Case Study: Physical Pentest, Healthcare

Client Challenge

A healthcare organization requested that SecureState assess the physical security of their data center, and that of a specific server in the data center. The server was used by a research group and housed proprietary research data and thousands of patient records containing Protected Health Information (PHI). The organization was concerned with maintaining the confidentiality of that data, as well as meeting HIPAA compliance requirements. The data had already been assessed to have low potential for access from an external attack, but how secure would it be if an attacker achieved physical access to the server?

Services Rendered

SecureState performed a Physical Attack & Penetration Assessments on the data center of the healthcare organization. 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 and side access doors. Finding side doors properly secured, SecureState attempted to use Social Engineering techniques to get past the front desk. When that proved unsuccessful, we continued to observe the building.

SecureState watched the receptionist leave at 5:00p.m. After observing that no one else seemed to be around the front entrance, we tried to open front doors, which proved to be unlocked. SecureState later learned that these doors didn't automatically lock until 5:30. This gave us initial access to the building. Through searching the reception area, we discovered a locked metal key box mounted on the wall behind the front desk, which we were able to lock pick. After picking the lock, the team found that it housed all the different keys to the building. After grabbing a handful of keys, they were able to find the master key that opened all the doors within the entire building.

We were able to use this to bypass card readers and other locks in getting to the data center. However, the master key did not work on the data center door. Through observation, SecureState noted that the walls to the data center did not have six-wall integrity. This allowed a team member to remove a ceiling tile and crawl over the wall, circumventing all security controls. The first person then let the rest of the team in from the inside.

Once inside, we then located the server of interest, which was an Apple server. Although we found the console to the server, no obvious passwords were posted on it or left around. Luckily, Apple servers have FireWire ports, through which we could launch more advanced attacks on the server. In connecting a laptop, we were able use the Inception tool to dump and manipulate the memory from the server through the FireWire port, which gave us access to sensitive information on the server.

Results and Lessons Learned

As a result of this engagement, SecureState achieved full access to the building, the data center, the target server, and achieved full compromise of the server. The server contained thousands of patient records and other PHI. Such a breach would leave the client in violation of HIPAA laws and lead to potential fines and loss of patient confidence.

Once SecureState had physical access to the device, we achieved full compromise in a matter of minutes. The entire physical attack on the building took under an hour, and we were able to leave without detection. There were no alarm systems triggered, despite bypassing multiple card readers with the master key. Because we were able to open the data center door from the inside, it read it as a legitimate exit. Even though there were cameras in several areas, no one stopped the team's activities, which lead us to the conclusion that these cameras were either not monitored, or not turned on.

Conclusion

Even though the server was in what was thought to be a highly secure data center, it was not that secure at all. Once we had access to the device, we were able to very easily dump the memory through the port, read that data, and gain credentials to access to a significant amount of proprietary research data and protected PHI.

Almost any set of physical security controls will have weaknesses that can be exploited. In addition to technology, SecureState uses social engineering techniques to gain access to your company. We realize that humans play the most important role in securing your organization's data; however, they are usually the weakest link. Your organization should not depend solely on personnel 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.