ALTEVIA TECH

LIVRE BLANC · ÉDITION CABINETS D'AVOCATS

Cybersécurité et cabinets d'avocats

Protéger vos dossiers, sécuriser votre activité, préserver votre responsabilité.

Ce que tout dirigeant de cabinet devrait savoir avant le prochain incident.

www.altevia-tech.com

PRÉAMBULE

La confiance de vos clients passe désormais par votre informatique

Dans un cabinet d'avocats, la confiance est l'actif fondamental. Elle repose sur la compétence juridique, la déontologie, le secret professionnel et la capacité à accompagner un client sans rupture ni exposition.

Aujourd'hui, cette confiance dépend aussi d'un élément devenu central et souvent mal maîtrisé : **le système informatique**. Les dossiers, les délais, les échanges avec les juridictions et les clients y transitent en continu. Quand il s'arrête, le cabinet s'arrête avec lui.

La cybersécurité est devenue une composante directe de la responsabilité professionnelle du cabinet. En juin 2023, l'ANSSI a d'ailleurs consacré aux cabinets d'avocats un rapport dédié sur l'état de la menace : le secteur est désormais identifié comme une cible à part entière.

Ce livre blanc s'adresse aux dirigeants qui veulent :

- comprendre les risques réels, chiffres et cas à l'appui ;
- distinguer ce qui protège vraiment de ce qui rassure à tort ;
- poser un cadre clair, durable et assumé ;
- garder la main, sans céder à la complexité ni à la peur.

Objectif : repartir avec une grille de lecture nette et de quoi décider.

L'ÉTAT DE LA MENACE

Le risque est déjà chiffré

Ce que disent les chiffres officiels, avant même de parler de votre cabinet.

4 386

événements de sécurité traités par l'ANSSI en 2024, soit **+15 %** en un an.

ANSSI, Panorama de la cybermenace 2024

≈ 12

cabinets d'avocats français compromis par rançongiciel depuis 2017, un total que l'ANSSI juge « très probablement sous-évalué ».

ANSSI / CERT-FR, État de la menace, 2023

3,85 M€

coût moyen d'une violation de données en France en 2024.

IBM, Cost of a Data Breach 2024

72 h

le délai légal pour notifier la CNIL après une violation de données personnelles.

Article 33 du RGPD

68 %

des violations impliquent un facteur humain (erreur ou piège). L'hameçonnage reste la première porte d'entrée.

Verizon, DBIR 2024

99 %

des attaques par vol de mot de passe sont bloquées par la double authentification.

Microsoft

Les cabinets d'avocats restent hors du périmètre des opérateurs d'importance vitale et des services essentiels. **Leurs incidents sont donc peu déclarés, et largement invisibles dans les statistiques.**

01

L’informatique, outil de production juridique critique

Votre système d’information est devenu l’outil de production du cabinet.

Un cabinet moderne repose intégralement sur son système d’information pour l’essentiel de son activité :

- l’accès aux dossiers
- la production des actes
- la gestion des délais
- la facturation
- la communication clients et juridictions
- l’archivage et la conservation des pièces

L’activité juridique est désormais continue, numérique et souvent nomade. La moindre indisponibilité a un impact **immédiat** : continuité de l’activité, respect des délais, relation client, responsabilité du cabinet.

Une dépendance qui coûte cher quand elle échappe au contrôle

En 2016, un cabinet américain frappé par un rançongiciel a vu **l’ensemble de ses documents de travail paralysés pendant au moins trois mois**. Après paiement de la rançon, les outils de déchiffrement fournis se sont révélés inexploitables ; les attaquants ont alors exigé davantage. Pertes totales estimées : **700 000 $**.

L’informatique est devenue une chaîne de production. Elle se sécurise comme telle.

02

Pourquoi les cabinets sont une cible de choix

Des données à très haute valeur, une exposition juridique directe.

Les cabinets détiennent, par nature, des informations parmi les plus sensibles qui soient : stratégies de défense, contentieux en cours, données personnelles, éléments financiers, secrets d'affaires de leurs clients. Ces données **s'achètent, se revendent et se monnaient**. Certains groupes se sont même spécialisés dans la compromission de cabinets pour commettre des délits d'initié.

Trois grandes familles de menaces

01

Le gain

Rançongiciel, revente de données, détournement de comptes bancaires. La menace la plus fréquente en volume.

02

L'espionnage

Vol de secrets d'affaires et de dossiers clients par des acteurs parfois liés à des États, avec des campagnes visant spécifiquement des cabinets.

03

La déstabilisation

Divulgation de dossiers sensibles pour nuire, exposer ou faire pression. Le préjudice est réputationnel autant qu'opérationnel.

La « double extorsion » change la donne

Les attaquants exfiltrent vos données **avant** de les chiffrer, puis menacent de les publier si la rançon reste impayée. Même avec une sauvegarde parfaite, la fuite a déjà eu lieu. Et le secret professionnel, une fois éventé, reste éventé.

Les conséquences d'un incident dépassent largement le cadre technique. **Elles sont financières, opérationnelles, réputationnelles et déontologiques.**

CAS RÉELS · FRANCE

De vrais cabinets, de vraies fuites

Trois affaires documentées par l'ANSSI et les sources publiques.

ATTAQUE PAR LA CHAÎNE D'APPROVISIONNEMENT

Everest, au moins 7 cabinets français d'un coup

Le groupe Everest a exfiltré les données et chiffré les systèmes d'**au moins sept cabinets d'avocats français** en compromettant leur prestataire d'infogérance commun. Parmi les victimes, un cabinet représentant des parties civiles aux procès de l'attentat contre *Charlie Hebdo* et de l'assassinat de Samuel Paty. Des éléments d'instruction ont été rendus publics : PV d'auditions, rapports d'autopsie, comptes-rendus d'écoutes, données d'enquêteurs et de magistrats.

RANÇONGICIEL · DÉBUT 2022

LockBit 2.0

Publication de documents dérobés à un cabinet français : contrats de travail, photos d'identité, et un simple **fichier texte de mots de passe en clair**, ouvrant potentiellement l'accès à un compte bancaire et au RPVA.

ÉTATS-UNIS · 2016

La rançon payée pour rien

Trois mois de paralysie, un déchiffrement inexploitable malgré la rançon versée, une seconde demande des attaquants. Bilan : **700 000 $** de pertes.

Point commun : ces attaques ont réussi avec des moyens simples. Un prestataire mal surveillé, un mot de passe en clair, une sauvegarde absente suffisent.

03

Les fausses certitudes les plus répandues

Beaucoup de cabinets se croient couverts. Les incidents réels racontent autre chose.

CE QUE BEAUCOUP DE CABINETS PENSENT

« Nous sommes protégés »

- on a un antivirus
- on fait des sauvegardes
- on utilise des outils reconnus
- on n’a jamais eu d’incident

Ces éléments sont utiles. Ils restent très insuffisants pris isolément.

CE QUE MONTRENT LES INCIDENTS RÉELS

Là où ça casse vraiment

- des environnements partiellement protégés
- des configurations mal maîtrisées
- des outils mal compris par leurs utilisateurs
- une responsabilité floue, sans pilote désigné

Le maillon faible, c’est presque toujours l’usage

L’hameçonnage reste la première porte d’entrée : tout commence par un clic. Une sauvegarde vaut ce que vaut sa restauration, une fois qu’elle a été réellement testée. Un prestataire laissé sans contrôle devient votre angle mort, exactement comme dans l’attaque Everest.

La cybersécurité repose avant tout sur une organisation claire et assumée. **Les outils viennent ensuite.**

LA DIMENSION DÉONTOLOGIQUE

Un incident cyber est aussi un risque de responsabilité

Fuite, perte ou indisponibilité : les conséquences vous suivent bien après la remise en service.

Secret professionnel

La révélation d'une information couverte par le secret par celui qui en est dépositaire est punie d'**un an d'emprisonnement et de 15 000 € d'amende** (art. 226-13 du code pénal). Une fuite de dossier suffit à le mettre en cause.

RGPD et CNIL

Notification de la violation à la CNIL sous **72 heures** (art. 33), information des personnes concernées, et sanctions pouvant atteindre **4 % du chiffre d'affaires mondial ou 20 M€**.

Responsabilité professionnelle

Quand un client subit un préjudice (perte de pièces, délai manqué, divulgation), la responsabilité civile du cabinet peut être recherchée.

Réputation

La confiance se construit sur des années et se perd en une notification. Le préjudice réputationnel est souvent le plus durable et le plus difficile à chiffrer.

La vraie question, le jour d'un incident : pouvez-vous prouver que vous aviez pris les mesures raisonnables ?

04

Le changement de paradigme nécessaire

Trois principes valent mieux qu’un empilement de solutions.

Simplicité

Un système simple, documenté et compris protège mieux qu’un système complexe et mal maîtrisé. Une sécurité comprise est une sécurité appliquée.

Intégration

La sécurité s’intègre au fonctionnement quotidien du cabinet : accès, sauvegardes, postes, prestataires. Elle tient dans la durée, au-delà du projet ponctuel qu’on finit par oublier.

Responsabilité

Quelqu’un assume clairement le bon fonctionnement, la sécurité, la continuité et la réaction en cas d’incident. Une responsabilité diffuse est une responsabilité vacante.

La cybersécurité est d’abord un **cadre de responsabilité à poser**, tenu dans le temps.

CE QUI PROTÈGE VRAIMENT

Le socle qui arrête la grande majorité des attaques

Directement issu des recommandations de l'ANSSI pour les cabinets d'avocats.

1 · Double authentification (MFA)

Partout où c'est possible : messagerie, connexions à distance, outils métier. À elle seule, elle bloque l'essentiel des attaques par vol de mot de passe.

2 · Sauvegarde 3-2-1, testée

Trois copies, deux supports, une hors-ligne et hors site. Et surtout : une restauration vérifiée pour de vrai.

3 · Comptes maîtrisés

Des comptes standard au quotidien, une séparation stricte des usages professionnels et personnels, le principe du « besoin d'en connaître ».

4 · Chiffrement et mots de passe

Chiffrement intégral des disques, gestionnaire de mots de passe (coffre-fort). Les identifiants restent toujours protégés, jamais en clair.

5 · Prestataires sous contrôle

Traçabilité des interventions, sécurisation des accès distants. Les prestataires sont devenus une porte d'entrée privilégiée pour les attaquants.

6 · Humain et plan de crise

Sensibilisation à l'hameçonnage, un référent sécurité identifié, et un mode dégradé préparé *avant* l'incident.

Prises séparément, ces mesures sont simples. Ensemble, elles écartent la grande majorité des scénarios observés sur le terrain.

05

Questions clés pour les dirigeants de cabinet

Sept questions. Si les réponses tardent, le risque est déjà là.

- ? Savez-vous exactement **où** sont stockées vos données sensibles, et sous quelle juridiction ?
- ? Pourriez-vous garantir l'accès aux dossiers en cas d'incident majeur, dès demain matin ?
- ? Les accès sont-ils strictement maîtrisés (double authentification, comptes nominatifs, droits limités) ?
- ? Vos sauvegardes sont-elles réellement **exploitables**, et l'avez-vous vérifié ?
- ? Les interventions de vos prestataires sont-elles tracées et encadrées ?
- ? Sauriez-vous notifier la CNIL dans les 72 heures, et qui s'en chargerait ?
- ? Qui, nommément, pilote votre informatique et votre sécurité au quotidien ?

Si certaines réponses manquent, vous savez déjà par où commencer.

06

L’approche Altevia Tech pour les cabinets d’avocats

Claire, progressive, sans jargon inutile, orientée responsabilité et sérénité.

Nous prenons en charge l’ensemble du système informatique du cabinet. La cybersécurité y est **intégrée par défaut**, comprise dans le fonctionnement quotidien.

- gestion du parc informatique
- support des utilisateurs
- supervision continue
- sauvegardes et continuité d’activité
- gestion des accès et des identités
- conformité RGPD et secret professionnel

Ce que vous y gagnez

Un système pilotable

stable, prévisible, documenté.

Une exposition réduite

un cadre clair, des mesures qui tiennent dans la durée.

Nous assumons la responsabilité du bon fonctionnement de votre informatique. **Vous vous concentrez sur vos dossiers.**

07

Une méthode progressive et durable

Vous démarrez simplement. Nous construisons dans la durée.

Étape 1. Comprendre l’existant

Cartographier le système, les données sensibles et les dépendances, prestataires compris.

Étape 2. Identifier les risques

Prioriser factuellement, avec sang-froid : ce qui expose vraiment le cabinet passe en premier.

Étape 3. Stabiliser le socle

Double authentification, sauvegardes testées, comptes, chiffrement, plan de crise. Le socle avant le reste.

Étape 4. Définir une trajectoire

Une feuille de route réaliste, adaptée à la taille et aux moyens du cabinet.

Étape 5. Superviser et faire évoluer

La sécurité se maintient dans le temps : supervision continue et ajustements réguliers.

CONCLUSION

La cybersécurité est d’abord un choix de gouvernance

Un cabinet qui maîtrise son informatique protège ses clients, assume sa responsabilité, préserve sa réputation et travaille sereinement. Tout est affaire de cadre, plus que de budget.

Avec Altevia Tech, vous faites le choix :

- d’un partenaire qui assume la responsabilité
- d’un cadre clair et documenté
- d’une sécurité intégrée au fonctionnement
- d’une informatique enfin tranquille

La vraie question : serez-vous prêts le jour où ça arrivera ?

PROCHAINES ÉTAPES

Un diagnostic cybersécurité confidentiel pour votre cabinet

Une analyse factuelle

l'état réel de votre exposition, sans jargon.

Des priorités claires

ce qu'il faut traiter d'abord, et pourquoi.

Une vision maîtrisée

une trajectoire réaliste, à votre rythme.

POUR EN DISCUTER

Prenez 15 minutes avec nous

contact@altevia-tech.com
www.altevia-tech.com
Altevia Tech · Infogérance, cybersécurité et automatisation · Toulouse / Occitanie

Sources principales : ANSSI, *Panorama de la cybermenace 2024* · ANSSI / CERT-FR, *État de la menace informatique contre les cabinets d'avocats* (CERTFR-2023-CTI-004, 27 juin 2023) · CNB, *Guide pratique : la sécurité numérique du cabinet d'avocat* · IBM, *Cost of a Data Breach 2024* · Verizon, *DBIR 2024* · RGPD (règlement UE 2016/679) · Code pénal, art. 226-13. Chiffres arrondis à des fins de lisibilité.