Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Fatality File

Hacker gains remote access to Florida water treatment plant and attempts to poison water supply of 15,000 residents by manipulating chemical control systems

What Happened

On February 5, 2021, an unauthorized hacker gained remote access to the Bruce T. Haddock Water Treatment Plant in Oldsmar, Florida using TeamViewer – a remote desktop application shared by all plant employees under a single password with no firewall in place. The attacker accessed the facility's SCADA system and changed the sodium hydroxide concentration from 100 parts per million to 11,100 parts per million – a level capable of causing severe chemical burns or death if it reached consumers. An alert plant operator noticed the cursor moving on his screen, watched the attacker navigate the system live, and immediately reversed the change before it could take effect.

What Went Wrong

Investigation revealed that employees had been using an unsupported version of Windows with no firewall and shared a single TeamViewer password across all staff – giving any external actor who obtained the password full, real-time control over a safety-critical chemical process. No multi-factor authentication existed. No anomaly detection flagged the unauthorized access. The only barrier between a lethal chemical release and 15,000 residents was one worker watching his screen at the right moment.

The Bottom Line

This incident was stopped by human alertness — not by the systems designed to monitor and control the plant. Every connected safety system is only as secure as its weakest access point, and every sensor reading is only as trustworthy as the system reporting it. Workers must know what their digital systems cannot catch — and be prepared to verify conditions independently.

Source: https://www.securitymagazine.com