REFERENZ

CYBERSECURITY SERVICES

GREY-BOX-PENETRATIONSTEST & UMFASSENDE SICHERHEITSBEWERTUNG

KISTLER

STARKE SICHERHEIT DURCH REGELMÄSSIGE TESTS

myKistler ist eine smarte, benutzerfreundliche E-Commerce-Plattform, über die Kunden Zugang zu Produktdetails, Preisen und Bestellabwicklungen erhalten. Im Rahmen ihrer Cybersecurity-Strategie führt die Kistler Gruppe regelmässig Penetrationstests durch, um potenzielle Schwachstellen ihres Kundenportals zu identifizieren und zu beheben. SPIE ICS wurde für einen anstehenden Grey-Box-Penetrationstest beauftragt, um Kistler bei seinem Ziel zu unterstützen, das Risiko von Sicherheitsverletzungen weiter zu minimieren.

DIE HERAUSFORDERUNG

Plattformen wie myKistler werden zumeist regelmässig internen und externen Sicherheitstests unterzogen. Das Sicherheitskonzept der Kistler Gruppe setzt zudem auf einen Rotationsansatz, sodass verschiedene externe Cybersecurity-Partner und Testmethoden zum Einsatz kommen. Offensichtliche Sicherheitslücken sind also oft bereits geschlossen. Der Anspruch von SPIE ICS war es deshalb, potenzielle Schwachstellen zu identifizieren, die andere bisher übersehen hatten.

Besondere Hürden waren:

- **Die Grey-Box:** Es standen nur eingeschränkte Zugänge und Benutzerrechte der Plattform zur Verfügung.
- **Notwendigkeit einer Staging-Umgebung:** Damit der laufende Geschäftsbetrieb von myKistler für Kunden ungestört und Backend-Systeme geschützt bleiben, musste der Penetrationstest in einer speziellen, realitätsnahen Testumgebung durchgeführt werden.
- **Das strikte Zeitbudget:** Die Vorbereitungen und Abläufe des Tests mussten perfekt geplant werden.

KISTLER

measure. analyze. innovate.

Gegründet 1959 und mit Hauptsitz in Winterthur ist Kistler heute eine weltweit agierende Unternehmensgruppe und Weltmarktführer im Bereich der dynamischen Messtechnik. Mit rund 2'000 Mitarbeitenden an mehr als 60 Standorten leistet Kistler einen bedeutenden Beitrag zur Weiterentwicklung aktueller Branchentrends, zur Reduktion von CO_2-Emissionen und zur Industrie 4.0.

Kistler hält rund 860 Patente und investiert im Schnitt jährlich 9% seines Umsatzes von 424 Millionen Franken (Stand 2025) in Forschung und Entwicklung.

EINE UMFASSENDE LÖSUNG DURCH TESTVIELFALT

SPIE ICS setzte 20 spezialisierte Analysetools ein und orientierte sich an anerkannten Best Practices und Methoden gemäss OWASP (Open Web Application Security Project). Beispielsweise konnten mit einem einzigen Tool über 42'000 automatisierte Einzeltests an den API-Endpunkten von myKistler durchgeführt werden. Und durch den Einsatz eines Grey-Box-Testverfahrens konnten realitätsnahe Szenarien von Cyberangriffen simuliert werden, die auch mögliches Insiderwissen miteinschlossen.

Erst ein solch umfassender Lösungsansatz ermöglichte eine systematische Analyse der Sicherheit und Stabilität der verschiedenen Plattform-Schnittstellen, um eine breite Vielfalt potenzieller Schwachstellen identifizieren zu können. So konnte Kistler eine branchenkonforme und detaillierte Sicherheitsbewertung seiner E-Commerce-Plattform erhalten, die sowohl technische Empfehlungen gibt als auch Geschäftsrisiken durch Sicherheitslücken sichtbar macht.

> „Die Sicherheitsbewertung lieferte uns konkrete, umsetzbare Empfehlungen sowie eine transparente Einschätzung der Geschäftsrisiken. Besonders überzeugt haben uns die fachliche Tiefe, die praxisnahen Angriffsszenarien und die klare, verständliche Aufbereitung der Ergebnisse."
>
> **Kistler**

PROJEKTABLAUF

Um die Einhaltung des strikten Zeitbudgets von Anfang an zu gewährleisten, definierten die Cybersecurity-Experten von SPIE ICS einen konkreten Ablauf:

1. **Vorbereitungsphase:** Festlegung der Ziele, des Umfangs und der Logistik mit den wichtigsten Stakeholdern
2. **Informationsbeschaffung:** Sammlung technischer und organisatorischer Informationen zur Erfassung der aktuellen Sicherheitslage und Angriffsfläche
3. **Bedrohungsmodellierung:** Identifizierung kritischer Systemressourcen und wahrscheinlicher Angriffsszenarien auf myKistler
4. **Schwachstellenanalyse:** Erkennen von potenziellen Sicherheitslücken durch automatisierte und manuelle Testmethoden
5. **Exploitation:** Kontrollierte Ausnutzung von Schwachstellen, um Sicherheitsrisiken zu validieren und deren Auswirkungen sichtbar zu machen

Besonders der Aufbau einer detaillierten Informationsbasis trug massgeblich dazu bei, die Sicherheitsanalyse und -Bewertung vollumfänglich vornehmen zu können.

MESSBARE ERGEBNISSE

- **Umfassende Bewertung** der Sicherheitslage von myKistler in einem 79-seitigen Bericht
- **Konkrete Empfehlungen** für die Technik-Teams zur Behebung von Sicherheitsmängeln
- **Klare Darstellung** der Sicherheitsrisiken, damit Entscheidungsträger die geschäftlichen Auswirkungen verstehen können

SPIE ICS AG ist Ihr unabhängiger Servicepartner in der Schweiz für Lösungen rund um Cybersecurity.

Kontaktieren Sie uns, um von unserer Expertise zu profitieren und erfahren Sie mehr über unsere Services und Lösungen:

info.ch@spie.com

spie.ch/security-services