TEMPS DE LECTURE : 2’50

ALORS QU’IL NE RESTE PLUS QU’UN MOIS POUR SE METTRE EN CONFORMITÉ AVEC LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES, PEU D’ENTREPRISES LE SONT. CES MANQUEMENTS EXPOSENT POURTANT LES ENTREPRISES À DES RISQUES JURIDIQUES, RÉPUTATIONNELS ET FINANCIERS MAJEURS. IL EST PLUS QUE TEMPS DE PROTÉGER LES SECRETS DE VOS CLIENTS AUSSI DANS L’UNIVERS NUMÉRIQUE.

Par Anne-Laure Joubaire

UN CYBER PANORAMA PEU RASSURANT

Selon un baromètre effectué par le CESIN, 92% des entreprises sondées ont affirmé avoir subi au moins une cyber-attaque en 2017 et la moitié d’entre elles ont remarqué une hausse significative de l’intensité des attaques par rapport à 2016. Ces chiffres sont alarmants et devraient pousser toutes les structures et plus particulièrement les petites, visées à 80%, à revoir en profondeur leur stratégie cyber.

Dans le panel d’attaques possibles, viennent en premier les logiciels malveillants ou ***malware*** puis les **spams** visant à obtenir de l’argent ou des données bancaires. Parmi les techniques gagnant d’ampleur, on relève notamment les **logiciels rançons** ou la **fraude au président**, qui consistent à soutirer de l‘argent à une entreprise en bloquant les ordinateurs pour la première et en usurpant l’identité du dirigeant pour la deuxième. Enfin les attaques de déni de service peuvent paralyser votre site internet pendant des heures.

Les cybercriminels cherchent également à profiter des failles des nouvelles technologies que sont le cloud, les objets connectés, les assistants vocaux ou encore les cryptomonnaies. Un hacker a ainsi réussi à pirater la base de données d’un casino américain via un thermomètre connecté présent dans l’aquarium du casino !

DES RISQUES ELEVES

La portée d’une cyberattaque va généralement bien au-delà de la paralysie du site ou de la perte des données puisque même lorsque le problème est solutionné rapidement, il entraîne des conséquences lourdes tant au niveau réputationnel que financier. En moyenne une attaque **coûte en effet 773.000 euros** à l’entreprise. A partir du 25 mai, toute entreprise collectant des données personnelles et qui se les fait dérober pourra se voir infliger des **amendes allant jusqu’à 4% du CA mondial** si le système de sécurité (ou celui de leurs sous-traitants) ne respecte pas le protocole du RGPD et/ou si l’entreprise oublie de prévenir les propriétaires de ces données. A cette menace vient s’ajouter le **risque juridique** puisque des clients pourront lancer une action de groupe. **Il revient en effet à l’entreprise de constituer à l’avance la preuve de sa conformité avec le RGPD** et de sécuriser les données personnelles collectées.

Ces risques sont d’autant plus élevés que les professionnels des services que sont les avocats, les experts-comptables ou les gestionnaires de patrimoine sont amenés à gérer des informations **très sensibles** sur leurs clients et sont donc des cibles de choix pour les cyber-criminels.

DES MESURES A METTRE EN PLACE DES QUE POSSIBLE

Les sites internet collectent un ensemble de données gigantesque via différents outils : cookies (traceurs d’activité), formulaires de contact, newsletters ou encore les espaces personnels des clients. A partir du 25 mai il sera obligatoire de proposer l’option de refuser ou non les cookies, d’en préciser la finalité, de vérifier l’accord de réception de la newsletter et d’informer le propriétaire des données de l’usage qui en sera fait. Les entreprises devront mettre en place un **registre des activités de traitement** comprenant le délai d’effacement de ces données, leur transfert éventuel à l’étranger ou encore les **mesures prises pour les sécuriser**.

Les obligations imposées par le RGPD sont une occasion en or de revoir votre cybersécurité, un domaine trop souvent négligé, faute de temps ou de moyens. Or pour l’avocat Daniel Kadar « *la cybersécurité et le RGPD sont les deux faces d’une même médaille : se conformer au RGPD permettra à l’entreprise de se prémunir des cyber attaques* ».

Parmi les mesures à prendre, citons la **cartographie** de vos SI et des données collectées, le renforcement des procédures d'**authentification** des collaborateurs ; la mise en place d'un **chiffrement** solide (via le protocole HTTPS) ; la **formation des employés** ; le renforcement de la gouvernance avec la désignation d'un **Délégué à la Protection des données**. Enfin il faut bien sûr procéder à un **audit complet et régulier** de vos systèmes d'information, du wifi et du cloud ainsi que de ceux de vos sous traitants.

POUR ALLER PLUS LOIN

Piratage informatique : un risque majeur

Guide des bonnes pratiques de l'informatique, ANSSI .

Cybersécurité et RGPD : « il ne doit pas y avoir de zones grises », LJA

Entreprises : les clés d'une application réussie du GDPR, Guide réalisé par le CIGREF, l'AFAI et TECH IN France à l'aide d'August Debouzy, De Gaulle Fleurance & Associés, Osborne Clarke et SAMMAN

Guide pratique : Les avocats et le règlement général sur la protection des données, CNB