Sortir du syndrome de Kaa et protéger ses données

Philippe LOUDENOT
Cyber Security Strategist - BlueFlies
Senior Advisor - CyberCercle

Allez Zou ! un petit tour en « Amnésie »…

Si en 1884, dans le livre originel de Rudyard Kipling, *Le Livre de la Jungle*, Kaa est un ami de Mowgli, il devient en 1967, dans le célèbre dessin animé de Walt Disney, un de ses prédateurs avec une phrase marquante : « Aie confiance, crois en moi ». On peut se demander si on ne se retrouve pas dans cette même situation avec le numérique où la confiance est régulièrement invoquée ou mise en avant.

Avec l'explosion du numérique, les échanges se multiplient entre citoyens, citoyens/entreprises, citoyens/administrations, entreprises/entreprises, administrations/administrations et tout cela avec une confiance ou des gages de confiance plus ou moins annoncés.

Mais qu'en est-il réellement ? Y aurait-il un piège ? Quelle méfiance devrions-nous avoir devant cette confiance annoncée ? Quels sont les risques ? Confiance et risques seraient donc les deux faces d'une même médaille ?

« Le trop de confiance attire le danger » Pierre Corneille, Le Cid

Gérer la confiance numérique consiste à identifier le niveau de risque que l'on est prêt à prendre avec les données que l'on traite ou qui nous sont confiées, dans un cadre professionnel ou personnel. Mais, souvent, une confiance « aveugle » est faite dès lors que l'on réalise une action par voie numérique, sans mesurer, ni cerner avec précision la gravité potentielle ou avérée des conséquences.

S'agissant des données, ce que l'on appelait il y a encore peu la « sécurité des systèmes d'information » promouvait la protection des données. Avec l'avènement de la cybersécurité, il semblerait que seuls les spécialistes de l'intelligence économique ou les délégués à la protection des données traitent de cet aspect.

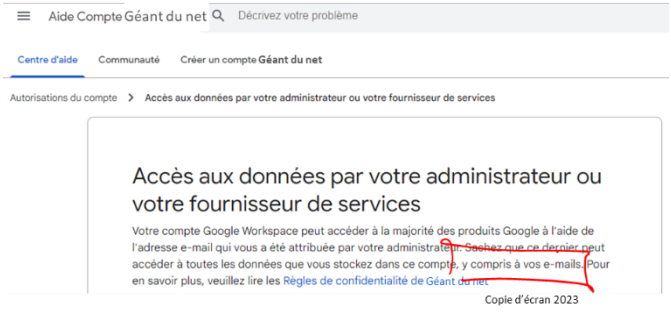
Pourtant, depuis l'Antiquité, les hommes ont éprouvé le besoin de protéger certaines informations.

La crainte de voir certaines informations interceptées fut à l'origine du développement de procédés le plus souvent appelés codes ou chiffres. Le secret des correspondances et les enjeux d'accéder à certaines informations ont entrainé la création par Henri IV d'un « Cabinet Noir » qui devint par la suite le « Cabinet du secret des Postes » en charge d'intercepter les correspondances. Dans l'histoire de la cryptologie et des moyens de protéger les informations, un message, le radiogramme de la Victoire décrypté par le Capitaine Paivin, aurait fait dire à Clémenceau « qu'à elle seule, l'équipe du chiffre valait tout un corps d'armée ». A titre anecdotique, ce message fut incorporé sur le premier « logo » de l'ANSSI qui avait proposé un challenge de déchiffrement. Connaissant l'importance historique de ce message, certains ont donné le résultat quasi immédiatement. Mais sans aucune recherche de déchiffrement, simplement en préjugeant que ce message était un symbole et que cela

ne pouvait être autre.

Tout individu, toute entreprise est à même de collecter, rédiger, traiter et communiquer des données.

Et ce, en interne comme à l'extérieur. Cependant, et particulièrement avec le numérique, ces contenus sont parfois mal maîtrisés, et représentent ainsi une menace à court comme à long termes. Si autrefois les informations sensibles étaient envoyées sous pli, aujourd'hui elles le sont par mail. Si certains opérateurs proposent des messageries dites sécurisées, il y a quelques années un géant du web avait pourtant annoncé lui-même avoir renoncé à scanner le contenu des boites mail de ses utilisateurs pour personnaliser les publicités. Ceci, bien sûr, dans un souci de confidentialité et de sécurité. Les employés peuvent également lire des e-mails, mais uniquement dans "des cas très spécifiques où vous nous demandez et donnez votre consentement, ou lorsque nous en avons besoin à des fins de sécurité, comme enquêter sur un bogue ou un abus", a déclaré le même géant. Et si ce n'est lui, cela peut être un autre…



Si exposer sa vie privée sur Internet ne semble pas poser de problème, toute personne peut également être amenée à envoyer par mail, en « toute confiance », copie de pièces d'identité, bulletins de salaire, déclarations fiscales ou données de santé. En « toute confiance » parce que les demandeurs sont des « professionnels » : banques, assureurs, collectivités, administrations… Les données personnelles se retrouvent ainsi désormais à des endroits que l'on ne saurait imaginer… et des fuites d'informations confidentielles peuvent arriver à tout moment. Pour mémoire, une fuite ou une violation de données personnelles est l'accès ou la divulgation non autorisés d'informations personnelles détenues par un tiers (sites Internet, services en ligne, entreprises, associations, collectivités, administrations). L'origine de la fuite peut être accidentelle ou malveillante, interne ou externe à l'organisation qui détient ces données. Voici aujourd'hui ce que l'on peut retrouver aisément en vente sur le Dark web : dates de naissance, passeports, numéros de carte de crédit, données biométriques, numéro de sécurité sociale, adresses, documents financiers, photographies, numéros de permis de conduire, numéros de téléphone…

Dans la catégorie des entreprises (pris ici au sens large), combien d'entre elles envoient aujourd'hui par mail leurs données stratégiques, leur bilan comptable, leurs projets de R&D, des résultats d'audit… ? Et il est illusoire de croire que la protection de l'information en entreprise ne vaut que pour les données sensibles. La protection de l'information doit également porter sur toute indication utile et pertinente relative à l'activité de l'entreprise, y compris celles postées sur les réseaux sociaux permettant des tentatives de « fraude au président ». Il est primordial de s'assurer que l'ensemble du personnel est parfaitement conscient de la manière d'assurer la sécurité des informations dans une entreprise. Les éléments à protéger doivent être clairement Identifiés afin d'éviter les fuites intentionnelles ou non, au risque de provoquer de nombreuses fuites causant des dommages irréversibles.

Quelques règles de bonne pratique permettent pourtant de protéger les informations.

Une règle de base : assurez-vous au niveau personnel que vous et votre entourage êtes conscients des données mises en pâture lors des échanges, et au niveau professionnel que l'ensemble des personnels d'une structure est lucide sur les données sensibles produites ou confiées.

Pour ce faire :

- Sensibilisez périodiquement le personnel, si besoin en faisant appel aux services de l'Etat (Gendarmerie, DGSI, DRSD…).
- Organisez un schéma de circulation de l'information et instaurez une culture de l'échange au sein de l'entreprise : avant de diffuser une information, il faut absolument en mesurer les impacts.
- Choisissez le support de diffusion.

- Vérifiez à qui vous partagez l'information.
- Mettez en place des solutions de confiance pour protéger vos mails et transferts de fichiers, mais qui sont simples si vous tenez à ce qu'elles soient utilisées.
- Montrez l'exemple.

La meilleure manière de protéger vos informations passe ainsi par la mise en œuvre de bonnes pratiques pour les politiques et procédures de sécurité de l'information à l'échelle d'une organisation.

Sinon, ayez confiance, continuez à envoyer mails et pièces jointes en clair… ça va bien se passer ;-)