CASE STUDY: PHYSICAL ATTACK AND PENETRATION ASSESSMENT

Situation

On a recent engagement, RSM worked with a large manufacturing organization to identify weak points within its physical security program. This particular organization maintains a very open, trusting internal culture. There are no cameras in the corporate offices or on the manufacturing lines within their facilities, as the administrative team wishes to avoid any semblance of Big Brother. This attitude puts a particular emphasis on perimeter security as well as the security awareness training of individual employees.

In addition to general employee safety, the organization’s primary concern was the integrity of their product. Attackers who are able to reach the production line or final packaging areas would have the ability to tamper with or destroy products. This could both harm customers and severely damage the reputation of the brand. Thus, the challenge was to find a way to protect the organization without destroying its culture.

Solution

To meet this need, we performed a physical attack and penetration test against the target facility. During this type of engagement, our security experts attempt to gain physical access to a target facility using any means necessary, while drawing as little attention as possible. Our team members take advantage of any and all weaknesses present within the organization’s security program to simulate how an attacker would attempt to access sensitive areas and specific targets.

During the remote and on-site reconnaissance phases of this particular engagement, several important factors were noted and later exploited by the team:

• Remote reconnaissance: Our team makes extensive use of publicly available mapping software and websites to identify potential gaps in perimeter security. In this case, an open fence gate leading to a train yard adjacent to the target was observed. Google Earth, specifically, allows for the searching of historical map data going back as far as twenty years; the gate appeared to have been left open in all historical maps as well.


Onsite reconnaissance: Under cover of darkness, our team was able to approach the facility via the adjacent train yard and confirm that the gate in question was left open. Additionally, despite the low level of activity at the site given the late hour, the cover provided by the trains in the yard permitted the team to sit for an extended period of time and observe a number of employees enter and exit the facility without the use of keys or radio-frequency identification (RFID) badges.

Our team then used this information during the attack phase of the assessment. One consultant posed as an employee and approached the facility through the open gate. Once on site, the consultant moved directly to the door through which the employees had been seen entering and exiting the plant. Despite having been seen by multiple employees, the consultant was not approached or stopped. After entering the plant, the consultant had unfettered access to the manufacturing line and clearly labeled crates of finished product ready for shipment.

After the success of the first breach, two other team members were able to repeat the process and gain additional access to plant resources, including unlocked computers used to control manufacturing equipment on the line. It should be noted that while exiting the premises, the team noted two additional gates in the perimeter fence that, while locked, were not properly secured to the ground. Both could be opened enough to allow for a person to pass through with ease.

Results

Based on the results of this assessment, we developed several suggestions for improving the security and safety of the organization’s facility. Our immediate tactical recommendations centered largely on the improvement of perimeter security. Those gates flagged during the assessment should have been closed, locked and properly secured. The plant door through which the team entered the line included a badge reader, but the reader itself had been disabled for the sake of convenience.

Based on our strategic recommendations, the organization is in the process of rolling out a newly revamped security awareness training program. Such an investment is an effective way to address some of the issues identified during the physical attack and penetration test without necessitating a complete cultural shift. This training highlights the potential dangers to employees and product rather than delivering a simple checklist of do’s and don’ts. Additionally, a formalization of incident response policies and the appropriate dissemination of those policies will help to prevent similar breaches from occurring in the future.

While technological solutions are important, physical security is at its strongest when an organization’s people, processes and technology are all in alignment.

In seeking to protect its brand name and ensure customer and employee safety, the client focused on the physical security of its manufacturing locations. Our physical attack and penetration assessment demonstrated the importance of maintaining strong perimeter controls and comprehensive security awareness training. By developing recommendations that met the client’s need without requiring significant internal cultural change, RSM helped to balance the strength of the people, processes and technology to improve the client’s overall physical security posture.