CYBERSECURITY POLICY AND INCIDENTS BRIEFING

ICYMI: Hard evidence of **direct threat to commercial building control systems** from Nation States.

08/02/21

SUMMARY

Classified documents were allegedly obtained from Iran that revealed secret research on how cyber attacks could be used to destroy equipment or even kill people using operational technology. These documents reveal a particular interest in researching companies and activities in western countries, including the UK, France, and the United States. To be even more specific, **Smart Buildings are identified as an attack vector**. The documents list several building controls manufacturers, such as Honeywell, Schneider Electric, KMC, Siemens, and others. This signals that the Iranians are getting very specific on what to attack and how to attack it.

According to General Sir Patrick Sanders, the top military officer overseeing UK cyber operations, "[Iranians] are among the most advanced cyber actors. We take their capabilities seriously. We don't overstate it. They are a serious actor, and they have behaved really irresponsibly in the past."

WHAT IT MEANS

This is concrete proof that **building controls systems are being targeted**. These reports, and the government memorandum, show clear and present danger to building control systems, including steps to compromise them. For building owners, property managers, facility operations, IT, and system vendors, this should be the wake-up call and motivation to **create a proactive cyber program for building control systems**.

You can prepare by:

- Verifying that no building control device is exposed to the public web. If it is, put it behind a firewall. Better yet, incorporate a zero-trust solution.
- Locking down access by making sure that no shared accounts are used.
- Making sure that all users are given only the access necessary to fulfill their job function.
- Controlling remote access. Do not leave it to the vendor.
- Monitoring control system networks for unusual activity.
- Creating a robust incident response plan for building control systems.
- Protecting against a socially engineered or a brute force compromise of your systems by implementing two-factor authorization.

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 to provide you with an easy-to-follow plan to secure your building control systems. Additionally, our managed service can ensure these steps are being followed and **bring your systems and contractors into compliance**.