Top Cybersecurity Concerns for Commercial Real Estate

05.01.18

Until a few years ago, many commercial real estate (CRE) organizations had not been specifically targeted by hackers and could avoid cyberattacks by simply employing the concept of “security by obscurity.” Then the infamous Target hack happened. The original entry point for the Target breach was a facility HVAC system. Starting with the exploitation of a simple HVAC management system that connected to the facility network, complete compromise of customer data (and headlines) followed.

Today, many owned and tenant systems are potential attack points, including:

- HVAC, building management, and generator/ uninterruptable power supply systems,
- Physical lock mechanisms,
- RFID electronic lock mechanisms,
- Wi-Fi networks,
- Point-of-Sale systems,
- Portfolio Management software,
- Wireless peripherals,
- Etc.

There are a multitude of web vulnerabilities, like those that breached Target, Deloitte, Equifax, and many others. These attacks take advantage of network gears, web servers, email, and web/cloud applications.

Many facility attacks don’t make headlines because these attacks often go undetected. Attacks on physical buildings can take both physical and electronic forms. Here are a few examples.

Surveillance systems are highly specialized and often poorly understood by CRE facilities and IT personnel. They are also notoriously unsecure. Surveillance systems are often configured with weak default credentials and web-facing versions that are sometimes vulnerable to brute force guessing attacks (see Figure 1).

Many CRE personnel assume physical security controls, such as door locks, work as advertised. As it turns out, door locks often don’t often work as advertised and worse yet, even those that do often require extremely precise installation procedures or they’re rendered effectively useless (see Figure 2).

Electronic door locks are also susceptible to direct attacks. The most common type of electronic door lock attack is to stealthily steal RFID badge credentials. Using a powerful badge reader hidden within a laptop bag or backpack, the attacker steals the RFID card information, either on-premise or at a nearby coffee shop. Once they gained possession of the employee’s card data, the hacker can easily replicate a fake card. After creating the fake card, then all those wonderful records generated by the card system will point to an innocent employee, not the real perpetrator (see Figure 3).

Another common site attack involves injecting keystrokes into wireless keyboards and mice. Many models from major manufacturers may be susceptible, and from ranges in excess of 100 feet. At such long ranges, an attacker can remain safely outside a facility, while compromising internal BMS, alarm, HVAC or any other system connected to a computer with a wireless keyboard or mouse. The attacker can, with a couple dozen lines of pre-scripted code, completely commandeer a victim’s computer (see Figure 4).

Defending against these varied attacks starts with knowing where your sensitive data resides and what systems can access that data. Then, a risk assessment can provide guidance in regards to which security and privacy controls are appropriate for your organization. Rigorous deployment of applicable controls requires detailed documentation and close attention to hardening vendor-default credentials that are vulnerable. Finally, comprehensive controls testing and audits validate their effectiveness and provide guidance on priorities for reinforcing protections.

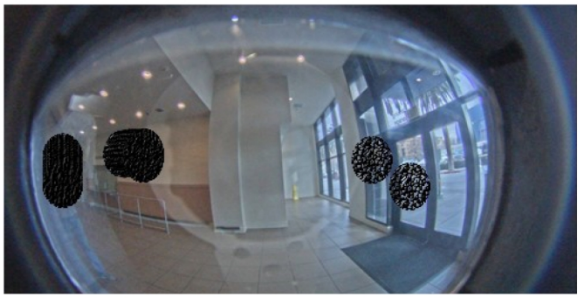

Figure 1. Surveillance systems often have default credentials and/or are susceptible to brute force attacks.

Figure 2. Typical panic bars are one of many door lock types tha are vulnerable to simple, non-destructive attacks.

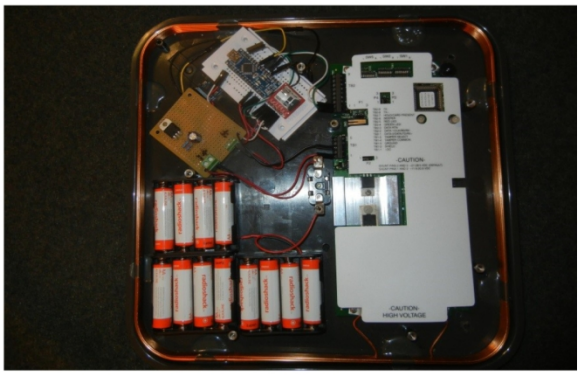

Figure 3. A parking garage RFID badge reader has been weaponized for badge theft and replication.

Figure 4. Remote injection devices can inse keystrokes into wireless keyboar mouse ports fro over 100 feet aw

David Trepp, *partner in BPM's Information Security Assessment Services practice, has led over 1,100 information security penetration test engagements for satisfied customers across all major industries throughout the United States and abroad. Contact David at dtrepp@bpmcpa.com or 541-687-5222.*