Temps de lecture : 1”30

Par Anne-Laure Joubaire

Les cabinets de services professionnels (avocats, notaires, experts-comptables…) manient des données ultra-sensibles et représentent à ce titre une des cibles favorites des cyber-criminels. Même si les protections ont été renforcées, la prise de conscience semble encore trop lente.

DES RISQUES MAJEURS

80% des entreprises françaises ont constaté au moins une cyber-attaque en 2018 selon le baromètre de la cyber-sécurité des entreprises du CESIN. Ces attaques sont pour près des ¾ du phishing (envoi de mails avec liens ou pièces jointes infectés), pour 50 % des fraudes au président et du rançongiciel pour 44 %. Si certaines attaques ont des effets immédiats (comme le déni d’accès au site ou la séquestration des données), d’autres peuvent être plus pernicieuses : certains hackers peuvent rester des mois, voire des années dans un système sans se faire détecter. Ils peuvent ainsi effectuer de l’espionnage industriel ou corrompre subtilement certains documents.

« Pirater une étude d’avocats présente l’avantage d’être peu coûteux à exécuter tout en offrant une rentabilité rapide. » Steven Meyer, co-fondateur de ZenData.

Ces attaques peuvent avoir des **conséquences dévastatrices pour les activités de services professionnels** (avocats, experts-comptables, notaires…) devant gérer des données sensibles : arrêt de l’activité, dédommagement des clients, risques judiciaires et surtout perte de crédibilité. Selon une étude PwC de 2017, 85 % des consommateurs américains refuseraient de travailler avec une entreprise dont ils ne seraient pas certains qu’elle protègerait bien leurs données. On peut gager que ce chiffre atteint quasiment les 100 % pour les clients B to B.

UNE PRISE DE CONSCIENCE GRANDISSANTE…

D’après une étude menée en 2019 par Robert Half Legal auprès d’avocats aux Etats-Unis, plus de 75 % d’entre eux prévoyaient d’augmenter leurs dépenses de cyber sécurité d’en moyenne de 20 %. Ils étaient seulement 41 % à répondre la même chose en 2017, progression qui démontre une nette prise de conscience de la réalité des dangers cyber.
Cette volonté se traduit concrètement puisqu’en 2019 68 % des cabinets interrogés par l’International Legal Technology Association (ILTA) ont conduit des tests phishing (vs 38 % en 2016). De plus en plus de cabinets ont également introduit des systèmes d’identification à double entrée (mot de passe et sms) pour l’accès à distance. Les professionnels de la cyber-sécurité témoignent également d’une augmentation du nombre d’experts recrutés au sein des cabinets ainsi que de la souscription d’assurances spécifiques. Conscientes de l’importance du partage d’informations dans la lutte contre ce fléau, les grandes firmes ont créé le réseau LS-ISAO tandis que l’ILTA a lancé l’initiative LEGAL Sec.

…MAIS UN FACTEUR HUMAIN TOUJOURS PORTEUR DE RISQUE

Malgré la hausse des investissements en cyber-sécurité (infrastructures, recrutement), les risques demeurent élevés, notamment à cause du facteur humain. En effet, élaborer des procédures de sécurité n’est en rien une garantie si les associés ou dirigeants négligent de les suivre par la suite en cliquant sur des liens infectés. Pour diminuer ces risques, deux solutions doivent être mises en place régulièrement : la formation et l’audit des risques (internes et externes).

POUR ALLER PLUS LOIN

Etat de la menace liée au numérique, Ministère de l’Intérieur, 2019

Baromètre Data Breach 2020

Accès à privilèges : les cabinets d’avocat plus que jamais sensibles aux tentatives de cyberattaque

Il est temps pour les études d’avocats d’assurer leur cyber défense

Précautions élémentaires – Recommandations ANSSI

Cybermalveillance.gouv.fr

Guide de la cyber-sécurité pour les experts-comptables

As hackers get smarter can law firms keep up ?