ÉTUDE DE CAS CLIENT

ÉTAT DES LIEUX EN CYBERSÉCURITÉ POUR ODONATECH, ÉDITEUR D'UNE SOLUTION LOGICIELLE À DESTINATION DES INSTITUTIONS FINANCIÈRES

- **Audits cybersécurité et RGPD**
- Étude et installation d'équipements de sécurité
- Pratiques de développement sécurisé
- Gouvernance de sécurité et de conformité
- RSSI et DPO externalisés
- Formation et sensibilisation

CYBERSECURA
Cybersécurité & Conformité

ÉTATS DES LIEUX POUR UN LOGICIEL FINANCIER - CAS CLIENT

ACTIVITÉ

- Solutions logicielles à destination des institutions financières, courtiers, réseaux de banques, etc.
- Montbonnot Saint Martin (38), Isère
- TPE (-10 employés)
- 2020

Le besoin

L'entreprise avait besoin d'un rapport afin de démontrer à leurs clients que leur solution était bien sécurisée.

Besoin d'un état des lieux afin d'évaluer la sécurité de cette fonctionnalité. Les résultats de cet état des lieux ont permis de mettre en avant certains besoins de sécurisation de la solution.

La solution

Travail de sécurisation de l'application et de ses fonctionnalités afin d'en limiter les vulnérabilités.

- 1/2 journée de test ;
- présentation des contres-mesures à mettre en place ;
- application des contre-mesures par les équipes d'Odonatech ;
- réalisation d'un nouvel audit pour vérifier la bonne implémentation des contres-mesures.

Le(s) résultat(s)

Présentation du rapport aux clients d'Odonatech.

Grâce à l'audit mené par CyberSecura, Odonatech peut maintenant rassurer ses clients quant à la sécurité de leurs produits et des données clients.

Intervenants et méthodes

- Framework OWASP et guides OWASP (pour les tests applicatifs).
- Consultante senior en cybersécurité, certifiée ISO/IEC27001 Lead Implementer.
- Méthodologie d'état des lieux développée en interne par CyberSecura.

STÉPHANE DOTHEE

CEO chez Odonatech

Quels éléments appréciez-vous le plus dans la solution apportée par CyberSecura ?

“La rapidité, la réactivité des équipes, et la proximité.”

Pourquoi avoir choisi CyberSecura ?

“Pour deux raisons principales : tout d’abord le professionnalisme reconnu de CyberSecura, et deuxièmement la proximité de nos deux entreprises.”

Le mot de la fin

"Nous avons choisi de confier cette mission à CyberSecura pour son professionnalisme reconnu, et pour la proximité de nos deux entreprises. [...]. Nous avons particulièrement apprécié la réactivité des équipes."

LES SERVICES D'AUDITS DE SÉCURITÉ

Un audit est une évaluation d'un système, d'un processus et/ou d'une organisation afin de visualiser les points faibles ainsi que les points forts du système d'information associé.

Les audits techniques de sécurité

Les audits techniques de sécurité ont pour objectif de détecter les failles et vulnérabilités d'un système d'information ou d'une organisation avant qu'elles ne soient exploitées.

Trois types de méthodologies existent pour les audits techniques. Il s'agit de :

- L'audit boite noire (ou pentest, pour penetration testing/test d'intrusion): technique d'audit qui vise à reproduire une cyberattaque en conditions quasi-réelles, afin d'identifier les failles exploitables.
- L'audit boite blanche : Le consultant dispose de toute la documentation nécessaire (configurations, architecture) pour lister toutes les failles existantes, sans effectuer de test d'intrusion.
- L'audit boite grise : Intermédiaire entre l'audit boite blanche et boite noire. Le consultant dispose de quelques éléments d'information, typiquement accessibles par social engineering ou phishing.

Les audits non-techniques de sécurité

Les audits non-techniques ne concernent pas un produit, une application ou un système d'information en particulier mais font état de la situation de sécurité en interne. CyberSecura vous propose les audits non techniques suivants :

- L'audit organisationnel, afin de faire le point sur vos pratiques, procédures et politiques de sécurité en interne.
- L'audit interne, dans le cadre de la poursuite d'une certification ISO 27001 et afin de tester le SMSI en place, de vérifier les procédures et politiques internes, etc.
- Le Gap Analysis, également dans le cadre de la poursuite d'une certification ISO 27001 et afin de faire un bilan des éléments actuels et à mettre en place.

En fonction des objectifs d'exhaustivité, du temps et du budget disponibles,
nous proposons différentes profondeurs d'audit.

	AUDIT FLASH	ÉTAT DES LIEUX	AUDIT INITIAL	AUDIT APPROFONDI
Cartographie de l'existant	●	●	●	●
Identification détaillée des failles et menaces	○	●	●	●
Tableau détaillé des contre-mesures	○	○	●	●
Volume de travail (SI et applicatif)	1 jour	⩽ 3 jours	4 à 7 jours	5 à 10 jours
Modalités et contenu de restitution	Rapport des résultats restitué sous forme de présentation			
Livrables en option*	X	Rapport clients	Rapport clients Plan d'actions	Rapport clients Rédaction PAS Plan d'actions

Valorisez vos engagements

CYBERSECURA
Cybersécurité & Conformité

PECB ISO/IEC 27001 LEAD IMPLEMENTER

FRANCE RELANCE

PRESTATAIRE RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

3 Avenue du 8 Mai 1945
38130 Échirolles

06.21.54.42.37

www.cybersecura.com

contact@cybersecura.com