637

La sécurité numérique au sein des cabinets d'avocats

La sécurité numérique, ou cybersécurité, peut se définir comme l'ensemble des actions techniques, juridiques et humaines visant à sécuriser l'intégrité des machines et des contenus.
Les avocats, longtemps freinés par l'inadéquation du droit - notamment le droit de la preuve – aux réalités techniques, et par l'absence de formation et de culture informatique, sont désormais largement connectés.
Leurs principales préoccupations actuelles sont essentiellement de deux ordres : d'une part, garantir l'intégrité des documents et d'autre part, garantir le secret professionnel.


Jean-Christophe Guerrini, Avocat Associé, DS avocats

Violaine Selosse, Avocat, DS avocats

Quelles sont les principales formes de cybercriminalité et les comportements à adopter ?
La cybercriminalité se définit comme l'ensemble des infractions pénales commises *via* les réseaux de communications électroniques. Sa répression est désormais une priorité, en France comme au niveau européen, la Commission européenne l'ayant placée parmi les trois priorités de l'Union inscrites à l'agenda européen de sécurité, publié le 28 avril 2015.
Les cyberattaques peuvent prendre de nombreuses formes, telles que le déni de service distribué (*Distributed Denial of Service*, ou DDoS – visant à saturer le système d'information ou de communication afin de l'empêcher de fournir le service attendu), ou la défiguration (modifier l'apparence ou le contenu d'un serveur Internet).
Cependant, les cibles les plus sensibles des cyberattaques, particulièrement en ce qui concerne les cabinets d'avocats, sont les données.
Les formes d'attaques les plus fréquentes sont ainsi les escroqueries, telles que le *phishing* (le pirate tente d'obtenir des données, et notamment des données bancaires, en se faisant passer, par exemple, pour un opérateur de télécommunication ou une administration telle que le Trésor public) ou le *skimming* (l'utilisation frauduleuse de numéros de cartes bancaires sur Internet).
Une autre escroquerie, particulièrement redoutable, est le *ransomware* ou rançongiciel. Il s'agit d'un logiciel malveillant se propageant par courrier électronique, à l'ouverture d'un lien ou d'une pièce jointe. Les données sont alors « prises en otage » (par le biais d'un chiffrement, par exemple) par le pirate, qui conditionne la libération des données au paiement d'une rançon.
La majorité des *ransomwares* et des tentatives de *phishing* se propagent par le biais de courriels, et plus particulièrement, par leurs pièces jointes.
Il est donc essentiel de former et sensibiliser tout le personnel du cabinet, de l'associé au stagiaire, à ces problématiques. Le premier réflexe doit toujours être d'identifier l'émetteur d'un courriel.
À défaut, il est plus prudent de supprimer le courriel ou demander à l'émetteur d'en confirmer le contenu. Le cas échéant, il est également possible de transmettre le courriel au service informatique pour vérification.
En cas d'attaque, il est important de préserver les traces de l'activité illicite et de prendre immédiatement contact avec les responsables informatiques ou, à défaut, avec le Centre Opérationnel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
L'adoption d'un plan de préparation et de continuité peut permettre d'atténuer le préjudice subi, en prévoyant les mesures permettant de prévenir, détecter et répondre aux incidents de sécurité numérique et d'assurer la reprise des activités.

Comment garantir la sécurité des documents dématérialisés ?
La première règle, et la plus essentielle, en matière de sécurité de documents dématérialisés est de créer une sauvegarde.
Celle-ci permet de récupérer rapidement ses données, que cela fasse suite à une cyberattaque ou à un dysfonctionnement informatique.
Pour être efficace, la sauvegarde doit d'abord être fréquente. Il peut également être judicieux d'organiser une séparation entre l'endroit où sont installés le système d'exploitation et les programmes (le disque C:) et celui où seront sauvegardées les données. Cela permet de ne pas abîmer ses données en cas de problème avec le système d'exploitation. De plus, il faut vérifier régulièrement le bon fonctionnement des outils de sauvegarde.
La sécurité en interne est assurée par une gestion des authentifications (remise d'un identifiant unique à chaque utilisateur) et des habilitations (contrôle *a priori* des droits d'accès aux données pour chaque catégorie d'utilisateur), ainsi que des sites dont l'accès est autorisé.
Ainsi, les ordinateurs – et notamment les ordinateurs portables de même que les smartphones qui sont très souvent oubliés dans les aéroports ou halls de gare -, serveurs et les données qu'ils contiennent, doivent toujours être protégés par un mot de passe robuste, difficile à deviner aussi bien par des tiers que par des outils automatisés.
Ces règles de sécurité doivent bien évidemment être complétées *a minima* par l'installation d'un logiciel antivirus/sécurité Internet sur son ordinateur.
Pour se prémunir efficacement contre d'éventuelles attaques informatiques, le système d'exploitation et les logiciels (navigateur, antivirus, bureautique, etc.) doivent être mis à jour régulièrement. En effet, les cyberpirates recherchent généralement des ordinateurs dont les logiciels n'ont pas été mis à jour afin d'en utiliser les failles non corrigées.
Enfin, toutes les données numériques, que ce soit sur les serveurs ou par courriel, peuvent faire l'objet d'un chiffrement. L'utilisateur peut mettre les techniques de chiffrement en œuvre lui-même, par le biais d'un certificat de signature qu'il détient, ou choisir un tiers de confiance dont le site sécurisé assure le chiffrement des données, dont il détient la clé de décryptage.
Une attention particulière doit être portée aux données à caractère personnel, abondantes au sein des cabinets d'avocats. En cas d'externalisation des serveurs, par exemple par le biais d'un service de *Cloud Computing*, le cabinet d'avocats, en tant que responsable du traitement

restera garant de la sécurité des données. En effet, l'hébergeur a la qualification de sous-traitant au regard de la loi dite Informatique et Liberté du 6 janvier 1978. Cependant, cette charge de responsabilité sera bientôt modifiée grâce au nouveau règlement européen 2017/679 relatif à la protection du traitement des données à caractère personnel, applicable au 25 mai 2018. En effet, le règlement prévoit que l'ensemble de la chaîne de traitement de données pourra être saisi et attrait dans une procédure de conformité ou de sanction. La responsabilité du responsable de traitement et de ses sous-traitants pourra ainsi être conjointe.

De quelle façon gérer l'archivage numérique des documents ?

La conservation des documents relève des obligations légales de l'avocat et s'inscrit dans le prolongement de ses obligations professionnelles déontologiques.

C'est ainsi que l'archivage est également touché par la migration vers un support numérique. Tout en restant vulnérables aux mêmes failles de sécurité que les autres documents, les questions d'authenticité et d'intégrité sont décuplées en particulier dans l'hypothèse des originaux nativement dématérialisés.

Il est donc essentiel de mettre en place une politique d'archivage décrivant clairement le cycle de vie de l'information ainsi que les garanties mises en œuvre pour assurer son intégrité.

Ce système d'archivage doit répondre à plusieurs exigences : la capacité à identifier l'origine de l'information et son intégrité (lisibilité et stabilité du contenu informationnel, traçabilité des opérations effectuées sur le document) ; respecter les éventuelles contraintes spécifiques (telles que l'obligation d'utiliser une signature électronique) ; et permettre la réversibilité des documents vers un autre système, en vue de la migration des données pour permettre leur conservation pendant la durée nécessaire.

En effet, la pérennité des supports est généralement bien inférieure à la durée légale d'archivage des documents. Dès lors, la mise à niveau périodique des systèmes et le remplacement régulier des supports sont indispensables. L'évolutivité du système doit pouvoir être assurée sans impact significatif sur la qualité du service rendu.

Pour pallier ces problèmes techniques et règlementaires, il peut être fait appel à un tiers archiveur. En ce cas, le cabinet devra s'assurer que le prestataire choisi est qualifié et pérenne, et présente des garanties de restitution (en fin de contrat ou en cas de défaillance).

En outre, la profession s'est dotée d'un outil spécifique en ce qui concerne l'archivage d'actes sous seing privé contresignés par un avocat : la plateforme numérique AvosActes, dédiée à l'enregistrement centralisé de ces actes d'avocat. Ce service permet la conservation numérique, l'archivage d'un exemplaire original et la retransmission de la copie numérique d'un acte, de façon sécurisée.

Comment s'assurer de la protection des communications entre avocats et juridictions ?

Les communications entre avocats sont elles aussi largement dématérialisées aujourd'hui. La profession s'est en conséquence rapidement mobilisée pour le développement d'outils permettant d'échanger tous types de documents dans des conditions optimales de sécurité et de confidentialité.

Ainsi, le Conseil national des barreaux a mis en place un intranet dédié à la profession d'avocat : le Réseau privé virtuel avocat (RPVA). Parallèlement, le CNB a créé la plateforme e-Barreau, portail unique donnant accès à différents services à ses abonnés.

Le RPVA comprend une messagerie électronique sécurisée, ainsi qu'une certification de la qualité d'avocat, ouvrant la voie à une signature électronique spécifique de la profession. L'accès se fait *via* le réseau Internet, et comprend la mise en œuvre d'un outil de chiffrement et d'un outil d'authentification.

Dans l'architecture développée par le CNB, l'outil de chiffrement se situe dans un boîtier « RSA », c'est-à-dire « routeur sécurisé avocat », placé en amont de la connexion à Internet du cabinet. Ainsi, un tunnel hautement sécurisé est établi entre le cabinet et la plateforme de services e-Barreau.

Quelle que soit l'architecture adoptée, le boîtier est doté d'un pare-feu, faisant l'objet d'une maintenance et d'une mise à jour quotidienne, et peut également être mutualisé au sein de structures d'exercice ou de moyens.

L'outil d'authentification, quant à lui, est un certificat électronique installé sur une clé USB cryptographique. Il fait office de carte d'identité professionnelle électronique de l'avocat, qu'il identifie lors de son accès aux services, et de « sceau numérique », lui permettant de signer électroniquement des documents.

Afin de s'assurer d'une utilisation sécurisée d'e-Barreau, il est essentiel de procéder à une mise à jour régulière du navigateur Internet.

La plateforme e-Barreau permet également d'échanger avec les juridictions. En effet, elle bénéficie aussi d'un point de connexion unique et sécurisé avec le Réseau privé virtuel justice (RPVJ). Ainsi, l'avocat peut régulariser les actes de procédure, échanger avec les greffes et communiquer ses pièces de façon dématérialisée et sécurisée.

Qu'en est-il de la protection des communications avec les clients ?

L'un des piliers de la profession d'avocat est le secret professionnel, qui couvre les communications verbales ou écrites échangées avec le client. Celui-ci est général, absolu et illimité dans le temps, s'applique dans toutes les matières du droit et dans tous les domaines d'intervention. Obligation légale et déontologique, sa violation est sévèrement sanctionnée.

Si aujourd'hui, la majorité des cabinets a choisi de troquer la plume pour le clavier, une étude récente révèle que rares sont ceux qui utilisent Internet pour sécuriser leurs dialogues avec leurs clients (étude menée par MyCercle, mars 2016).

Essentiellement, les sites de cabinets d'avocats sont de simples vitrines destinées à informer les futurs clients. En effet, selon cette même étude, seul 1 cabinet français sur 100 aurait équipé son site Internet d'un espace client sécurisé, à l'image des grandes institutions ou des sites marchands. Cet espace peut prévoir un espace de dépôt de documents, une messagerie dédiée ou tout autre service complémentaire. Surtout, il peut intégrer, outre une protection par identifiant et mot de passe, un cryptage des transactions (par exemple, avec le HTTPS) voire un certificat électronique.

Actuellement, les échanges avec les clients se font très majoritairement de manière non sécurisée, sans chiffrement, sous forme de courriels et de pièces jointes. Or, ceux-ci sont exposés tant au piratage qu'aux erreurs de destinataire.

Le Cloud privé des avocats, lancé en mars 2016 par le CNB, apporte une solution à ce problème, en proposant, parmi une gamme de services, une messagerie électronique permettant l'envoi de messages sécurisés à destination du client, avec mot de passe unique et cryptage.

À l'inverse, lorsque les avocats sont destinataires du courriel, certaines précautions doivent impérativement être prises lors de leur réception. En effet, les courriels et leurs pièces jointes sont souvent des vecteurs de risques (messages frauduleux, pièces jointes piégées, etc.). Il faut donc vérifier la cohérence entre le contenu du message et son expéditeur présumé ; ne pas ouvrir les pièces jointes provenant d'émetteurs inconnus ; ne pas cliquer sur des liens hypertextes sans les avoir vérifiés (au besoin auprès d'un service informatique) ; et ne jamais communiquer d'informations personnelles ou confidentielles. ■

Pour aller plus loin

- Agence nationale de la sécurité des systèmes d'information (ANSSI) : http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/
- Conseil national des barreaux (CNB) : http://cnb.avocat.fr/
- Commission nationale de l'informatique et des libertés (CNIL) : http://www.cnil.fr/
- Agence européenne chargée de la sécurité des réseaux et de l'information (de son acronyme anglais ENISA) : https://www.enisa.europa.eu/