Are smart buildings safe from hackers and privacy breaches?

March 14 2017, by Sam Edwards

Credit: Youris.com

The automated home and office market is predicted to grow quickly in the next few years. But as reports of cyber attacks increase, is it still possible for a home to be a castle in the age of smart buildings, or are we

lowering the drawbridge to hackers?

Smart buildings offer better energy efficiency and the kind of futuristic mod cons that appeal to many consumers, but some experts warn our appetite for new technology is putting us at risk from increasingly sophisticated cyber attacks.

The smart home market – worth an estimated $47 billion (44.5 billion euros) in 2015 – is expected to grow to more than $120 billion by 2022 (almost 114 billion euros). Yet while the appetite for smart homes is growing, there are several cases that highlight the weakness apparently inherent in internet connected buildings.

In January, hackers reportedly took control of the electronic key system of a hotel in the Austrian Alps. Fully booked and with little alternative, the hotel paid the 1,600 euro ransom to regain control of the system.

As consumers buy increasing numbers of internet-connected devices from a range of manufacturers, security experts are warning that we risk unknowingly exposing ourselves to the risk of privacy breaches or ransomware attacks. "When you look at the internet of things (IOT) devices and other technology you can always see the same problem, there are vendors trying to go to market quickly and they don't pay attention to security," says Cesar Cerrudo, CTO at security consultancy IOActive.

Cerrudo argues that companies need to think more about security, claiming that regulation is often either too lax or not enforced, leaving manufacturers to auto-regulate in many cases. Consumers, meanwhile, are advised to protect themselves by being more aware of the risks, and demanding better standards from manufacturers.

Avoidable security problems include using outdated operating systems.

"If you are running new technology, which is maybe secure, you are making it insecure because you are running it on Windows XP," Cerrudo says.

To highlight such risks, IBM's research department, known as X-Force, recently hacked into a Building Automation System (BAS) that controlled thermostats in several buildings. The team found weaknesses in both the individual buildings and the central server.

Credit: Youris.com

Given the considerable potential for security breaches, how can we benefit from the energy efficiency offered by smart buildings while minimising the risk of cyber attacks?

European project BRESAER is developing a Building Energy Management System (BEMS) designed to manage the different functions of a smart system, using energy more efficiently, and prioritising renewable sources where possible. Using algorithms and artificial intelligence to control production and consumption of energy, the system hopes to offer a 10% saving on energy used.

While data in public buildings is perhaps less sensitive than, for example, a private home, where energy use indicates many details of a resident's schedule, it is still desirable to take measures to minimise the risk of cyber attack.

If an automation system were compromised, hackers could potentially take control of lighting, heating or even security functions such as locking doors. While thieves could potentially thus gain access to a building, more common threats may include inconvenience, or potentially ransom of the sort reported recently in the skiing resort in the Alps.

All information in the BEMS is communicated via a private internal network, says José Luis Hernández García, a researcher at Cartif, a technology firm working on the Bresaer project.

"However, for future consideration, [the BEMS system] is designed to function using secure communication channels, which function to improve security," added García. "Furthermore, we employ a procedure of data backup to avoid the loss of data in the event of an intrusive attack, virus or malware."

To combat threats to security and privacy, EU regulation will come into effect from May 2018. For García, the European General Data Protection Regulation (GDPR) could help standardise what he sees as a complex mix of current regulation across the continent.

Cerrudo says that better regulation could help, though for it to be effective, authorities must work hard to verify manufacturer's claims.

More information: BRESAER will design, develop and demonstrate an innovative, cost-effective, adaptable and industrialized envelope system for building refurbishment. This system will include combined active and passive pre-fabricated solutions integrated into a versatile lightweight structural mesh.

Provided by Youris.com