Building automation and artificial intelligence creates new cybersecurity threats - by Richard Luna

May 30, 2023 - Spotlights

Richard Luna

Cybersecurity threats are changing on a daily basis with criminals and bad actors constantly looking for vulnerabilities. Through the increased use of cloud applications, real estate managers and owners seek to enhance tenant and visitor experiences; they are, at the same time, creating new cybersecurity weaknesses.

Building automation relies on the use of data and hard-wired connections as well as wireless networks. Multiple access control changes were rapidly implemented during the COVID-19 pandemic to make entry into buildings seamless and without guests having to touch surfaces. At the same time, there was a strong push to have tenants use cloud applications for access, rent payments and maintenance requests.

Here is a real-life example: in Manhattan at a commercial office building, a visitor approached a security desk, their name was given, appointment confirmed and photo taken. The guest was then directed to a specific elevator. The building's AI followed them, using cameras and sensors. The elevator, which had no buttons inside, automatically took the guest to the correct floor for their meeting. When the meeting was over, cameras and sensors again detected the guest's presence and elevator doors opened; the guest was taken to the lobby and monitored as they exited the building.

This demonstrates how technology enhances our lives and experiences. It looks and feels great, until we examine what makes it all work. Each of the systems and all of the IoT devices (Internet of Things – any device or sensor connected to the internet) in the building could be attacked through various means; Wi-Fi, guest networks, open ports or any system that is not hardwired and isolated from the Internet. Like any engineering student knows, the more complex a system, the more potential points of failure are present, and thus, it is more vulnerable to cyberattacks from either outside or from within.

For owners with multiple properties in their portfolios or real estate management companies, cybersecurity is becoming more challenging. These property owners must monitor, maintain and update firmware, software and equipment regularly. While the new technology and applications add great functionality, they also create added security burdens. Now property owners and managers need to work with both their IT providers and applications vendors to ensure access points as well as data are secure.

Adopting technology is a double-edged sword. Efficiency and experiences are enhanced for tenants and guests but new and dangerous challenges arise. With increased automation, infrastructure systems become potentially exposed to determined nefarious actors. Cyber attackers are determined, creative, and learn quickly how to exploit these weaknesses. To fight them, a greater investment in monitoring, security, firewalls and anti-malware is essential. All new and connected systems have to be monitored, and have protocols in place to prevent unwanted access to sensitive infrastructure and data.

Adding to the complexity is the use of mobile applications by tenants and guests. In some cases, multiple apps are used to provide services. Apps for entry, guest management, rent payments, maintenance requests and environmental controls are often provided by different companies. To be efficient and user friendly, these applications need to be interconnected and allow for data to be shared and stored by management companies and owners. Every time a new application is layered onto a database or connected to different systems, security gaps can and often do occur. Consider that many high-rises have hundreds or thousands of residents. Each resident may have multiple apps on their devices and each, will house or access critical data including names, addresses, banking and payment information. With large numbers of users and massive amounts of data, security becomes even more problematic.

Many property owners turn to their IT Managed Service Providers, MSPs, to support them and offer advice for data protection. Not all MSPs offer this level of support. Today, managers need to be savvy and know what security questions to ask of their app and software vendors. These questions include who exactly is storing, monitoring and protecting this data and how? Can building management hold their app vendors accountable for data breaches? What is being done to protect against cyber loss? How do residents/tenants know that their data is safe? Will insurance coverages of application providers and building managers cover the loss of data or possible financial losses incurred from a breach? Is business interruption insurance part of policies that protect commercial tenants?

Additional questions need to be explored in terms of how information is shared and how apps communicate with each other. With the use of multiple apps by tenants, how do they work together? Do they securely “talk” to each other and share data? Each app will have different user agreements and at this time there is no one comprehensive app that can do everything that is needed.

Building management companies must do their due diligence regarding their software developers and ask every one of their app vendors what their security and data management policies are. These questions include: does the company enforce two-factor authentication on their employees? Is their data comingled, or is it isolated per client? What is their stated policy for data breaches? Do they have cyber insurance? How many data breaches have they had? Who are they sharing information with? Do they have backups and redundancies?

Industry trends indicate that the future is cloud services and software as a service (SaaS) applications. More people are utilizing only their smart devices for all of their personal and business needs. For many today, and more to follow, subscription-based apps are all that they use. This means that all their data will be stored in the cloud and almost nothing saved locally. This makes it even more difficult to ensure security.

The new reality is that real estate managers and owners need to work with savvy cyber-security and IT consultants who offer a full spectrum of protective services to clients. With clients, IT providers will need to ensure that backups are routine and frequent, data is housed and transmitted with end-to-end encryption, employee safeguards are in place and all mobile applications must communicate with each other in a correct and secure way. This will all need to be done

transparently to assuage tenants’ concerns and safeguard data.

Richard Luna is CEO of Protected Harbor, Orangeburg, N.Y.