L'AFFAIRE A FAIT EN 2016 LES GROS TITRES DE LA PRESSE JURIDIQUE ET ÉCONOMIQUE. DES MALFAITEURS, DIRIGÉS PAR UN GOUVERNEMENT ÉTRANGER, AVAIENT VISÉ PLUS D'UNE QUARANTAINE DE CABINETS SPÉCIALISÉS EN FUSIONS-ACQUISITIONS (CRAVATH SWAINE & MOORE, WEIL GOTSHAL & MANGES …) AFIN DE LEUR DÉROBER DES INFORMATIONS STRATÉGIQUES.

Temps de lecture : 3'30

Le piratage économique est un **phénomène bien réel**, comme le prouve la multiplication de casses retentissants (Mossack Fonseca) toujours plus ingénieux (piratage informatique, vol de documents physiques et de terminaux, usurpation d'identité, phishing…).

Les cabinets de service sont vus comme des **cibles stratégiques** de par la sensibilité des dossiers traités (transactions majeures, litiges complexes, audits comptables…) et la **faiblesse de protection** de ces données.

En effet, « 90% des cabinets juridiques n'emploient que 5 personnes ou moins pour gérer la sécurité de leurs données ».

Or être piraté induit des **risques majeurs**, pour la continuité des dossiers, la responsabilité juridique du cabinet (affaire Jonhson&Bells), la confiance du client et surtout pour la **notoriété du cabinet**.

Il est donc impératif de s'**appuyer sur une politique de sûreté solide,** qui permettra de circonscrire l'étendue des dégâts et servira d'atout pour **rassurer les clients.**

– Les failles sont majoritairement d'origine humaine. Il est donc crucial de **sensibiliser continuellement** vos collaborateurs à cet enjeu, de manière ludique (vidéos) ou pratique (fausses tentatives de phishing). Cela vous permettra également de montrer aux clients l'importance que ce sujet a pour le cabinet en entier et non pour les seuls informaticiens.

– **Eviter les fuites internes** :

- Sécuriser les fax,
- limiter autant que possible les clés USB,
- changer les mots de passe régulièrement,
- désactiver les comptes des ex-collaborateurs,
- proscrire l'accès à Gmail / Yahoo / Dropbox.

– **Circonscrire l'information** : chaque collaborateur doit avoir accès à ses dossiers, pas à celui des autres. En **personnalisant l'accès**, on réduit la quantité d'information à laquelle un pirate peut avoir accès en s'emparant de ce compte. En outre, si fuite il y a là, il est possible de retracer les personnes ayant eu accès à la donnée. Etablir une **cartographie des données** est également un outil d'aide à la décision efficace.

– Disposer d'une **politique de conservation de emails** écrite et respectée (suppression des emails au bout d'un certain temps, le plus court possible). Le piratage est impossible à éviter. Les dégâts, eux peuvent être limités.

– **S'assurer de la fiabilité des tiers :** Plus de la moitié des brèches constatées résultent d'un niveau de sûreté trop faible des parties prenantes des cabinets. Ils doivent donc être audités et testés régulièrement.

– **Disposer d'une infrastructure robuste :** Parefeu et antivirus de dernière génération, testés et patchés quotidiennement. Maintenance et mise à jour des dispositifs de sécurité de vos sites internet… copier régulièrement votre site internet. Serveurs cryptés, délocalisés et gérés par une équipe fiable. Plateforme interne de messagerie. Bureaux virtuels (ce qui transforme un terminal volé en coquille vide).

– **S'appuyer sur des moyens humains** : Choisir une équipe externe au fait des techniques les plus pointues, pour surveiller le trafic, détecter les intrusions, évaluer l'étendue des dommages, élaborer un protocole de confinement …

– **Crypter** tous les documents/mails et y adjoindre une **double authentification.**

– Faire **certifier selon un standard reconnu** votre politique de sûreté.

Peu de cabinets peuvent aujourd'hui garantir à leurs clients la sûreté de leurs données. En mettant en œuvre les mesures ci-dessus puis en communiquant dessus, **vous gagnerez un avantage majeur** sur vos concurrents.

POUR ALLER PLUS LOIN

A Brief History Of Law Firm Cyberattacks,

https://www.law360.com/articles/800579/a-brief-history-of-law-firm-cyberattacks

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

https://digitalguardian.com/blog/law-firm-data-security-experts-how-protect-legal-clients-confidential-data