INTELLIGENT BUILDINGS

CYBERSECURITY POLICY AND INCIDENTS BRIEFING

ICYMI: The first water treatment facility attack of 2021 happened in San Francisco—weeks before the Florida water treatment facility hack.

06/28/21

SUMMARY

On January 15, 2021, a water treatment facility in the San Francisco Bay area was hacked using a former employee's TeamViewer account username and password. After logging in, the hacker deleted programs that the water plant used to treat drinking water. The hack was not noticed by the facility staff until the following day, at which time the staff changed passwords and reinstalled programs. Though this incident happened in January, it was only recently reported and released to the general public. The hack caused considerable damage, but the hacker's name and motives have not yet been identified by law enforcement.

How did this happen? This incident is indicative of the rise of cyberattacks on building/operational technology (OT) systems worldwide. This is not an informational technology (IT) problem alone, but a combination of IT and OT. The facility's network settings allowed a remote user to log into any desktop connected to the control system via the installed remote viewing software. Meaning, anyone on the outside with a username and password can access the system at any time, with any motive. In most cases, companies use a single username and password for all employees and a single username and password for all vendors. Typically, the login credentials are not changed, even when employees leave the company. So, if a former employee wants to access the system, they can—and they are unlikely to be identified. This makes it easier for the login credentials to fall into the wrong hands.

WHAT IT MEANS

This attack could have been easily avoided if the company had followed these best practices:

- Issue unique accounts to each building user and vendor user to enable full control and audit of each person's access.
- Remove an employee's unique user credentials the same day they leave the company or no longer require access to the system. This includes building and vendor employees.
- Use a secure remote access connection that is controlled by the building owner.

HOW INTELLIGENT BUILDINGS CAN HELP

We have assessed thousands of buildings in the US, Canada, and overseas. In our experience, most building owners don't know what's connected, how it's connected and configured, and do not have recovery strategies in place. For example, even if backups are being performed, they are usually not being performed correctly or securely. Intelligent Buildings can assess your building systems and the contractors who support them and provide you with an easy-to-follow plan to secure your building control systems. Additionally, our managed service can ensure that these steps are being followed and bring your systems and contractors into compliance.

https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206