Bad connection

25 May 2018

Smart building technology brings many benefits but is also vulnerable to hackers and viruses. Robert Miller looks at how you can protect connected buildings

---

Buildings have for a long time included a host of electronic components to control everything from physical access to air conditioning. Traditionally, such components have been stand-alone, isolated devices that required physical access to monitor and manage.

However, many technology manufacturers have now taken advantage of mobile devices and the Internet of Things (IoT) to offer connected, modern alternatives for building systems. These enable building managers and their tenants to control their offices and homes remotely, monitor cameras from across the globe, access real-time information, operate more efficiently to reduce waste and cost or even have devices interact with other systems, presenting new opportunities.

In order to achieve this, smart building devices need to be connected to networks, and in some cases given access to the internet. As such, core building systems are for the first time being exposed to cyber-security risks.

So although you may wish to install these systems to take advantage of their new features, you may also feel concerned about the risk of being hacked. This feature looks at what the risks are, why hackers are interested in such systems, and what steps we can all take ? without needing a PhD in cyber security.

Meet the hackers

According to many articles in the press, people who hack smart buildings want one thing ? to invade our privacy. Why else would someone hack a smart camera other than to watch us through it?

Although this may be some people?s motivation, it is at most a niche interest. As malware such as Mirai showed us, the value of such systems for many hackers is simply that they are connected to the internet.

Websites can only handle so many visitors at the same time before they cannot cope with the volume of traffic, and deliberately creating such a situation is called a denial of service (DoS) attack. Achieving a DoS with a single computer these days is nearly impossible, but with thousands of devices under their control, Mirai?s owners could have all of these start to make requests to web pages in incredible volumes. Don?t like a company? Want to make its web page inaccessible? Just pay Mirai?s owners to take it offline by flooding its site with traffic.

There is another reason that smart building technology is a concern for IT security

professionals, however. These systems are sometimes on the same network as their developer?s PCs or servers that host customer data, and they therefore represent a route into companies? most prized possessions ? but they are run and managed by staff who may not understand cyber security.

Cyber security is an ongoing process of investing time and effort in protecting systems

Attacking smart buildings has for this reason been uncommon so far, and has been limited to certain high-profile targets. In one case, a North American casino was partly hacked through the system controlling its fishtank ; in another incident, the Wall Street Journal reported that the a hack of the US Chamber of Commerce may have been possible due to a thermostat that was communicating with an IP in China .

Skilled attackers will look for an easy route into an organisation, preferably one that lands them near the data they seek. In many cases the easiest route is a phishing attack, where passwords are obtained by contact with an employee under false pretences. However, should a hacker discover an externally accessible and easily compromised device, they are likely to attempt an attack.

Similarly, smart devices are often not secure enough to install in our buildings. Many lack basic security protections, and are regularly supplied with guessable passwords, out-of-date software and poorly secured applications. Worse still, many modern building systems are connected to the internet without first being redesigned to deal with the risk of exposure to attackers. In some cases, this means that they are open to anyone who wants to connect to them from across the internet, and also contain known software issues. It?s a recipe for disaster.

The first 4 steps

Although integrating cyber security into smart buildings may seem a daunting task, it turns out that simple actions can make a huge difference in keeping hackers out of your network ? and your company?s name out of the papers.

Passwords

We all know that choosing 'password1' to access our internet banking is probably a bad idea. Yet many smart building systems come with such passwords as default, leaving it to us to change them. The Mirai botnet operated in a deceptively simple way: it tried to access devices that were on the internet and were listening for connections; it then tried the 60 or so default passwords used by various IoT devices.

Changing building systems? passwords from their defaults, however, would have prevented some 400,000 devices from being compromised by Mirai in 2016 . The UK?s National Cyber Security Centre (NCSC) provides guidance on how organisations can best manage passwords securely, including rules to follow when creating them, and how to help employees avoid 'password overload'.

Limit access

The principle of least privilege is a core concept of computer security: applications should only be able to access what they need to access. Not only does this decrease the likelihood of a device being accessible to hackers in the first place, but it then reduces what the hacker can do even if they were to compromise that device.

It can be tricky to implement this principle, however. Removing user privileges and configuring networks is a full-time job for many IT professionals. And although there are normally some simple and effective measures that can be employed with smart building systems, they require thinking about before the system is installed.

Most building systems connect either entirely or partly to wifi, ethernet or other IT networks, allowing them to be accessed and managed by PCs and by smartphone apps. It can be tempting therefore to install and connect these devices to the building?s existing IT infrastructure. But it is important to consider what else is connected to this network, and what may be connected in the future. If tenants may be connecting personal devices or if corporate networks might be integrated in future, then a separate network should be used for the building system.

Update whenever possible

Readers who use Windows regularly may have noticed Microsoft has changed how it performs updates. Gone are the days of manually checking and installing updates, so it now occurs auto-magically whenever we shut down our computers. Why? Because we were all too unreliable at updating our machines ourselves, and hackers took advantage by exploiting the breaches this left in our defences.

Modern IT companies will have strict policies in place to update their computers whenever new software or patches become available in order to mitigate this threat. Yet some devices, including many smart building systems, do not offer automated updates, so it is important that processes to enable this are in place. It may simply require a monthly calendar reminder to check the device manufacturer?s website for update notices, or signing up to its newsletter.

Think about incident response

Incident response means handling a suspected cyber security breach. This will involve reviewing a network?s systems to understand what happened, what the impact was, and what you need to do to recover. A major part of this process is to review the logs of any affected systems to understand what the hackers accessed, and what actions they took.

Time is critical in these incidents, so it is important to understand what logs are available and how they can be accessed in advance. Many building management systems offer logging, though this may need to be enabled by the owner. An isolated building management network will usually have a minimal volume of traffic, so monitoring software could be a simple and affordable addition.

So I'm safe now?

Safer, yes: not just from preventing compromise in the first place, but also from the inevitable media fallout. Many media articles will after all focus not only on the incident but the mistakes that allowed it to happen.

Ultimately, cyber security is an ongoing process of investing time and effort in protecting systems and users from hackers. It needs to be balanced against other business requirements, and focused to prevent the greatest threats.

Cyber attackers will always change tactics to take advantage of the latest technologies, so what is secure today may be vulnerable tomorrow. Keeping an eye out for reports on the latest cyber attacks and asking how you would be affected is a great way to keep your buildings safe.

Robert Miller is a senior security consultant and researcher for MWR InfoSecurity

Further information

- Related competencies include: Data management and Property management
- This feature is taken from RICS Property Journal (May/June 2018)
- Related categories: Property management