



Cas d'étude: Cabinet d'expertise comptable

Sécuriser les données clients et assumer la responsabilité du dirigeant, sans freiner la production

Le contexte

Cabinet d'expertise comptable d'une quinzaine de collaborateurs, avec une activité rythmée par des échéances fiscales et sociales, et une forte dépendance aux outils numériques.

Chaque jour, le cabinet manipule des données particulièrement sensibles:
données financières, sociales, accès aux portails fiscaux et sociaux, échanges de pièces comptables avec les clients.

L'environnement informatique permettait de travailler efficacement.

Les outils étaient en place, les équipes productives, et l'activité se déroulait sans incident majeur.

La prise de conscience

Avec le temps, une inquiétude s'est installée côté direction.

Les associés ont progressivement pris conscience de ce que leur informatique impliquait réellement:

une concentration importante de données clients sensibles, des accès critiques utilisés au quotidien, et une surface d'exposition croissante aux risques cyber.

La question n'était plus

“est ce que ça fonctionne ?”

mais

“que se passe t il le jour où quelque chose arrive ?”

Une fuite de données, un compte compromis, un accès non autorisé pouvaient avoir des conséquences lourdes

interruption d'activité, perte de confiance des clients, mais surtout engagement direct de la responsabilité du dirigeant.

Cette crainte n'était pas théorique.

Elle est devenue un élément déclencheur dans la volonté de reprendre le contrôle de la cybersécurité du cabinet.

Le problème

L'environnement informatique présentait plusieurs fragilités

- Accès utilisateurs peu formalisés
- Sécurité hétérogène selon les poste
- Peu de visibilité sur la continuité d'activité
- Dépendance à une personne clé pour les sujets IT

Côté direction, cela générait une gestion essentiellement réactive, avec un manque de cadre clair et de pilotage.

Le dirigeant a donc consulté les équipes Altevia Tech pour moderniser et sécuriser l'ensemble de son informatique.

La solution

Le cabinet a choisi le **Pack Cybersécurité Opérationnelle**.

Ce choix permettait

- de sécuriser rapidement les accès, les postes et les données
- d'intégrer la cybersécurité dans le fonctionnement quotidien du cabinet
- sans lancer un projet long, ni recruter de ressources dédiées

L'intervention Altevia

L'accompagnement a été conçu pour être **rapide, pragmatique et compatible avec les contraintes métier.**

Phase de cadrage

Un échange initial à distance a permis de comprendre les usages réels du cabinet
organisation des dossiers, circulation des pièces, périodes de forte activité, contraintes réglementaires.

Cette phase a permis d'identifier les risques prioritaires et de définir un niveau de sécurité adapté, sans sur sécuriser inutilement.

Déploiement de la cybersécurité opérationnelle

La mise en œuvre a été réalisée en **quelques jours**, majoritairement à distance, sans interruption d'activité.

Les actions ont porté sur

- La sécurisation des accès utilisateurs et des comptes sensibles
- Le renforcement de la protection des postes de travail
- La mise en place de règles simples et compréhensibles pour les équipes
- La réduction des risques liés aux erreurs humaines et aux tentatives d'hameçonnage

Suivi dans la durée

Une fois le socle en place, Altevia assure un **suivi continu** de la **sécurité**, avec une **supervision active** et des **ajustements réguliers**, intégrés au fonctionnement normal du cabinet.

Les bénéfices

- Une réduction concrète des risques de fuite ou de compromission des données clients
- Une cybersécurité intégrée aux usages quotidiens, sans freiner la production
- Des collaborateurs mieux protégés, sans complexité supplémentaire
- Une meilleure maîtrise des obligations réglementaires et de la responsabilité du dirigeant
- Un dirigeant plus serein face aux risques cyber

Aujourd'hui, le cabinet dispose d'une cybersécurité adaptée à son métier, compréhensible et assumée, au service de la continuité d'activité et de la confiance client.

Échanger sur votre situation

Chaque organisation est différente.

Les enjeux, les usages et les contraintes ne sont jamais exactement les mêmes.

Si les problématiques décrites dans ce cas vous parlent, un premier échange permet simplement de comprendre votre contexte et de voir si notre approche est adaptée.

Pour en discuter

contact@altevia-tech.com
www.altevia-tech.com

