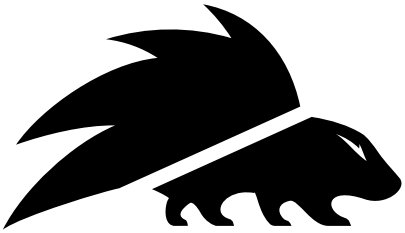

RED TEAMERS

PHYSICAL PENETRATION TEST

Case Study

RED TEAMERS

Our mission is to spotlight vulnerabilities and weaknesses, both in the digital and physical realms. With two decades of experience, we shed light on potential risks, guiding clients to take informed actions. We're your trusted partner in understanding and addressing security concerns, helping you safeguard what matters most.

Author: Jiří Vaněk, Chris Cowling

Date: 05/09/2025

Version: 20250905-01

Confidentiality: public

Benya IT s.r.o.
sady Pětatřicátníků 173/31
301 00 Plzeň

ID: 26414660
VAT: CZ26414660
Registered: Regional Court in Pilsen, C 18712

www.redteamers.eu
sales@benya.cz
+420 603 798 952

1 CONTENT

2 PHYSICAL PENETRATION TEST AT A TIER-1 EUROPEAN INSURANCE COMPANY

2.1 Background

A Tier-1 European insurance company engaged our red team to perform a **comprehensive physical penetration test**. The exercise was commissioned both as part of ongoing regulatory compliance (DORA, NIS2) and to address concerns raised by the CSO regarding the effectiveness of physical security measures.

The scope included:

- **Passive reconnaissance** – collecting information using OSINT techniques.
- **Active reconnaissance & surveillance** – confirming gathered intelligence on-site.
- **Exploitation** – attempting covert entry into the target building and restricted areas.
- **Post-exploitation** – deploying covert surveillance simulators and collecting sensitive information.

2.2 Objectives

1. Assess physical security controls preventing unauthorised access to sensitive areas.
2. Evaluate employee resilience against physical intrusion and social engineering attacks.
3. Provide actionable recommendations to strengthen both technical and procedural defences.

2.2.1 Phase 1 – Passive Reconnaissance

Open-source intelligence revealed a surprising level of detail about the facility:

- Exact **camera placements, angles, and blind spots** outside the headquarters.
- **Building entrances** and likely locations of elevators and stairwells.
- Information on the **public café and canteen** within the building, including opening hours.
- Layout of the **lobby and reception area**.
- **Access badge design** obtained from social media.
- Several photos showing employee workplaces.

This demonstrated that the company's **attack surface extended far beyond its walls** – much could be pieced together from public information.

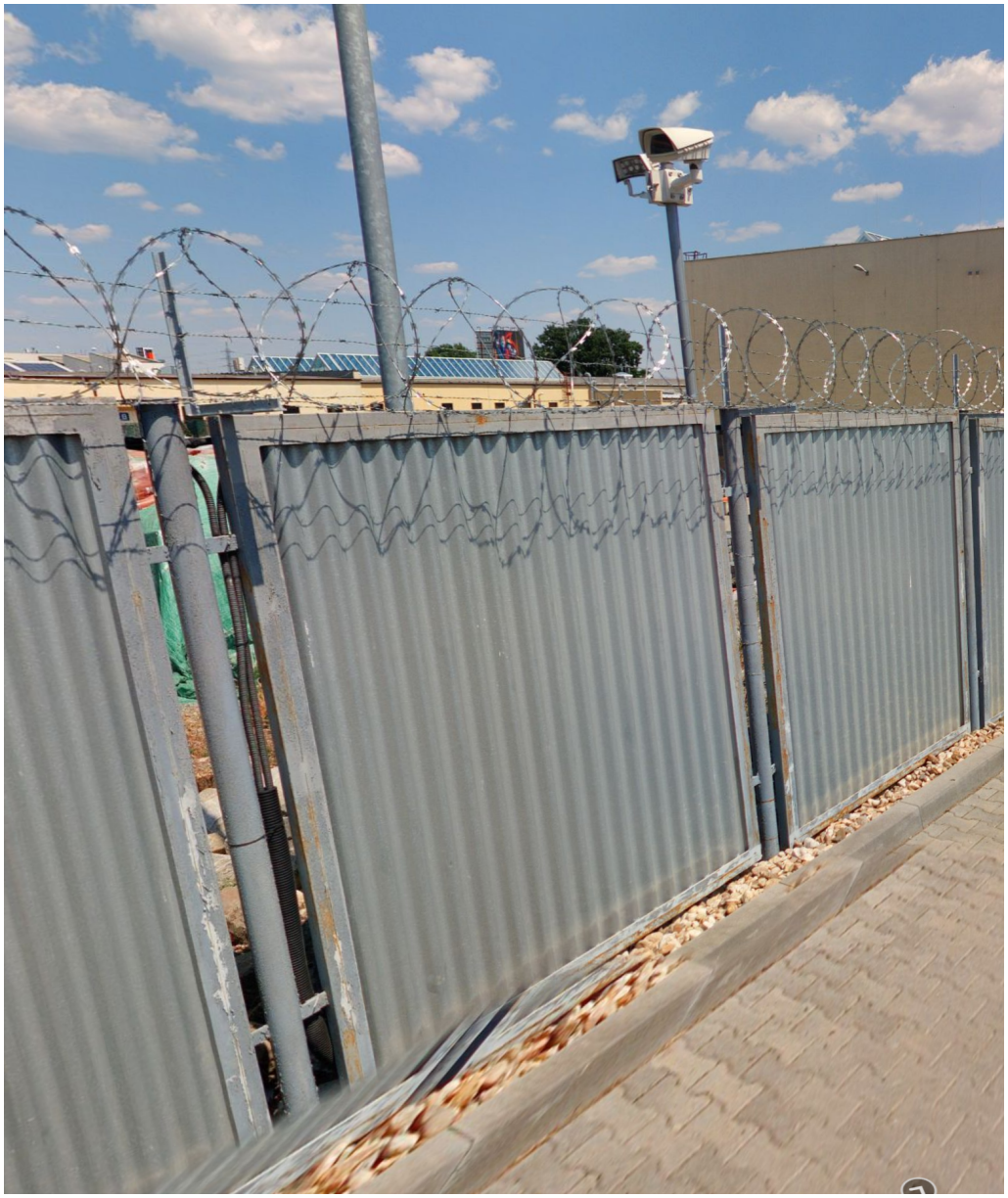

Fig. 1 – a camera with infrared light.

2.2.2 Phase 2 – Active Reconnaissance & Surveillance

On-site surveillance confirmed and expanded these findings:

- Identified **locks' manufacturer and model type**.
- Obtained **floorplans** of publicly accessible floors from emergency evacuation plans.
- Verified **access card designs** by photographing employees from a distance.
- Noted use of **multiple lanyard colours**, making blending in trivial.
- Mapped **camera coverage and blind spots** within the lobby.
- Observed **lax behaviour of guards**, especially during shift changes.

- Tested reception:
    - Receptionists asked for ID but accepted excuses, issuing visitor badges after only a surname check.
    - Visitor badges could be cloned due to insecure card technology.

The team also confirmed the café and canteen provided ideal proximity for **cloning cards**. No alarm sensors were identified anywhere in public or semi-restricted areas.

Fig. 2 – clone of a visitor's badge.

2.2.3 Phase 3 – Exploitation

Based on reconnaissance, three intrusion scenarios were defined:

1. **Cloning employee badges** in the café, canteen, or lobby using a long-range reader (~70 cm).
2. **Tailgating** behind employees and attempting opportunistic badge cloning.
3. **Social engineering reception** by impersonating an employee who lost their card.

Attack vector **#1 (cloning badges)** proved the most effective. Multiple functional clones were created and tested successfully across several restricted areas.

Using these, the red team:

- Accessed multiple office floors.
- Placed **surveillance simulators** (dummy listening devices) in meeting rooms, phone booths, and workplaces.
- Prepared for the main objective – gaining access to the **executive floor**.

Fig. 3 – placed surveillance simulators (grey boxes) in multiple meeting rooms.

2.2.4 Phase 4 – Post-Exploitation

With cloned badges, the team entered the **executive floor** unnoticed.

- **COO's office:** locked; picked open in ~60 seconds. Photos were taken, and a symbolic team flag (company mascot) was placed.
- **CEO's office:** accessed even faster via lock-picking; again, photos and flag placement.
- **Boardroom:** older, worn lock – picked in under two minutes. Surveillance simulator placed and documented.

Fig. 4 – placed surveillance simulator in the Board room and picked open the lock on the CEOs office.

To test human vigilance, the team conducted an additional **bold social engineering attempt**:

- A deepfaked voice of the COO instructed reception to issue visitor badges to "auditors."
- Reception complied, granting badges with executive floor access.
- Although reception later phoned the executive floor to verify, the "auditors" were never intercepted and even enjoyed coffee at the café before leaving through a side exit, unchallenged.

2.3 Results

Successes:

- Offices of executives were locked after hours.
- Reception eventually attempted verification (but too late).

Weaknesses:

- Obsolete access card technology easily cloned.
- Guards and receptionists insufficiently trained, repeatedly allowing tailgating and unauthorised entry.
- Employees frequently held doors open for strangers.
- Locks protecting executive offices could be picked in seconds.
- No alarm system in sensitive areas.

2.4 Outcome & Recommendations

The exercise demonstrated that the company's **security model was perimeter-oriented**: once inside, there were virtually no obstacles preventing an attacker from escalating access to the most sensitive areas.

Recommendations included:

1. **Upgrade physical access control system (PACS)** to a secure standard resistant to cloning.
2. **Comprehensive training** for guards, receptionists, and staff to identify and handle suspicious behaviour.
3. Replace locks in executive and sensitive areas with **high-security cylinders**.
4. Implement **intrusion detection/alarm systems** in executive offices, boardrooms, and data-sensitive zones.
5. Establish a **regular red-team/penetration testing cycle** to validate improvements.

2.5 Business Value

The exercise provided the Board and regulators with tangible assurance that security controls were being realistically tested against a determined adversary. By simulating a real-world attack chain, the company:

- Identified critical blind spots in its physical security posture.
- Strengthened resilience against both insider and outsider threats.
- Aligned its physical security testing with broader **NIS2 and operational resilience requirements**.

The result was a clear, prioritised roadmap for closing the gap between paper policy and real-world defence.