Les entreprises suisses face au défi du vol de données

Dix mille cas par an. Le chiffre des infractions commises au sein des entreprises en Suisse et mesuré par KPMG est loin d'être négligeable. Gestion déloyale, vol d'argent, escroquerie, corruption… Tout cela constitue l'inventaire à la Prévert des malversations et autres fraudes survenues souvent dans le cadre feutré des banques, des cabinets de conseil ou de diverses institutions financières. Les PME de tous les secteurs d'activité sont bien entendu aussi concernées. La lecture de la publication *Actualités en matière de criminalité économique*, publiée au début de l'été par KPMG, spécialiste des prestations de services d'audit et de conseil, montre la relative impunité dont jouissent les collaborateurs malhonnêtes – les entreprises préférant dans l'immense majorité des cas régler discrètement le problème sans passer par une procédure judiciaire – et souligne la progression du vol de données, qui devient l'infraction principale subie par les sociétés helvétiques, notamment par les trente plus grandes d'entre elles. A noter que les fraudeurs sont en majorité issus des rangs de l'employeur, le *management* étant même impliqué dans presque 40% des cas de conduites répréhensibles. L'informatique d'entreprise – ses potentialités techniques, les professionnels qui s'en occupent – serait-elle aujourd'hui plus que jamais le talon d'Achille de l'économie privée?

GRÉGORY TESNIER

***LES ACTES MALHONNÊTES,** au sein des entreprises, sont avant tout le fait de fraudeurs issus de leurs rangs, 40% des cas étant imputables au personnel dirigeant.*

«Ce phénomène est nouveau et la Suisse compte parmi les principaux pays concernés en comparaison internationale», confirme haut et fort Philippe Fleury, responsable de l'unité forensique de KPMG en Suisse romande, en parlant des vols de données, devenus en 2012 le principal souci des entreprises helvétiques en matière de sécurité. Il corrobore également l'idée que l'informatique constitue un maillon faible difficile à gérer pour elles. Interrogée sur ce point, Jacqueline Reigner, directrice et fondatrice de Sémafor Conseil SA, cabinet d'experts en cybersécurité, complète ce propos et mentionne que «la majorité des risques à haut potentiel de nuisance se situe bel et bien dans le secteur informatique et que les sociétés les sous-estiment trop souvent par excès de confiance dans leurs équipes». KPMG, consciente de cette réalité, propose pour sa part à ses clients un modèle spécifique de prévention de la fraude, qui agit à plusieurs niveaux: la gouvernance (responsabilité des cadres), la stratégie (définition des risques), le risque (gestion), la sensibilisation (programme adapté) et la surveillance (mesure de l'efficacité de la stratégie mise en place). Posséder une telle méthode de prévention demeure un atout certain pour une organisation, qui découvre souvent trop tard l'acte malhonnête en bénéficiant d'une information reçue de collaborateurs, par l'intermédiaire d'un audit interne ou par hasard. Toutefois, le meilleur des dispositifs d'alerte n'arrivera jamais à supprimer tous les risques. Philippe Fleury, comme son collègue Paul Wang, directeur au sein de la même unité de KPMG, en conviennent. Tout comme Sami Coll, expert des questions de traçabilité et maître-assistant au Laboratoire de recherche de l'Institut des sciences de la communication, des médias et du journalisme de l'Université de Genève, qui insiste sur «l'impossibilité du contrôle total des données».

RECRUTEMENT DES INFORMATICIENS

Doit-on pour autant se résigner? Pas forcément, le salut venant peut-être d'ailleurs. De la gestion des ressources humaines, par exemple. Pour Sami Coll, le problème «est humain avant d'être technique». Dans la continuité, Jacqueline Reigner souligne que «pour réduire encore les probabilités d'être victime d'un vol de données et pour moins douter de ses équipes informatiques, il est nécessaire de s'intéresser de manière approfondie au processus de recrutement des professionnels de la technique. Et de poser les bonnes questions: cet ingénieur-réseau peut-il se prévaloir de bonnes références? Ce développeur a-t-il menti sur ses diplômes? Ce chef de projets possède-t-il un passé judiciaire? Etc. Plus que pour d'autres métiers, ces interrogations sont légitimes lorsqu'il s'agit d'informaticiens, quel que soit leur niveau de compétences. Evidemment, dans les cas de sous-traitance, tout cela est plus compliqué et, pourtant, théoriquement indispensable».

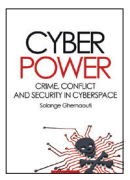
La directrice de Sémafor Conseil, qui est aussi présidente du Clusis, l'association suisse consacrée à la sécurité de l'information, est rejointe dans ces propos par plusieurs experts en gestion des ressources humaines. Karin Berney, directrice et fondatrice de HR@Work, insiste elle aussi sur l'importance de la vérification des références: «Un candidat qui refuse de communiquer le ou les noms de ses supérieurs hiérarchiques lors de la précédente fonction qu'il a occupée se met en difficulté. S'il n'explique pas dans le détail les raisons de son comportement et de sa réticence à donner les informations demandées – que l'on peut entendre en tant que professionnel du recrutement –, il convient d'écarter son dossier. Les données informatiques d'une entreprise représentent un enjeu si crucial pour les organisations qu'avoir un doute sur un collaborateur en contact avec ces informations correspond à un risque inacceptable». Carla Villafuerte-Griessler, *division director* de Careerplus IT, à Fribourg, agence qui concentre son activité sur le recrutement et la sélection de personnel qualifié dans le domaine informatique, mentionne que le niveau de vérification des parcours et des CV des candidats dépend aussi des secteurs dans lesquels ils sont censés évoluer par la suite. Les banques ou les multinationales seront plus exigeantes concernant le profil de leurs futurs employés. Mais cette exigence accrue est aussi une question de moyens financiers. «Bien sûr, les prestations en lien avec le recrutement ont un coût. Parfois, celui-ci semble élevé pour certaines entreprises, mais un engagement qui tourne mal aura des conséquences financières bien plus graves», argumente Carla Villafuerte-Griessler. Forte d'une expérience professionnelle de plusieurs années aux Etats-Unis, elle note également que les mentalités des deux côtés de l'Atlantique sont différentes. «Les Américains comprennent et acceptent la plupart du temps sans réserve l'investissement nécessaire en temps et en argent pour l'embauche d'un spécialiste IT. Ils ont intégré que les risques encourus sont trop grands pour supporter un comportement trop léger. La situation, en Suisse, évolue dans la même direction, mais avec du retard.»

TOUS LES EMPLOYÉS «TRACÉS»?

Si la sécurité informatique passe par un recrutement de qualité, les ressources humaines ont également un rôle à jouer dans le suivi au jour le jour des employés. Pour prévenir le vol de données, les équipes spécialisées peuvent par exemple s'inspirer des normes ISO 27000, comme l'explique Jacqueline Reigner. Ces directives ont trait aux meilleures pratiques concernant le *management* de la sécurité de l'information. Sami Coll rappelle pour sa part que la traçabilité peut avoir un effet préventif: «Pour un employeur, communiquer intelligemment et de manière raisonnable sur le fait que toutes les tentatives d'accès à des données sensibles sont enregistrées, cela dans l'intérêt de tous, impose un effet dissuasif aux plus mauvaises intentions». Bien entendu, certains criminels en puissance arriveront toujours au bout de leurs idées, malgré toutes les précautions prises. Toutefois, rien n'aura été fait pour leur faciliter la tâche. Et, comme l'affirme Charles Bélaz, directeur *ad interim* de Manpower Suisse, les personnalités des collaborateurs et leurs motivations, bonnes ou mauvaises, restent au cœur du système. Ces personnalités, il est possible de les sélectionner ou de les tester lors du processus de recrutement, mais elles évoluent au fil du temps et il sera toujours très compliqué de savoir ce qui se trame dans les esprits des uns et des autres. «Toutes ces réflexions montrent que cultiver une bonne ambiance de travail et un climat de confiance au sein d'une entreprise représente non pas une option, mais une nécessité pour une direction véritablement soucieuse de la sécurité de l'information et d'une bonne gestion des risques. La loyauté des collaborateurs s'obtient en partie à ce prix!» ■

A LIRE

Cyberpower
Crime, Conflict and Security in Cyberspace
Solange Ghernaouti
EPFL Press,
Collection Forensic Sciences, 2013
472 pages



Le cyberespace? Un vaste champ de bataille économique et militaire, dans lequel émergent et se développent de nouvelles formes de criminalité et de conflits. Solange Ghernaouti, professeure en systèmes complexes et cybersécurité à HEC Lausanne, experte internationale reconnue, décrypte cette réalité dans un ouvrage sorti ce printemps et qui offre des clés de lecture précieuses pour comprendre le monde actuel. L'auteure prévient: «La sécurité informatique est aujourd'hui plus que jamais devenue un réel enjeu de pouvoir. Les organisations se refusant à cette réalité doivent s'attendre, à plus ou moins court terme, à de très mauvaises surprises».