Les Petites Affiches de Vaucluse depuis 1839

Ecrit par Echo du Mardi le 18 janvier 2023

Protéger les avocats et les équipes juridiques contre les cyber-risques



Qu'ils fassent partie d'un cabinet d'avocats ou qu'ils soient juristes au sein d'une entreprise, les avocats traitent chaque jour des informations sensibles et sont susceptibles d'être la cible de cyberattaquants.

Les avocats ont des obligations éthiques et légales de protéger les données de leurs clients et de les signaler rapidement aux autorités compétentes ainsi qu'à leurs clients s'ils subissent une violation de données. Ils ont également un rôle essentiel à jouer à la suite d'une violation. Ce seul fait en fait des cibles prisées des cybercriminels.
Quels sont les cyber-risques auxquels les avocats sont alors confrontés ? Et de quelle manière les équipes informatiques et les cabinets d'avocats peuvent-ils protéger leurs clients et leurs organisations ?

Ecrit par Echo du Mardi le 18 janvier 2023

Des informations sensibles
Selon le domaine d'activité et le contexte, les avocats gèrent une grande variété d'informations sensibles et confidentielles. Les clients, les employés et leurs entreprises comptent sur le fait qu'elles restent en sécurité entre leurs mains. Les avocats spécialisés dans l'emploi peuvent traiter les Informations personnelles identifiables (IPI) de leurs clients, notamment les numéros de sécurité sociale, les numéros de permis de conduire, des informations bancaires, les dates de naissance ou encore les dossiers médicaux.

La cybermenace contre les équipes juridiques
Les avocats comprennent bien la valeur de la sécurité des informations. Elle est essentielle à la confidentialité qui rend possible le conseil juridique et la relation avocat-client. Cependant, avec des ressources informatiques parfois limitées, leur traitement d'informations sensibles et les failles de sécurité des logiciels juridiques, les équipes juridiques sont régulièrement sujettes aux cyberattaques.

Des failles de sécurité dans les technologies juridiques
Depuis plusieurs années, la technologie juridique (ou Legal Tech) facilite grandement leur quotidien, de la comptabilité à la facturation en passant par les communications avec les clients et la gestion des documents. La confiance et la confidentialité étant des éléments fondamentaux des pratiques juridiques, il est essentiel de disposer d'une technologie juridique sécurisée. La technologie juridique permet aux organisations de traiter plus rapidement les données, de réduire les erreurs administratives, de créer une transparence dans la facturation et de permettre aux équipes juridiques internationales de collaborer plus efficacement. Les logiciels de découverte électronique (ou eDiscovery) aident les avocats à trouver et à trier les documents et à se concentrer sur des tâches plus importantes.
Dans les grands cabinets d'avocats et les équipes juridiques internes, des professionnels de la sécurité disposant de moyens sont équipés pour gérer la sécurité de l'information et la technologie. Cependant, le fait de disposer de plus de moyens ne se traduit pas nécessairement par une diminution des attaques ou des violations, bien au contraire.

Le manque de temps favorise la praticité au détriment de la sécurité
Peu importe où et comment ils exercent, les avocats ont le devoir de protéger les informations de leurs clients. Cependant, les exigences en matière de productivité et d'heures facturables se heurtent souvent à la sécurité des informations d'une manière qui porte atteinte à la confidentialité. Bien qu'elle ne soit pas à proprement parler une cybermenace externe, la non-conformité comporte un risque important de litiges coûteux ou d'interruptions des activités. Heureusement des solutions existent. Une formation à la sécurité peut aider les avocats et le personnel non-juriste à reconnaître les vecteurs de menace et à instiller l'importance de la sécurité de l'information dans un cabinet axé sur le client.

Ces dernières années, des cyberattaques très médiatisées contre de grands cabinets d'avocats ont mis en évidence la menace omniprésente contre les avocats et les données sensibles. Il devient donc nécessaire de protéger les avocats et les données confidentielles qu'ils traitent au quotidien face aux cybermenaces. L'hygiène des mots de passe, par exemple, contribue grandement à atténuer le risque et l'impact des cybermenaces.

Ecrit par Echo du Mardi le 18 janvier 2023

Arnaud De Backer – Channel Sales Manager EMEA – Chez Keeper Security