REFERENCE

CYBERSECURITY SERVICES

GREY-BOX PENETRATION TEST & COMPREHENSIVE SECURITY ASSESSMENT

KISTLER

STRONG SECURITY THROUGH REGULAR TESTING

myKistler is a smart, user-friendly e-commerce platform that provides customers with access to product details, pricing, and order processing. As part of its cybersecurity strategy, the Kistler Group regularly carries out penetration tests to identify and address potential vulnerabilities in its customer portal. SPIE ICS was commissioned to conduct an upcoming grey-box penetration test to support Kistler in its goal of further minimising the risk of security breaches.

THE CHALLENGE

Platforms like myKistler are typically subjected to regular internal and external security tests. In addition, the Kistler Group's security concept is based on a rotation approach, meaning that different external cybersecurity partners and testing methods are employed. As a result, obvious security gaps are often already closed. Therefore, SPIE ICS aimed to identify potential vulnerabilities that had previously gone unnoticed by others.

Key Challenges Included:

- **The Grey Box:** Only limited access and user rights to the platform were available.
- **Requirement for a Staging Environment:** To ensure uninterrupted business operations for myKistler's customers and protect backend systems, the penetration test had to be conducted in a dedicated, realistic test environment.
- **Strict Timeframe:** Preparations and test procedures had to be perfectly planned.

KISTLER

measure. analyze. innovate.

Founded in 1959 and headquartered in Winterthur, Kistler is now a globally active group of companies and the world market leader in dynamic measurement technology. With around 2,000 employees at more than 60 locations, Kistler makes a significant contribution to the advancement of current industry trends, reduction of CO_2 emissions, and Industry 4.0.

Kistler holds around 860 patents and invests an average of 9% of its annual turnover of 424 million Swiss francs (as of 2025) in research and development.

A COMPREHENSIVE SOLUTION THROUGH DIVERSE TESTING

SPIE ICS used 20 specialized analysis tools and relied on recognized best practices and methodologies according to OWASP (Open Web Application Security Project). For example, more than 42,000 automated individual tests were performed on myKistler's API endpoints using a single tool. In addition, the use of a grey-box testing approach allowed for the simulation of realistic cyberattack scenarios, even those involving potential insider knowledge.

Only such a comprehensive approach made it possible to systematically analyze the security and stability of the various platform interfaces in order to identify a wide range of potential vulnerabilities. This enabled Kistler to receive an industry-standard and detailed security assessment of its e-commerce platform, providing both technical recommendations and visibility into the operational risks associated with security vulnerabilities.

> "The security assessment provided us with concrete, actionable recommendations as well as a transparent evaluation of business risks. We were particularly impressed by the depth of expertise, the realistic attack scenarios, and the clear, comprehensible presentation of the results."
>
> **Kistler**

PROJECT WORKFLOW

To ensure adherence to the strict time constraints from the outset, the cybersecurity experts at SPIE ICS defined a clear process:

1. **Preparation Phase:** Definition of goals, scope, and logistics in coordination with key stakeholders
2. **Information Gathering:** Collection of technical and organisational information to assess the current security status and attack surface
3. **Threat Modeling:** Identification of critical system resources and likely attack scenarios targeting myKistler
4. **Vulnerability Analysis:** Detection of potential security gaps using both automated and manual testing methods
5. **Exploitation:** Controlled exploitation of vulnerabilities to validate security risks and reveal their potential impact

The development of a detailed information base was particularly instrumental in enabling a comprehensive security analysis and assessment.

MEASURABLE RESULTS

- **Comprehensive assessment** of the security posture of myKistler documented in a 79-page report
- **Concrete recommendations** for the technical teams to address security deficiencies
- **Clear presentation** of security risks, enabling decision-makers to understand the business impact

SPIE ICS AG is your independent service partner in Switzerland for cybersecurity solutions.

Contact us to benefit from our expertise and learn more about our services and solutions:

info.ch@spie.com

spie.ch/cybersecurity-services