Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Telecommunications Industry Association

27 December 2018

PIN Number

20181227-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

Anticipatory Awareness Message: Cyber Security for Smart Buildings

Summary: *The FBI and the Telecommunications Industry Association (TIA), on behalf of its members, judge as next-generation information and communication technologies (ICT) provide increasing utility for smart buildings, the resulting system integration and connectivity potentially will provide new threat vectors for malicious cyber actors. This notification provides a primer on presumed and anticipated security issues which may arise from the increasing number of smart buildings across the United States, and presents partners in industry with some mitigation measures and best practices for cyber security. Further, the FBI and TIA recommend smart building developers consider and address potential vulnerabilities through the identification of specifications, frameworks, and standards during the initial phases of smart building development.*

This report is intended for individuals and organizations responsible for the management and/or maintenance of smart buildings, including building managers and network administrators. The recommendations outlined in this report do not represent the full range of risk mitigation measures for smart buildings. Additional recommendations for building physical security is also addressed in this report.

ICT are increasingly important for modern buildings, and advances in the sophistication and performance of networking and computing technologies are accelerating the connectivity of these facilities.

Further, the coming rollout of next generation communication technologies like 5G likely will result in the placement of edge infrastructure–computing, networking, and data transmission systems–in urban environments, particularly in smart buildings.

Smart buildings will feature a number of integrated ICT systems, and make use of automation and other smart infrastructure. This can include, but is not limited to building management; heating, ventilation, and air conditioning (HVAC); access control; industrial control systems (ICS); supervisory control and data acquisition (SCADA); and other cyber-physical systems.

- Malicious cyber actors have exploited vulnerabilities in HVAC and ICS/SCADA systems in attempts to gain access to commercial and critical infrastructure networks.

Because of the varying architectures, networking protocols, operating systems, and potential integration with other physical components, these system-of-systems will present an expanded cyber attack surface to malicious actors. Further, the integration of new ICT with smart infrastructure and legacy cyber-physical systems may create vulnerabilities which are not apparent to system developers or network administrators, and may not be fully addressed by standard cyber security practices.

Smart buildings will make use of a wide variety of Internet of Things (IoT) devices. Integration of these devices into building systems–in the form of cameras, thermostats, other sensors, and multimedia devices–likely will create situations where building managers and network administrators are unaware of the numbers and types of systems connected to their networks. This shadow infrastructure creates additional cyber security vulnerabilities due to the challenges associated with performing necessary system updates, patching, and configuration management.

Comparing ICT and IoT

ICT refers to all technologies which capture, store, retrieve, process, display, represent, organize, manage, secure, transfer, and interchange data and information. The Internet of Things refers to a broad network of Internet connected objects and sensors which collect and exchange data. IoT devices communicate with the Internet to send and receive data, and are often referred to as *smart devices*.

As smart buildings integrate IoT devices, facility managers and network administrators should take a holistic view of the entire device ecosystem to enable dynamic vulnerability identification and risk management.

Owners and operators of smart buildings should consider how facilities are connected to municipal utilities. As more municipal services are enabled with networking functionalities, reliance on these systems may create unintended physical vulnerabilities if they are rendered inoperable by a malicious cyber attack. Accordingly, connection to or reliance on other smart infrastructure may introduce additional vulnerabilities.

- Smart buildings managers should consider appropriate risk management processes as they relate to facilities, including ongoing identification, evaluation, and mitigation of cyber and physical vulnerabilities. As smart system integration and implementation in buildings will vary from location to location, managers should determine which specifications, frameworks, standards, and risk management processes are appropriate for their facilities.

Smart building physical control and management systems like ICS/SCADA, HVAC, access control, security, and other systems could provide a vector for malicious cyber attacks. Building managers and network administrators should consider the same types of security measures on these systems as they would with traditional networked systems.

Finally, some smart systems like access control and facility security systems, which may use biometric and other sensors, can capture personally identifiable information (PII) of facility occupants and visitors. Building managers and network administrators should be conscious of how this information is processed and stored, as it may be of interest to malicious actors seeking to harvest PII and other sensitive information.

Recommendations

The FBI and TIA recommend organizations developing or integrating smart building systems consider the following security practices. Specific attention should be paid to the integration and management of networked ICT with cyber-physical systems, including data transmission, storage, and archival infrastructure.

In addition to the cyber best practices highlighted at the bottom of this notification, the following seven strategies[a] were developed in conjunction with the FBI, the National Security Agency (NSA), and the Department of Homeland Security (DHS). These strategies are intended for ICS, which can be found in many of the cyber-physical systems associated with building management, monitoring, and access control technologies.

- **Implement Application Whitelisting** – Can detect and help prevent attempted execution of malware uploaded by adversaries
- **Ensure Proper Configuration/Patch Management** – Safe importation and implementation of trusted patches can help keep systems secure
- **Reduce Your Attack Surface Area** – Isolate systems from untrusted networks, disable unused ports and services
- **Build a Defendable Environment** – Segment networks into logical enclaves and restrict machine-to-machine communication paths
- **Manage Authentication** – Implement multi-factor authentication where possible and follow least-privilege principles
- **Implement Secure Remote Access** – Limit remote accesses, consider monitor-only access, and eliminate persistent remote connections
- **Monitor and Respond** – Perform system baselines and monitor for changes, develop detailed response and restoration plans

Measures to Deter Unauthorized Access to Computer Networks

In general, recommendations for cyber security include, but are not limited to, educating personnel on appropriate preventative and reactive actions.

- Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.
- Disable macros. Be careful with pop-ups from attachments which require users to enable them.
- Only download software–especially free software–from known and trusted sites.
- Create a centralized e-mail account for employees to report suspicious e-mails.
- Change network default passwords, configurations, and encryption keys.

[a] NSA Cybersecurity; CTR U/OO/137677-18; Seven Steps to Effectively Defend Industrial Control Systems; 5 April 2018; source is a joint FBI, NSA, and DHS cybersecurity report.

- Recommend your organization’s IT professional(s) review, test, and certify the need/compatibility of a patch or update prior to installing it onto the operating system or software.
- Monitor employee logins which occur outside of normal business hours.
- Restrict access to the Internet on systems handling sensitive information.
- Install and regularly update anti-malware solutions, software, operating systems, remote management applications, and hardware.
- Do not use the same login and password for multiple platforms, servers, or networks.
- Monitor unusual traffic, especially over non-standard ports.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Isolate sensitive information within the network.
- Only allow required processes to run on systems handling sensitive information.
- Implement two-factor authentication for access to sensitive systems.
- Ensure proper firewall rules are in place.
- Be aware of the organization’s footprint and persona facing the Internet. Conduct searches using multiple search engines on multiple Internet domains of the organization’s names, Web addresses, key personnel, and projects to determine if there is an accidental weak point in the network security. Conduct infrastructure look-ups in the public domains to ensure additional information is not inadvertently advertised.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Regularly mirror and maintain an image of critical system files.
- Use strong passwords, implement a schedule for changing passwords frequently, and avoid reusing passwords for multiple accounts.
- Enable network monitoring and logging where feasible.
- Be aware of social engineering tactics aimed at obtaining sensitive information.
- Securely eliminate sensitive files and data from hard drives when no longer needed or required.
- Establish a relationship with local law enforcement and participate in IT security information sharing groups for early warning of threats.

Physical Security Considerations

Given smart buildings will integrate numerous ICT and physical systems, consideration of physical security for critical systems is also appropriate. Additional resources from DHS are available, and provide context and perspective regarding the safety and security of facilities and integrated systems.

- The DHS report *The Future of Smart Cities: Cyber-Physical Infrastructure Risk*, while tailored for smart cities, still provides key points to consider regarding the integration of smart systems.[b]
- The DHS report *Risk Management Process for Federal Facilities* provides additional best practices related to security of sensitive facility systems, related ICT, and physical infrastructure.[c]

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at cywatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

The Telecommunications Industry Association (TIA) represents more than 400 global companies that enable high-speed communications networks and accelerate next-generation ICT innovation. Through leadership in U.S. and international advocacy, technology programs and standards development and business performance solutions, TIA and its members are accelerating global connectivity across every industry and market. The FBI is not endorsing TIA or any of its constituent members through the publication of this notification. To learn more

[b] Report; Department of Homeland Security; The Future of Smart Cities: Cyber-Physical Infrastructure Risk; August 2015; source is a report authored by the National Protection and Programs Directorate.

[c] Report; Department of Homeland Security; The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard; November 2016; source is a report authored by the Interagency Security Committee.

about the TIA and the Smart Buildings Program, please visit https://www.tiaonline.org/ or contact Limor Schafman, Director, Smart Buildings Program at lschafman@tiaonline.org.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, please contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey