# Fallstudie 1: Schweizer Industrieunternehmen – Sicherheitsstrategie & Segmentierung

## Ausgangslage

Ein mittelgrosses Schweizer Industrieunternehmen mit Produktion und Büro-IT auf einem gemeinsamen Netzwerk stand vor einem klassischen, aber gefährlichen Problem: Es gab keine Trennung zwischen den operativen Systemen in der Produktion und der regulären Office-Umgebung. Ein einziger kompromittierter Arbeitsplatz hätte potenziell die gesamte Produktionslinie lahmlegen können. Die Geschäftsleitung wusste, dass Handlungsbedarf bestand – hatte aber weder den internen Know-how-Träger noch eine klare Vorstellung davon, wie eine Lösung aussehen könnte.

## Mein Beitrag

Ich begleitete die Geschäftsleitung und das interne IT-Team als **strategischer Sparringpartner** – nicht als Umsetzer. In Workshops analysierte ich zunächst die bestehende Netzwerktopologie und identifizierte die kritischen Übergangspunkte zwischen Produktion und Büro-IT. Darauf aufbauend entwickelte ich eine **Zero-Trust-orientierte Segmentierungsstrategie**, die den spezifischen Anforderungen des Unternehmens entsprach.
Entscheidend war dabei nicht nur das technische Konzept: Ich führte Gespräche mit den Produktionsleitern, um deren Arbeitsabläufe zu verstehen und sicherzustellen, dass die Segmentierung den Betrieb nicht behindert. Die Umsetzung übernahm anschliessend das interne Team zusammen mit einem lokalen Integrator – auf Basis meines Architekturplans.

## Ergebnis

- **Risiko deutlich reduziert:** Produktion und Büro-IT vollständig segmentiert – ein Angriff in der einen Zone kann die andere nicht mehr direkt erreichen.
- **Interne Kompetenz gestärkt:** Das IT-Team verstand die Architekturentscheidungen und konnte sie eigenständig weiterentwickeln.
- **Kein Vendor-Lock-in:** Die Lösung wurde herstellerneutral konzipiert, was langfristige Flexibilität sicherte.