Reducing Ransomware Risk in Smart Buildings

Ransomware is a type of malicious software that encrypts all of your data and then extorts the victim by demanding "ransom" to get the encryption key, without which the data is unusable. Ransomware has often been spread through phishing emails or by unknowingly visiting an infected website.

According to CNN Business, "Just this year alone, 140 attacks targeting public state and local governments and health care providers have been reported."[1]

These attacks have had significant impacts including causing school to be cancelled, shutting down municipal computing for weeks delaying or denying services to taxpayers and impacting healthcare services.

Here's what you can do to help reduce the risk that this unfortunate trend will begin to spread to building automation systems

- **Partnership.** Ensure local system and network managers and suppliers are on the same page. The proper functioning of this relationship is critical. As a team they are less likely to miss a critical risk that results in compromise. When working in silos it's difficult to identify and mitigate risks in time.
- **Assess your risks.** Work with your suppliers, internal resources or trusted security partner to assess your risk proactively, before there's an incident.
- **Secure remote access.** Ensure remote access from outside your facility into any industrial control system is secured. Systems should only be exposed directly to the internet if they were purposely built for such application. Refer to vendor product deployment guidelines.
- **Maintain product and other software updates.** While there may be an expense to regularly updating some types of building systems and underlying operating systems, the cost of maintenance compared to the cost and reputational damage or data loss from an incident puts this cost in perspective.
- **Limit configuration and use to intended functions.** Do not use building systems for email or other day to day computing activities.
- **Ensure Effective Backup and Recovery.** Effective Backups and Disaster Recovery plans and processes are critical to getting back to business quickly if you are the victim of a successful ransomware attack. This is a team effort that local system and network managers and suppliers all need to support.

Johnson Controls provides a number of resources to assist, including product hardening guides, product vulnerability notifications as well as contact information for our product security team.

https://www.johnsoncontrols.com/cyber-solutions

References

[1] https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html

Further Guidance and Information

US Department of Homeland Security Ransomware Resource
https://www.us-cert.gov/Ransomware

ENISA Ransomware Resource (EU)
https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware

US Department of Homeland Security Secure Remote Access Guidelines
https://www.us-cert.gov/ics/Abstract-Configuring-and-Managing-Remote-Access-Industrial-Control-Systems

About Johnson Controls

Johnson Controls is a global diversified technology and multi-industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat.

For additional information, please visit www.johnsoncontrols.com or follow us on LinkedIn, Twitter, and Facebook.

The power behind **your mission**

Johnson Controls