RÉFÉRENCE

SERVICES CYBERSÉCURITÉ

TEST D'INTRUSION GREY-BOX & ÉVALUATION DE SÉCURITÉ COMPLÈTE

KISTLER

SÉCURITÉ RENFORCÉE GRÂCE À DES TESTS RÉGULIERS

myKistler est une plateforme e-commerce intelligente et conviviale qui permet aux clients d'accéder aux détails des produits, aux prix et au traitement des commandes. Dans le cadre de sa stratégie de cybersécurité, le groupe Kistler réalise régulièrement des tests d'intrusion afin d'identifier et de corriger les éventuelles vulnérabilités de son portail client. SPIE ICS a été mandatée pour effectuer un prochain test d'intrusion grey-box, afin d'aider Kistler à atteindre son objectif de minimiser encore davantage le risque de violations de sécurité.

LE CHALLENGE

Les plateformes telles que myKistler font généralement l'objet de tests de sécurité internes et externes réguliers. Le concept de sécurité du groupe Kistler repose en outre sur une approche par rotation, faisant appel à divers partenaires externes spécialisés en cybersécurité, ainsi qu'à différentes méthodes de test. Les failles de sécurité évidentes sont donc souvent déjà corrigées. L'objectif de SPIE ICS était ainsi d'identifier des vulnérabilités potentielles qui auraient pu passer inaperçues jusqu'à présent.

Les défis particuliers étaient les suivants :

- **La grey-box** : seuls des accès limités et des droits utilisateur restreints à la plateforme étaient disponibles.
- **Nécessité d'un environnement de staging** : afin de garantir le bon fonctionnement de myKistler pour la clientèle et de protéger les systèmes backend, le test d'intrusion devait être réalisé dans un environnement de test spécifique et réaliste.
- **Le budget temps strict** : la préparation et le déroulement du test devaient être parfaitement planifiés.

KISTLER

measure. analyze. innovate.

Fondé en 1959 et basé à Winterthour, Kistler est aujourd'hui un groupe d'envergure mondiale et le leader du marché dans le domaine de la technique de mesure dynamique. Avec environ 2'000 collaborateurs répartis sur plus de 60 sites, Kistler contribue de manière significative à l'évolution des tendances actuelles du secteur, à la réduction des émissions de CO_2 et à l'Industrie 4.0.

Kistler détient environ 860 brevets et investit en moyenne 9% de son chiffre d'affaires de 424 millions de francs (état 2025) chaque année dans la recherche et le développement.

UNE SOLUTION COMPLÈTE GRÂCE À LA DIVERSITÉ DES TESTS

SPIE ICS a utilisé 20 outils d'analyse spécialisés et s'est appuyé sur les bonnes pratiques et méthodes reconnues selon l'OWASP (Open Web Application Security Project). Par exemple, un seul outil a permis de réaliser plus de 42'000 tests automatisés sur les points de terminaison API de myKistler. De plus, l'utilisation d'une approche de test grey-box a permis de simuler des scénarios réalistes d'attaques informatiques, y compris avec des connaissances internes potentielles.

C'est seulement grâce à une telle approche globale qu'il a été possible d'analyser systématiquement la sécurité et la stabilité des différentes interfaces de la plateforme, afin d'identifier une large variété de vulnérabilités potentielles. Kistler a ainsi pu obtenir une évaluation de sécurité détaillée et conforme aux standards du secteur pour sa plateforme e-commerce, comportant à la fois des recommandations techniques et une visibilité sur les risques opérationnels liés aux failles de sécurité.

> « L'évaluation de la sécurité nous a fourni des recommandations concrètes et réalisables ainsi qu'une appréciation transparente des risques métiers. Nous avons particulièrement été convaincus par la profondeur de l'analyse, la pertinence des scénarios d'attaque réalistes et la présentation claire et compréhensible des résultats. »
>
> **Kistler**

DÉROULEMENT DU PROJET

Afin de garantir dès le départ le respect strict du budget temps, les experts en cybersécurité de SPIE ICS ont défini un déroulement précis :

1. **Phase de préparation** : définition des objectifs, du périmètre et des aspects logistiques avec les principaux stakeholders.
2. **Collecte d'informations** : rassemblement d'informations techniques et organisationnelles afin d'évaluer la situation de sécurité actuelle et la surface d'attaque.
3. **Modélisation des menaces** : identification des ressources système critiques et des scénarios d'attaque probables ciblant myKistler.
4. **Analyse des vulnérabilités** : détection des failles potentielles à l'aide de méthodes de tests automatisées et manuelles.
5. **Exploitation** : exploitation contrôlée des vulnérabilités afin de valider les risques de sécurité et de rendre visibles leurs conséquences.

La constitution d'une base d'informations détaillée a particulièrement contribué à permettre une analyse et une évaluation de la sécurité exhaustives.

RÉSULTATS MESURABLES

- **Évaluation complète** de la situation de sécurité de myKistler dans un rapport de 79 pages.
- **Recommandations concrètes** pour les équipes techniques afin de corriger les défaillances de sécurité.
- **Présentation claire** des risques de sécurité pour permettre aux décideurs de comprendre les impacts sur l'activité.

SPIE ICS SA est votre partenaire de service indépendant en Suisse pour toutes les solutions liées à la cybersécurité.

Contactez-nous pour bénéficier de notre expertise et découvrez nos services et solutions :

info.ch@spie.com

spie.ch/services-securite