dailyreporter.com

Experts urge building designers, operators to be ‘cyber’ smart

By: Alex Zank, alex.zank@dailyreporter.com March 10, 2017 3:38 pm

It’s no longer good enough to put up “smart” buildings. Experts in cyber security say buildings that have automated systems to control room temperatures, ventilation and other environmental conditions must also be “cyber” smart in order to be safe from hacking.

To more efficiently monitor and manage their interior operations, smart buildings often have their HVAC controls and security systems connected to an external network. Buildings controlled this way can be run more efficiently and decrease costs.

With the benefits of these automated buildings, though, comes a new set of threats.

Any building feature or device that is connected to the Internet is susceptible to hacking, said Thomas Kaczmarek, director of the Center for Cyber Security Awareness and Cyber Defense at Marquette University.

Security cameras connected to a building network, for instance, can be hacked by someone who could then use the equipment as a “backdoor” to access other information.

This is particularly alarming for those who put up and maintain certain types of buildings, especially ones that house information not intended for public circulation.

Jason Rosselot, director of global product security at Johnson Controls, said various industries have recognized the dangers and taken steps to make their buildings more secure. The forerunners in this regard include energy producers, health care providers high-tech manufacturers and government agencies.

Rosselot said it’s not hard to understand the need for caution. A hospital, for instance, could take a serious financial hit if a hacker were to shut down an HVAC system in an operating room. Even worse, patients could be endangered.

“The cost to the hospitals … is tremendous, in addition to the patient-safety aspect,” Rosselot said.

Johnson Controls, along with the Virginia-based management-consulting firm Booz Allen Hamilton, recently published a white paper on “cyber smart” buildings. The document goes over cyber security risks that are almost inherent in the use of smart buildings and provides guidance to building owners, designers and builders on how to best avert these threats.

Protecting a building from cyber threats starts with placing trust in experts, Kaczmarek said. A network administrator, he said, can set up a building’s network in a way that gives it various “domains.”

Kaczmarek said these domains should be segmented, meaning that one used for security systems or temperature controls would be separate from those used for other purposes.

A system of this sort limits the information these networks can share freely, he said. The goal is to eliminate any backdoor a hacker could exploit to steal information or disrupt a building’s operations.

Another simple step building owners can take is to make sure any new device that’s installed, such as a “smart” TV in a conference room, is appropriately protected from cyber threats.

“Do your homework before you buy something and put it in,” Kaczmarek said.

Rosselot also suggested that building designers and builders work with manufacturers that understand cyber security.

Such safety measures should be taken as early as the design and construction phases of a new building, the Johnson Controls white paper argues. Although getting started so quickly could increase a project’s cost, it’s still cheaper than finding out later that an already completed building needs to be made cyber secure or, even worse, suffering a hacking attack.

Although many people understand the need for cyber security, large numbers of buildings remain exposed. Rosselot pointed to a study conducted by the security-software company Trend Micro looking at how many Internet-connected devices are exposed to hacking threats.

As part of the study, researchers used a search engine called Shodan to find Internet-connected devices in large U.S. cities. The researchers discovered more than 3 million exposed devices, or “assets,” in Los Angeles and Houston. A separate scan of New York City turned up only about 1 million exposed internet-connected devices.

Yet, for one reason or another, cyber threats to building-control systems have not gotten as much attention as related risks, such as massive data breaches at companies like Target and Yahoo.

“It is safe to say that this is an area of risk that has probably not been addressed to the level of other (Information Technology) related security risks,” Rosselot said.

Tagged with: HVAC

ABOUT ALEX ZANK, ALEX.ZANK@DAILYREPORTER.COM

Alex Zank is a construction reporter for The Daily Reporter. He can be reached at 414-225-1820.

RELATED ARTICLES

Furnace installed hours before house exploded
December 21, 2016 12:44 pm

Johnson Controls shakes up heating, cooling unit
September 15, 2014 12:56 pm

Stoughton company loses appeal against ASHRAE
June 20, 2014 4:06 pm