

La cybersécurité, une priorité pour les études d'avocats et une nécessité pour leurs clients

Aujourd'hui, les évolutions technologiques vont de pair avec les risques de cyberattaques. Dans le domaine du droit, si le besoin de changements et d'évolutions est important, il s'avère aussi essentiel de se consacrer à des stratégies adaptées aux risques en matière de sécurité.

Les études d'avocats représentent des cibles précieuses pour les cybercriminels, car les données qu'elles collectent sont nombreuses et monétisables. Mais de quelles données s'agit-il? Quels sont les risques de cyberattaques pour les avocats et que représentent-ils pour leurs clients? Comment les avocats peuvent-ils mettre en place une stratégie de cyberprotection efficace et calibrée sur les risques? Réponse avec Steven Meyer, ingénieur EPFL en cybersécurité et directeur de Zendata, entreprise de cybersécurité qui évalue les risques d'une organisation, fournit les services de protection adaptés et intervient sur des incidents de cyberattaques avec des investigations scientifiques digitales.

Steven Meyer, quelle est l'importance de la confidentialité dans le métier d'avocat?

Les avocats sont depuis toujours considérés comme des conseillers fiables et dignes de confiance, et ceci pour une bonne raison. Dès le début de leur formation en droit, ils apprennent l'importance d'assurer la confidentialité des informations de leurs clients. La confidentialité fait donc partie de l'ADN d'un avocat du point de vue professionnel, légal et éthique.

Et quels types de données sensibles sont collectées par les avocats?

Leurs systèmes constituent une source riche et profonde d'informations confidentielles, que ce soit des données de santé et financières des personnes physiques ou les valeurs de propriété intellectuelle et secrets commerciaux des personnes morales. De surcroît, les études ne détiennent pas seulement les données les plus

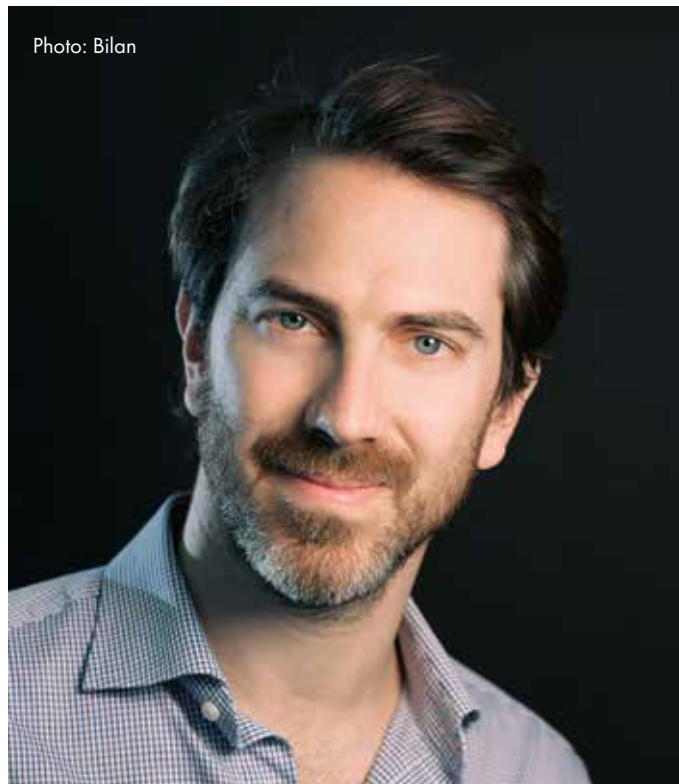


Photo: Bilan

sensibles de leurs clients, mais ont aussi des droits de procuration sur leurs biens, sociétés et fortunes.

Quels sont les risques en matière de cybercriminalité pour une étude?

Les risques encourus vont de l'espionnage industriel sur un projet de fusion à l'acquisition d'avantages stratégiques dans un cas de litige, en passant par le vol d'informations privilégiées sur une personne. Ils sont nombreux et les hackers sont à la recherche de ces informations pour leur propre utilisation ou pour les revendre.

Ces risques ont-ils augmenté à cause de la pandémie, et notamment avec l'obligation du télétravail?

La pandémie a eu un fort impact tant sur les méthodes de travail que sur le nombre de cyberattaques. La modification de l'environnement de travail a par exemple engendré une nette augmentation des fraudes au président (CEO Fraud). Les employés n'ont en effet plus la proximité physique et ne peuvent pas valider de vive voix des instructions émises par email.

Les entreprises ont aussi dû rapidement mettre en place des nouvelles technologies de télétravail qui n'ont pas été forcément bien configurées et pour lesquelles les utilisateurs ne maîtrisaient pas le fonctionnement.

Quelles sont les conséquences les plus importantes d'une fuite de données ou d'un piratage pour une étude d'avocats?

Hormis les problèmes légaux auxquels un avocat s'expose lors d'une fuite de données, la réputation de l'étude est très rapidement remise en cause. Les avocats perdent ainsi facilement la confiance de leurs clients.

Dans ce domaine, quels ont été les plus grands scandales de l'Histoire?

Le scandale des Panama Papers de 2016 était directement lié à un vol de données de l'étude Mossack Fonseca. Il a eu un impact sur l'étude d'avocats et ses clients, mais l'écosystème financier et légal du Panama en a aussi directement souffert.

Autrement, l'année dernière, l'étude Grubman Shire Meiselas & Sacks a été victime d'un ransomware où les criminels ont menacé de publier les données volées, si la rançon de \$42M n'était pas payée.

En Suisse, quel est le pourcentage d'études d'avocats qui ont une stratégie de cyberdéfense efficace?

Il nous est impossible de donner un chiffre exact. Cependant, à ce jour, nous n'avons eu aucun audit de cybersécurité d'une étude d'avocats où aucun problème critique n'ait été trouvé. L'efficacité d'une cyberdéfense s'évalue avec les risques auxquels l'étude s'expose, la tolérance aux risques des associés et les protections mises en place pour contrôler ces risques.

Comment expliquez-vous cela?

L'évaluation des risques digitaux est difficile pour tous secteurs d'activité. L'exposition aux attaques est souvent mal appréciée, les objectifs des criminels sont parfois obscurs et il est compliqué de quantifier l'efficacité des protections mises en place.

Pour un cybercriminel, quels avantages présente le piratage d'une étude d'avocats?

Les cybercriminels cherchent la profitabilité. Il est question de savoir quel va être le coût et l'effort pour commettre la cyberattaque par rapport au gain potentiel. La réalité du terrain révèle que, généralement, les protections mises en place dans les études ne sont pas proportionnelles à la valeur des données détenues. Pour un cybercriminel, le piratage d'une étude d'avocats ne demande donc pas beaucoup d'efforts.

D'ailleurs, les études d'avocats travaillent avec un grand nombre d'informations sensibles facilement monétisables par un criminel. Elles ont aussi des accès privilégiés pouvant être très rentables dans les mains de criminels. Finalement, dans l'esprit de ces derniers, elles ont beaucoup de moyens financiers à disposition.



Pourquoi les avocats doivent-ils se protéger aujourd'hui?

La menace est malheureusement bien réelle et l'impact va bien plus loin que l'étude victime de l'attaque. Se faire hacker est contagieux et les attaques réussies ont souvent des effets de boule de neige: elles impactent

non seulement la victime, mais aussi la région et la profession.

En quoi consiste une bonne stratégie de cyberprotection?

Mettre un antivirus et un firewall ne constitue pas une stratégie de protection. L'étude doit analyser les risques

et mettre en place une stratégie humaine, organisationnelle et technologique afin de diminuer le risque à un niveau reconnu comme acceptable par la profession et les associés.

Le processus n'est ni long ni compliqué, mais cela demande une bonne compréhension autant des enjeux que des capacités des hackers. En plus, en interne, il est essentiel d'avoir une réelle volonté de se protéger correctement.

Quels sont les bénéfices d'une stratégie efficace de cyberdéfense sur l'activité des études?

La confiance des clients est un pilier essentiel pour un avocat. Pouvoir démontrer une bonne cyberhygiène et avoir une compréhension des risques numériques sont des éléments qui peuvent rassurer un client sur les compétences de l'étude qui l'accompagne.

INTERVIEW **ANDREA TARANTINI**

DIVORCE.SA CONTENU SPONSORISÉ

Divorce et pensions: quelles nouveautés?

Dans les six derniers mois, le Tribunal fédéral a rendu cinq arrêts importants sur les contributions financières dues lors d'un divorce ou d'une séparation et sur l'obligation de travailler. Explications.



Me Douglas Hornung

Dorénavant, il n'y a plus qu'une seule méthode pour fixer les montants dus, celle du «minimum vital avec répartition de l'excédent». En revanche, auparavant, il y avait 26 méthodes différentes dans les 26 cantons. Il n'est donc plus question d'appliquer des pourcentages du revenu pour fixer les montants de contributions.

On fait d'abord le calcul des charges incompressibles, à savoir: le minimum vital est additionné au loyer

raisonnable, aux primes d'assurance ainsi qu'aux impôts. On prend ensuite le revenu net, dont on déduit les charges incompressibles pour arriver à un solde disponible à partir duquel le montant des contributions peut être fixé. On fait le même type de calcul pour les enfants et l'(ex-)conjoint. Les enfants doivent au moins avoir leur minimum vital couvert (par le parent qui a la garde et par l'autre parent qui paie une contribution). Si le montant de la pension due pour l'enfant absorbe tout le disponible du parent payeur, aucune pension n'est due pour l'(ex-)conjoint.

Il existe ainsi une hiérarchie des contributions. S'il n'y a pas de disponible suffisant, les pensions pour les enfants mineurs priment et, s'il

reste ensuite un disponible, il peut y avoir une pension pour l'(ex-)époux/épouse. Dans le cas où il reste encore du disponible, une pension est également envisagée pour l'enfant majeur à charge.

Sur l'obligation de travailler, le Tribunal fédéral a abandonné le principe qu'un adulte n'a pas à travailler si, lors de la séparation ou du divorce, il/elle est âgé(e) de 50 ans ou plus. Il faut, au contraire, partir du principe qu'on peut s'attendre à ce qu'un adulte travaille, sauf à démontrer la quasi-impossibilité concrète de le faire.

Enfin, le Tribunal fédéral part de l'idée qu'un parent n'a pas d'obligation de travailler tant que le plus jeune des enfants n'a pas atteint l'âge de la scolarité. Ensuite, on peut

attendre du parent qu'il/elle travaille à 50% jusqu'à ce que le plus jeune a atteint l'âge de 12 ans révolus, puis à 80% jusqu'à l'âge de 15 ans révolus et à 100% au-delà.

Ces nouvelles règles sont les bienvenues. Mais elles arrivent parfois à des aberrations: ainsi, un père gagne CHF 4500.- par mois, une mère ne travaille pas mais a une capacité de gain de 900.- et il y a un enfant de quatre ans à prendre en compte. Résultat judiciaire: une pension de CHF 2070.- par mois, soit 46% du salaire.

**N°1 du divorce en ligne
100% de succès depuis 2007**

divorce.ch