Quand les avocats sont appelés à renforcer la sécurité de leur SI

Protégé par l'article 8 de la convention européenne des droits de l'Homme, le secret professionnel constitue *« un des principes fondamentaux sur lesquels repose l'organisation de la justice dans une société démocratique »*, souligne le Conseil des barreaux européens *(Council of Bars and Law Societies of Europe*, ou CCBE) . La confidentialité des échanges entre les avocats et leurs clients est donc essentielle, mais elle est menacée par la cybercriminalité, le piratage et la surveillance illégale d'États.

C'est dans ce contexte que le CCBE a décidé de mettre à disposition des avocats et des barreaux un guide des bonnes pratiques à mettre en œuvre pour renforcer la sécurité informatique des avocats. *« La protection absolue des systèmes informatiques face à la surveillance, qu'elle soit légale ou non, et face à d'autres formes de piratage est impossible à atteindre »*, soulignent les auteurs du rapport. Néanmoins, il est indispensable de réduire ces risques en adoptant des mesures systématiques et structurées. Le chiffrement fait donc partie des priorités. Une analyse des risques s'impose également.

Analyse des risques

« Les obligations imposées aux avocats en matière de sécurité informatique par la loi de l'Union européenne sont exprimées de manière générale et tendent à s'inscrire dans le contexte précis de la protection des données », indique le CCBE. Or, ni le nouveau règlement général sur la protection des données, ni le projet de directive sur la sécurité des réseaux et de l'information ne devraient changer cette approche législative dans un avenir proche, selon les auteurs du guide.

Il est nécessaire d'identifier les ressources et les failles de sécurité potentielles, celles qui auraient le plus fort impact sur l'activité du cabinet d'avocats. L'accent doit être mis, enfin, sur les solutions qui permettent de réduire ce risque en s'appuyant sur des normes de sécurité informatique (ISO, NIST).

Chiffrement et VPN

Un autre recommandation du Conseil des barreaux européens consiste à sécuriser l'accés réseau, en particulier l'accès sans fil. *« La solution la plus sûre est d'établir une connexion à un réseau privé virtuel (VPN) entre le cabinet d'avocats et l'appareil mobile ou toute autre ressource informatique mobile à risque »*, précisent les auteurs du guide.

Par ailleurs, l'utilisation de l'Internet mobile (4G, WCDMA, LTE…) est plus sûre que l'utilisation du WiFi, qui, selon eux, n'est pas assez sécurisé pour un usage professionnel. *« Mais il n'est pas toujours possible d'utiliser l'Internet mobile à l'étranger »,* ajoutent-ils. Par conséquent, *« en l'absence d'une telle couche de chiffrement supplémentaire, l'avocat ne devrait pas utiliser de connexion WiFi sans contrôle d'accès fondamental pour envoyer des informations liées ».*

… de bout en bout

Pour les messages électroniques, même combat : *« il est primordial d'utiliser le chiffrement des courriels de bout en bout »*, commente le CCBE. *« La sécurité des courriels pourrait s'améliorer de manière significative au sein de l'UE s'il existait un répertoire facile à utiliser et fiable des certificats de chiffrement pour les avocats »*, ajoute le Conseil. *« Si ce chiffrement n'est pas possible parce que l'on a voulu envoyer un courriel à un client sans certificat de chiffrement par exemple, il serait préférable de chiffrer les informations les plus importantes du client dans une pièce jointe et d'envoyer un mot de passe unique au client par un autre moyen (par exemple par SMS ou par téléphone et non par courriel) »*, précise-t-il.

Lire aussi :

Règlement européen sur la protection des données : ce qu'en pensent les entreprises
Les établissements de santé ont leur plan de sécurité des SI

crédit photo © Photo via Activedia via Visualhunt.com