Protéger l'entreprise face aux actes cybercriminels

En un demi-siècle, c'est-à-dire du transistor aux données électroniques, l'irrésistible développement des échanges modifia de façon irréversible les règles des marchés. En particulier les Transports, la Logistique et la Supply Chain, premiers utilisateurs de ces nouveaux concepts. Un autre facteur amplifia ces processus, la possibilité technique de communiquer de façon instantanée des données électroniques dans le monde. Toutes ces évolutions impactent les consommateurs et ce, à tous les niveaux favorisant une « addiction » quasi automatique, qui engendre de nouveaux comportements contre productifs du consommateur.

©Leo Lintane-Fotolia

Le leader mondial dans le domaine de la cybersécurité (Symantec Corporation Nasaq Sym) dans son rapport annuel du 16 novembre 2016 sur les cyber-risques, présente ses résultats à partir d'un échantillon de 20.907 personnes réparties dans 21 pays dont 1.008 Français. Il est mentionné notamment *« le laxisme des utilisateurs français quant à leur sécurité en ligne tandis que les cyber-attaquants ne cessent de développer leurs compétences et la sophistication de leurs attaques. Plus de 3/4 des Français (77 %) savent qu'ils doivent activement protéger leurs informations en ligne, mais sont toujours enclins à cliquer sur des liens ou à ouvrir des pièces jointes de provenance douteuse. Les catégories les plus affectées par ces cybercriminels sont les 18-34 ans. 29 % d'entre eux en ont été victimes l'an passé.* Et de poursuivre : *Les internautes ont de plus en plus conscience qu'il est indispensable de protéger leurs informations personnelles en ligne mais n'ont pas envie de prendre les protections adéquates pour assurer leur sécurité »*, déclare Laurent Heslault, Expert en cyber-sécurité Norton by Symantec.

Quelques chiffres clefs

Les actions cybercriminelles sont si courantes qu'elles sont considérées comme un risque identique à celles du monde réel. Les faits marquants de l'étude Norton by Symantec :

- E-mail : 65 % des Français ont ouvert une pièce provenant d'un expéditeur non identifié,
- Gap générationnel : habitudes peu sérieuses de partage des mots de passe,
- Faille du mot de passe : même si une majorité des utilisateurs (58 %) affirme utiliser un mot de passe sécurisé sur chaque compte, quasiment 1/5 internaute (20 %) partage ses mots de passe avec d'autres personnes et nombre d'entre eux (42 %) ne voient pas le danger d'utiliser les même ''mots de passe'' sur plusieurs comptes,
- Manque de protection des appareils, vis-à-vis des ransomware et phishing messages.

©Conseilog

François Beaufils
Fondateur Conseilog, de la Commission Supply Chain Transport & Logistique (AFTE), membre d'Evolen et de Collin de Sussy
francois.beaufils@conseilog.eu

L'échantillon français reflète les données de 1.008 utilisateurs d'appareils mobiles de plus de 18 ans en France. La marge d'erreur pour l'échantillon français total est de +/-3,1 %. Les données ont été recueillies du 14 septembre au 4 octobre 2016 par Edelman intelligence.

Tour d'horizon des mesures prises à l'international

Au regard des résultats de cette étude, il convient de se poser la question ''sécurité'' sur l'entreprise française qui est confrontée à la numérisation de ses données électroniques. Les TPI/TPE et PMI/PME disposent-elles de moyens sécuritaires permettant de faire face à ce fléau qu'est la cybercriminalité ? Quelles sont les réactions à l'international ?

Etat-Unis

Faisant suite aux attentats du 11 septembre 2001 sur le territoire des Etats-Unis, une loi d'exception à caractère anti-terroriste a été promulguée le 26 octobre 2001, reconduite depuis à chaque élection présidentielle : le « Patriot Act » (USA Patriot Act Public Law 107-56 - 131 pages).
Cette loi vise à lutter contre le terrorisme et ses alliés, notamment *« le blanchiment d'argent servant [...] au financement du terrorisme menaçant non seulement la sécurité des Etats-Unis, mais aussi tout le système économique et financier mondial dont dépendent la prospérité et la croissance »*.
Les autorités américaines se sont érigées en gendarme vis-à-vis d'entreprises étrangères pour des faits commis hors de leurs frontières. Cette loi comporte des dispositions permettant d'accéder à tout moment, « sans autorisation judiciaire », aux données informatiques des entreprises ou des particuliers qui sont en lien avec les Etats-Unis.
Autrement dit, le risque de divulgation de vos données confidentielles (commerciales, juridiques, secrets de fabrication, privées etc.) dans un cadre de concurrence internationale est réel. Le fait que les données soient entreposées aux U.S.A. (i-Cloud), voire temporairement via un serveur américain, permet l'utilisation du Patriot Act.
En 2014, Microsoft (siège aux USA) a été sommée de céder aux autorités américaines les informations privées d'un client, bien que celles-ci fussent hébergées (i-Cloud) en Irlande.
L'achat du Groupe Norbert Dentressangle (avril 2015) par l'américain XPO Logistic implique le changement de nom, de nationalité et le transfert de l'ensemble des fichiers clients au siège social à Grenwich Connecticut (USA). Le piratage « massif » de plus d'1 Md de comptes chez Yahoo ! en 2013, reconnu seulement fin décembre 2016, confirme que tous les secteurs économiques d'intérêts sont des cibles.
La société américaine de cybersécurité Keeper Security, après analyse de 10 M de « mots de passe » en circulation, suite au vol de quantités massives de données, publie ces résultats :
- N°1 : pour 17 % des cas, le mot de passe est « 123456 »
- N°2 : « 123456789 » le mot de passe utilisé
- N°3 : « qwerty » le mot de passe utilisé

Union Européenne (U.E.)

L'accord USA/EU « Privacy Shield » devrait permettre de mieux protéger les transferts (de part et d'autre) des données privées. Les contrôles et les recours en justice seront possibles aux USA comme dans l'Union Européenne. En aucun cas, la question du « Patriot Act » n'a été résolue.

France

En France, la réforme européenne de la protection des données personnelles oblige certaines entreprises à désigner dès 2018 un délégué à la protection des données (Data Protection Officer – D.P.O.). Contrôles des règles et coopération avec l'autorité de contrôle

Douane - (O.M.D.) Statut de l'A.E.O/O.E.A. (2008)

2 piliers, celui de la « sécurité » et de la « sûreté », du personnel OEA en intra-entreprise sont obligatoires. Son implication est mondiale conformément aux accords de reconnaissances.
Favoriser les développements des échanges de biens marchands.

Suisse

Décision du 23 novembre 2016 : dans le cadre du nouveau système d'Echange Automatique de Renseignements (EAR) ; les Etats-Unis ne recevront pas d'informations bancaires de la Suisse.
La raison, le refus de Washington de garantir la réciprocité.

Russie

1er septembre 2015 : une loi russe impose aux sociétés de stocker, sur des serveurs localisés en Russie, les données personnelles de citoyens russes. Des géants du Web tels Ebay, Alibaba, Apple ou Uber ont accepté de se plier à cette règlementation.

LinkedIn (racheté par Microsoft pour plus de 26 Md$) ayant refusé son application fût condamnée en appel le 10 novembre 2016. Le site n'est plus accessible depuis le 17 novembre 2016. Apple et Google ont retiré LinkedIn de leurs catalogues d'applications.
Ainsi, les Etats comprenant les enjeux de demain, tendent à défendre leur souveraineté en matière de données personnelles.

Minimiser les risques de cyberattaques

Comment s'organiser de façon à minimiser le risque d'être victime d'attaques de cybercriminels ? Les risques encourus sont : la destruction de données, les vols, l'indisponibilité du matériel informatique, la divulgation de fichiers commerciaux et clients, de sous-traitants, du personnel, de coordonnées bancaires, de l'identité de toutes les parties de la Supply Chain, de contrats commerciaux, de fichiers des détenteurs du capital, la perte de notoriété, de crédibilité, etc.
Comment assurer sa confidentialité ? Dans ce contexte, l'entreprise devra se réorganiser et créer des zones et des moyens de contrôle :

1. Classifier les différents degrés de confidentialité et établir des seuils d'accès aux informations au sein de l'entreprise. Déterminer les enjeux à tous les niveaux de son organisation.

2. Donner la priorité à la formation des personnels intra et extra entreprise. Mise en œuvre des bonnes pratiques (Agence Nationale de la Sécurité des Systèmes d'Information – Anssi-, Guide Hygiène informatique (www.ssi.gouv.fr), Sécurisation des données informatiques gratuit), de la sécurité informatique, des process de recrutement, d'une politique d'acquisition de Normes ISO, statut de l'O.E.A., etc.

3. Une vigilance quasi continue sur les différents points ci-après :
- La nationalité du serveur,
- La nationalité de l'hébergeur,
- La nationalité de chacun des maillons de la chaîne des fournisseurs,
- Quel est le droit reconnu dans ses conditions générales de vente ou d'achat ?

4. Une mise en réseau intra-entreprise des différentes fonctions susceptibles de neutraliser toutes interventions.
Il appartient à l'entreprise de produire, une analyse de risques, d'établir une veille permettant d'obtenir une sécurité juridique. Pour ce faire, il faut déterminer systématiquement :
- la nationalité des opérateurs européens,
- le lieu de l'archivage et du stockage des données sensibles. Des solutions d'archivage et de stockage des données électroniques existent en France et dans l'U.E. Il appartient aux entreprises de choisir au mieux de leurs intérêts et ce, sans aucune limite.

Information sur l'extraterritorialité de la législation américaine

Le rapport parlementaire de P. Lellouche et K. Berger, le 5 octobre 2016, a fait état du développement des procédures initiées « en task force » par les différentes administrations américaines à l'encontre des filiales de groupes étrangers établies sur le territoire. Exemple de mesure sur le blanchiment de l'argent : le Congrès a voté (2010) le Fatca (Foreign Account Tax Compliant Act) qui contraint les banques étrangères dans le monde entier, à livrer des informations nominatives sur leurs clients américains sans limite de territorialité.
Verrouiller l'accès à l'entreprise aux éventuels intrus tel est le challenge. ■

© Leo Lintang-Fotolia