar's personnel hadn't used this particular software in months, but it remained installed on computers used to monitor and adjust chemical levels in the water system. In addition, the computers reportedly all ***shared*** one password to access the software and the computers ran on an outdated operating system. This incident highlighted multiple security risks in systems connected to critical infrastructure, but Oldsmar is not an outlier.

While many are calling this hack a "wake up call," it really shouldn't be – this attack is far from the first of its kind. We have previously ***warned*** of the increase in cyber threats against municipal and other ***public entities*** as hackers have accessed ***dozens*** of water utilities, ***including*** an intrusion of a system controlling a dam in New York State.

Responsibility for the Oldsmar incident remains unclear, but an increase in cyber threats from foreign actors remains a serious concern for public utilities and entities.[1] This is especially true in the wake of the ***SolarWinds*** hack, which began in March 2020 and was not discovered until December. Russian hackers are suspected of compromising widely used network management software to gain access to hundreds of local, state, and federal agencies as well as private companies' networks.

Government agencies and lawmakers continue to highlight the risks posed by cyberattacks, and understandably so. Last month, the Government Accountability Office released a ***report*** detailing concerns about gaps in the government's cybersecurity approach across several sectors of critical infrastructure. The report concluded by recommending further communication between the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) and the Environmental Protection Agency, specifically instructing the agencies to coordinate on how to close gaps in security at water and wastewater

facilities.

Anne Neuberger, the top White House cybersecurity advisor, ***told*** a federal advisory board this month that a national cyber strategy is in the works; citing the Oldsmar hack in particular, Neuberger said to "[w]atch this space for more of an explicit focus on control systems cybersecurity from the administration." Last week, Senate Intelligence Committee Chairman Mark Warner ***wrote*** to the FBI and EPA regarding the Oldsmar hack, requesting that the FBI provide updates on the investigation into the hack, that the EPA review Oldsmar's compliance with EPA security guidelines, and confirmation that the Federal Government is sharing threat information with similar facilities.

Public entities should keep an eye on changes in cybersecurity regulation and guidance, but in the meantime, there are a number of things they should do to proactively protect against cyberattacks. CISA ***recommends*** (1) segmenting and segregating networks and functions; (2) limiting unnecessary lateral communications; (3) hardening network devices; (4) securing access to infrastructure devices; (5) performing out-of-band network management, which limits access to infrastructure networks and separates user traffic from network management traffic; and (6) validating the integrity of hardware and software.

Remote work poses ***additional risks*** that warrant additional precautions. CISA ***recommends*** changing default passwords, restricting network access, encrypting data, installing firewalls, maintaining antivirus software, file sharing with caution, and connecting using VPNs. In its ***official alert*** about the Oldsmar hack, CISA also outlined recommendations to secure remote access software like the one used to access Oldsmar's system.

Public entities should also have an incident ***response plan***, including a list of law enforcement and cybersecurity professionals to call in the event of an attack. Municipal issuers should make sure they comply with Security and Exchange Commission reporting and disclosure ***guidance***. Some state laws mandate disclosure, meaning that public entities should also ensure their incident response plan includes any applicable state reporting. Having, and following, an incident response plan as well as taking robust preventative measures is critical to minimize the likelihood and ***impact*** of an attack on an entity's credit rating.

Additionally, ***cyber insurance*** policies can financially insulate policyholders by insuring against destruction of and loss of access to computer networks, including response costs and other damages caused by cyberattacks. In the case of public entities, insurance can be particularly important to protect against ***liability***. However, compliance with best-practices is still necessary, as coverage under such policies often requires the insured to comply with robust security standards.

Additional cybersecurity resources for the water sector are available through ***the American Water Works Association***, which provides free Cybersecurity workshops for small systems as well as a number of guides to assist water utility professionals in securing their systems. The EPA has also created a centralized page on their website with "***Cyber Resilience Resources***," including a Cybersecurity Incident Action Checklist and self-assessment tools. The Department of Homeland Security provides ***guidelines*** for reporting cyber incidents.

As cyber threats continue to increase in frequency and severity, it is critical to have a thoughtful, coordinated approach to cybersecurity. Organizations' risk management, IT, and

legal departments, as well as outside counsel, should work together to identify vulnerabilities in existing cybersecurity measures and take corrective measures, when necessary, to protect against cyberattacks and maximize coverage under cyber insurance policies.

As the Oldsmar water supply attack demonstrates, public entities need to maintain focus on cyber threats and their potential impact. If your systems oversee utilities, the worst-case scenario of a cyberattack can be much more than just losing data. Taking proactive steps to secure systems is crucial to avoiding the most severe consequences of cyberattacks.

---

[1] ***Ransomware*** attacks present particular concerns to public entities by holding important systems hostage in demand for payment, causing these systems to be offline for extended periods of time and compromising the data they held. For example, Baltimore was hit with ransomware attacks twice – once in ***2018***, when ransomware affected the city's phones and shut down automatic 911 and 311 dispatches, and again in 2019, when it immobilized the city's voice mail, email, and bill-paying systems, ultimately costing an ***estimated*** $18 million.