Hospitality IT Security

8 common flaws found in most hotel/resorts today

Charles Hornat
CBH Technologies, Corp.
www.infosecwriters.com

Overview:

This paper outlines some of the many IT security issues I have witnessed when taking over hotel/resort IT and security. These security lapses often times leave guest information free and open for the taking, usually requiring little to no effort to obtain. In my company's experience (over a decade) of supporting some of the most prestigious hotels in the world, we see many of the same issues time and time again and I outline some of the more common issues we have come across.

As hotel technologies continue to advance, so do the concerns around consumer data and privacy. Every year there is a report, such as the one posted on lodgingmagazine.com[1], about how consumer confidence in data protection and privacy within the hospitality and travel industry is at a low, while travel and hospitality continue to grow at an incredible rate. Additionally, with data theft on the rise, most industry experts are recognizing the gap in security as a real concern. For example, ehotelier.com posted a story on the top 5 risks and security challenges for hotels in 2015[2] in conjunction with Sky Touch Global Hotel Security Consulting. The #1 concern was identity theft leading to credit card fraud.

Hotel Networks 101:

Most hotel and resort networks are setup relatively the same. The only variation maybe between a few select vendors and or virtualization. The core of Hotel technology evolves around the Property Management System. There are two major vendors for this technology, and most properties use one or the other. The vendors are Opera and Maestro. The reason for this is that all the other hotel technologies must be able to plug in to the Property Management System, or the PMS.

Hotels usually have the following sub systems all created by and supported by third parties: Phone, Door Locks, a Point of Sales system for both room charges and a gift shop, television and movies, gift card or store outlet, and perhaps a restaurant that includes a reservations system like OpenTables and a Point of Sales system as well.

Each of the subsystems above will connect to the PMS so that any actions on the above will be charged or recorded to the correct room. It also stores this information so that when a guest comes for a second or future visit, the hotel staff knows what interest or special needs that guest may have. Special touches like this are what set apart common overnight hotels from the hotels that offer a true guest experience. However, this information also may contain some very personal information that an attacker may use.

Keycards that are electronic, standard in most hotels, are also a third party system that connects to the PMS. Every time a guest checks in, new keycards are created for that room and guest needs. Imagine if an attacker were able to create a master key or just a key to a specific room they are targeting? Or just crash the entire system and create a denial of service attack, preventing any guests from entering their rooms.

Since all these systems are created by different companies, each has their own security concerns and issues. Additionally, if one were to target the PMS, they could gain access to each of these subsystems through a trust relationship.

---

[1] http://lodgingmagazine.com/consumers-dont-trust-hotels-to-protect-personal-data/

[2] http://ehotelier.com/insights/2015/01/23/top-5-risks-and-security-challenges-for-hotels-in-2015/

Hotel networks are usually broken down to two distinct networks: the administration network and the guest network. They are usually configured by a third party who has expertise in doing so, and are usually not easy to cross over from one to the other.

Common Concern #1: We will start with the staff. Most hotel staff are there to make your stay as comfortable as can be. In fact, as crazy as it sounds, the higher end the hotel, the more you could probably get away with here.

The front desk or concierge are there to help you in any way they can. Explain to them that you need to print your boarding pass, or tickets to an event you wish to attend. They will more than likely point you to the guest computer. Explain that you either tried it and it didn't work and you need to print, or that it is occupied (have your friend sitting at it at that moment). They will more than likely step aside and let you use their computer. BINGO. You are on an authorized computer that has access to a lot of stuff, perhaps everything. Plant a keylogger or remote access tool and move on quickly. Then come back later in the day, sit so you can see the person at the computer you infected and pretend to work on your laptop, and wait for them to step away. When they do, take over their computer with yours and do what you want until they return.

Solutions: Hotel staff are there to help and do NOT think about computer security. One of the first things we do is approach the front desk, assign a unique user name and password for each. Then identify what they need access to and lock down their user accounts. Finally, teach the staff to not allow any non-employee on their computer ever.

Common Concern #2: Network jacks in common areas are often times connected to the main hotel network. Most hotels have a separated guest and admin network that more than likely you won't penetrate. Take a peek but don't spend too much time on this as it's usually implemented well by a third party that knew better.

Look for network wall jacks around the lobby or better yet, the conference rooms. Ask to use a conference room for an interview. They will more than likely accommodate you as they are there to please. Once in the conference room, close the door, ask for privacy, and plug in. Chances are management has meetings in this room and wanted access to their files. The guest network wouldn't grant them access to their admin network, so they had IT switch one of the jacks in the room to the admin network. If you cannot find a jack that connects you to the admin network, ask the staff if there is another conference room because the temperature isn't right in the current room, or any other excuse. They may give you a funny look, but access is what you are after, not friends.

Solutions: only offices under lock and key or areas of the property that are monitored should have jacks connected to the admin network. All other jacks should be disconnected or connected to the guest network for Internet access only.

Common Concern #3: Wireless is a desire for its convenience by most. Given this, I have always seen some employees, usually at management level, purchase their own access point, plug it in to the admin network and not password protect it, or change the default.

At one prominent top 10 lodge in the world, we identified that the assistant GM purchased a wireless access point and put it under his desk. He attached it to the admin network, and kept the default password.

Solution: search for access points, identify them through DNS or wireless scan tests, and disable. Teach the staff that this is wrong, and find better ways for them to work.

Common Concern #4:

Paperwork is usually just thrown out. Dumpster diving is the key here. Very few hotels/resorts shred their paperwork. Look for the front desk or reservations department trash. That's the paperwork that will have guest info and credit card info handwritten down.

Solution: purchase shredders for every office at the property and require all paper to be shredded. Don't let them decide what to shred and not shred. Many just grab any scrap when they are on the phone and jot notes quickly to get off the phone as fast as possible.

Common Concern #5:

The PMS is the keys to the kingdom. Email lists, credit card information, special guest information is all for the taking if you get in to this system. All systems today mask the credit card info, but most hotel staff record the credit card info in the notes section of the guest in case the guest has a special request that doesn't interact with the hotel PMS. They do not need to bother the guest with asking for the same credit card info again.

Some of the hotels/resorts also have exclusive guests, where their info may be important to resell to the paparazzi or etc. Obtaining this information could net a small payday for one.

Solutions: Hotel systems need to be isolated and locked down. They should not be accessible from the outside Internet or from the guest network ever. Additionally, patches on both the OS and application level should be maintained, and system logging should be enabled to a very high degree. Finally, ensure that only users who need access have access, and that their access is limited to only the data they need access to in order to do their jobs.

Common Concern #6:

Security Camera systems are often times setup by the physical security team, and may be connected to the admin network. If there are wireless cameras, you might have an easy jump here. If the cameras are connected physically via a cat5 cable, you will need to identify if it's possible to plug in to one of the cameras or an open jack next to the camera, since most jacks are dual jacks. There is a good chance that if you unplug one, it will be seen and addressed relatively quickly, so never unplug to get access.

Solutions: Put the cameras on a third, independent network, that the guest and admin network do not have access to.

Common Concern #7:

The most popular hotel systems require java, and usually an older version. The developers of these systems do not like to update very often, as it may break their overly complicated systems. So when installing the PMS software on an employee workstation, an older version of Java is required. By using some social engineering one could exploit the old java version locally and thus owning the system.

Opera, for a long time, required a java version that was several years out of date. This is unacceptable, but the hotels/resorts are at the mercy of the vendor.

Solutions: Unfortunately, the only hope here is not Java, but to lock the system down, patch regularly, and do all the little things you should do to protect the user as best as possible. Even a proxy at the firewall level is a good idea since the user could unintentionally get infected by a drive-by web site visit. Wrap all this up with some user education on browsing on their work computer.

Common Concern #8: Support is usually on an as needed basis. So if an attacker were to plant a remote access tool, if not discovered immediately, it would probably not be discovered until something really went wrong with that system. The only time most consulting companies are called is when something is broken. They generally do not do maintenance and audits.

CBH once found a keylogger that sent off logs every week to an unknown source on an accounting computer at a hotel in Atlantic City, NJ. The kicker is that the computer was 8 years old! CBH just came on board and did a common audit and identified the software immediately. So for however long it had been there, the previous IT consultants/department never identified it.

Solutions: be sure to do a software audit on a regular basis, and hirer a qualified consulting company or one with experience in security.

Common Concern #9: The guest computer(s) are usually setup and maintained by the same people who manage the hotel network. Therefore, the local admin password more than likely is the same or similar as the one for the Admin network.

Another point is running a simple tool like Cain and Abel will display other guest information that was saved during their use to check their email or other account. Many of these computers are running as a local administrator as well, making this even easier to get information.

Also be sure to check if it's on the admin network. Chances are it isn't, but if it is, you might have fond a nice access point to it.

Solution: Run the guest computer on the guest network, do not allow it to run as an administrator, and use a kiosk or other software that will reset the computer to a specified state after a reboot.

Computer Concern #10: The key card system has been riddled with flaws since inception. No matter the system, there are inherent flaws. Today, hotels are trying to move beyond the need for a guest to even check in and have the ability to go directly to their room. In order to do this, they guest key is changing dramatically. Hilton is in the process of launching keyless room entry via an app on a smart device like your cell phone. Obviously there is usually some pain to being in the forefront of technology, and something like this might concern some.

I once witnessed an entire NY hotel in NYC with almost 200 rooms go into panic mode when the server that manages keycards went offline due to hardware failure. Of course redundancy is a concern and in my opinion common sense, but the hotel cut corners. The end result, no guest having access to their room once they left, and the hotel had to resort to pulling out the old key system. The keys were not well organized and this led to some additional chaos, as well as the point to have a disaster recovery and incident handling plan in place.

However, if an attacker were to figure out the keycard system, especially in an app that they could reverse engineer and learn, what would be the damages[3]?

Solutions: Don't be the first. Let others test the technology, and once you see a level of comfort and less pain, decide on a plan to implement.

[3] http://hospitalityrisksolutions.com/2013/03/28/hospitality-industry-crime-risks-arizona-hotel-guest-reports-2000-stolen-after-front-desk-accidently-gives-out-victims-room-key/