Temps de lecture : 1’30’’

LE PIRATAGE ÉCONOMIQUE EST UN PHÉNOMÈNE BIEN RÉEL, COMME LE PROUVE LA MULTIPLICATION DE « CASSES » RETENTISSANTS CES DERNIÈRES ANNÉES.

L’affaire a fait les gros titres de la presse juridique et économique. En 2016, des malfaiteurs, dirigés par un gouvernement étranger, avaient visé plus d’une quarantaine de cabinets spécialisés en fusions-acquisitions dont Cravath Swaine & Moore et Weil Gotshal & Manges, afin de leur dérober des informations stratégiques.

DES DONNÉES TROP PEU PROTÉGÉES

Étant amenés à traiter de dossiers sensibles tels que des fusions, des litiges complexes ou encore des audits comptables, les cabinets de service sont des cibles privilégiées pour les pirates. Ces derniers recourent à des techniques de plus en plus sophistiquées : cryptage des données avec demandes de rançons, usurpations d’identité, *phishing*, transmission de virus, etc.

Être piraté induit des risques majeurs quant à la responsabilité juridique du cabinet (*cf affaire Johnson&Bell*), sa notoriété et surtout la confiance du client.
Pourtant, peu de cabinets protègent leurs données de manière adéquate. En effet selon Law360 : « 90 % des cabinets juridiques n’emploient que cinq personnes, voire moins, pour gérer la sécurité de leurs données. »

En mettant en place une politique de sûreté solide et en la faisant certifier, les cabinets peuvent donc gagner une longueur d’avance sur leurs concurrents.

ANTICIPER LE RISQUE ET S’EN PRÉMUNIR :

QUELQUES CONSEILS PRATIQUES D’ELIOTT & MARKUS

Si le piratage est impossible à éviter, les dégâts, eux, peuvent être limités.
Tout d’abord, il convient de f**aire appel à une équipe externe** au fait des techniques les plus pointues, afin de surveiller le trafic, détecter les intrusions, évaluer l’étendue des dommages et élaborer un protocole de confinement.

Comme le travail des pirates est souvent facilité par des **failles internes** (intentionnelles ou non), il est crucial de **sensibiliser les collaborateurs** aux risques de piratage de manière ludique et/ou pratique, avec de fausses tentatives de phishing par exemple.
Eviter les fuites internes passe aussi par la restriction de l’usage des clés USB, la modification fréquente des mots de passe, la sécurisation des fax, la désactivation des comptes des ex-collaborateurs ou encore l’interdiction d’utiliser Gmail/Yahoo/Dropbox.

Parallèlement à ces premières mesures, il faut veiller à **circonscrire les dégâts**. Pour cela, il est vivement conseillé que chaque collaborateur ne puisse avoir accès qu’à ses dossiers, et ce, afin de réduire la quantité d’informations accessibles à un pirate externe.
En cas de fuite interne, cette précaution permet d’identifier le responsable rapidement.

La **sécurité des partenaires** devrait également être auditée régulièrement : plus de la moitié des brèches constatées résultent d’un niveau de sûreté trop faible des parties prenantes des cabinets.

Enfin, il est recommandé de s’appuyer sur une **infrastructure robuste**, en équipant le système informatique de parefeux et d’antivirus dernier cri testés et patchés quotidiennement, de serveurs cryptés, délocalisés et gérés par une équipe fiable, d’une plateforme interne de messagerie ou encore de bureaux virtuels.

POUR ALLER PLUS LOIN

Pirate informatique : quels risques pour les avocats ?

How to Protect Legal Clients’ Confidential Data, Nate Lord,

Safe and Secure: Cyber Security Practices for Law Firms,

Cybersecurity & Law Firms: A Business Risk,