Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:
Red Team Exercise

caseStudy

How a large gas industry organisation ensured security policy adherence with a red team exercise

The Requirement

A large UK based gas industry group wanted to ensure that it was not at risk of a physical security breach, specifically concerned with tailgating or piggybacking, across its three main UK sites.

The group needed to ensure that employees across the entire organisation were adhering to its no tailgating policy. This was an explicit contractual obligation and policy that all employees in the group had to sign.

The group had identified that a physical red team assessment was needed to protect themselves against any potential breaches. It also wanted to understand any other potential risks and validate its internal escalation process as part of the overall exercise.

The group selected DigitalXRAID as its security partner to conduct the red team exercise.

The Solution

The entire scope was primarily focused on the physical aspect of the red team exercise, with a key objective for the DigitalXRAID team to test the ability to gain access to each of the three main UK sites.

The first phase of the red team exercise was to perform reconnaissance on all three sites. This included understanding where all security cameras and gates were located.

Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

caseStudy

External factors such as the weather had to be taken into account as these could positively or negatively affect the ability to gain access and could even provide an attack method.

The DigitalXRAID team spent time understanding general staff routines around the morning, lunchtime and the evenings to see if an attack could be attempted during any of these periods.

The first attack attempt tried to access the main entrance of one of the sites, however the team were denied access on entry.
The second site attempt took a different attack method. This building had a fully operational security desk at the main driveway entrance so it would be impossible to enter at this point. However, there was a gate with a gap large enough to access at the back of the building. The team spent time in communal areas until a member of staff entered the building and they were able to gain access by tailgating.

Once inside the second site, the team tested access policies from inside the building, spending time moving through kitchens, training rooms and other office areas and even setting up in a director's office for a meeting – all of which went unquestioned against the group's internal escalation policies.

The final site was the most secure of all sites as it had an area with direct access to central government systems. Through the reconnaissance phase, the team had identified that the best time to attempt access was at lunchtime, when staff were more likely to be caught off guard. By imitating a phone call on entering the building, staff held the door open, allowing the team to tailgate with no issues on entry.

Once inside the building, the DigitalXRAID team located the area of the office that had direct access to the high security government link. By pretending to be printer maintenance workers with a USB stick in hand, attending on site to upgrade printer firmware, the team were allowed entry to the high security area, with all their mobile devices, which was against internal policies.

Red Team Exercise - Case Study

Service:

Red Team Exercise

With time on the final day of the test, the team were able to revisit the first site and reattempt access as staff were leaving the building at the end of the working day. On this second attempt, the team were let into the building by staff on their way out.

The entire red team exercise was filmed using discrete body worn cameras, so every step was recorded without the need to stop and take photos during attack attempts.

The Results

The red team exercise was successful with all objectives completed. The gas industry organisation group is now able to understand the level of adherence with internal security policies across its employees, as well as other potential risks highlighted during the red team exercise.

On top of the objectives, the recording of the engagement allowed the DigitalXRAID team to offer additional advice on where there were risks of data potentially being publicly exposed.

The group can address all risks and make sure that it is fulfilling all contractual obligations under its no tailgating policy, including additional security and policy training and fixes to building security.

To see how DigitalXRAID could help you protect your systems, applications and data, get in touch with us today!