Client Challenge

Many organizations make use of a colocation facility to house servers and networking equipment. These data hosting providers advertise high levels of physical security, as organizations are often storing highly sensitive data. These physical controls often include a guarded front desk, security cameras, individually locked cages for each customer, and access card readers.

An organization who utilizes such a data center requested that SecureState assess whether the physical security of their colocation facility was as good as advertised. The organization was concerned with how well their provider was protecting their critical data, and if that provider was following security best practices. Additionally, they were concerned with the risks to their data if someone was able to gain physical access to their servers.

Services Rendered

SecureState performed a Physical Attack & Penetration Assessments on the data center of the hosting provider. The first step in a Physical Attack & Penetration is to perform intelligence gathering on the facility. SecureState observed all potential points of entry, including the front lobby, side access doors, and loading dock.

SecureState found that the main lobby was secured with several layers of security, including a guard and access card readers. However, noting the loading dock as an area of weakness, SecureState dressed up as maintenance workers and accessed the building through this entrance. No one questioned us, as multiple businesses used the loading dock on a daily basis. From there, we found a freight elevator we could take up to the hosting provider location. That allowed us to bypass the front guard desk and any other front line physical security controls in place.

At the reception desk outside the data center floor, SecureState was able to social engineer visitor badges by claiming to be from another company who used the space. SecureState was aided in this attack vector because the colocation bragged about who their clients were on their website, which allowed us to create fake IDs matching one of their clients. Additionally, by having bypassed the main guard, the employees at the data center were more trusting of us having a reason to be there. They assumed we had already passed the scrutiny of the main entrance.

Once SecureState gained access to the data center floor, we were able to move about unchecked. Most hosting providers have cameras at the doors that monitor who comes in and out, but once you are in (and have established a trust level) they do not really monitor where you go. SecureState was able to locate the target cage without being questioned by anyone. The cage was in fact locked, requiring a card swipe

to gain access. However, the cage also had a lock box that contained an emergency card. The box was protected by a fairly cheap lock, which we were able to easily pick.

Results and Lessons Learned

SecureState's "trophy" for this assessment was simply to gain physical access to the client's server. However, had we been actual attackers, at this point, with unchecked physical access to the server, we would have been able to perform any or all of the following attacks:

- Place a key logger on the system
- Perform a cold boot style attack to recover encryption keys or other sensitive information stored in memory
- Remove and create images of the hard drives
- Install malicious hardware which could monitor and tamper with the system

Conclusion

Colocation facilities make an effort to prevent physical access to your organization's data. However, as SecureState demonstrated, a skilled and dedicated attacker can still gain this access fairly easily. Once someone has physical access to a data center, there really are not many effective controls to stop someone. Since colocations are typically 3rd party, many of the common personnel controls of an office are not in effect. The workers do not know you, and they do not know who should or should not be there. The building that housed the data center shared space with multiple companies, presenting additional security challenges.

Also, people's actions are not very tight monitoring of once inside the main facility. Your organization should not solely rely on these controls to protect your confidential data. Additional protections on your servers may help mediate some of the risk if your servers fall into the wrong hands.

About SecureState

SecureState is an information security management consulting firm that is devoted to guiding our clients into the best strategic security practices. Our team has the expertise to engage clients from diverse industry verticals through the entire security lifecycle. Well respected industry leaders have trusted the design, implementation, and management of their information security architecture to SecureState's team. SecureState draws upon the skill sets of its team members, and their extensive experience in government, private-sector, and Big X consulting companies. The SecureState team is comprised of six specialties: Advisory, Audit & Compliance, Incident Response, Profiling, Research & Innovation, and Risk Management.