RGPG Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

	RGPD Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

Philippe Carrère, directeur de la protection des données et de l'identité, Europe du Sud chez Gemalto revient sur le nouveau règlement européen sur la protection des données personnelles et ce qu'il implique pour les entreprises en termes de stratégie de sécurité et de relation client.

L'adoption récente du règlement européen sur la protection des données personnelles constitue un tournant pour les entreprises implantées dans l'Union Européenne. En effet, il exige des gestionnaires d'infrastructures et des fournisseurs de services numériques – tels qu'Amazon ou Google – de faire part d'éventuels vols de données et de mettre en place des mesures de sécurité adéquates. Les chefs d'entreprises devraient y voir là un avertissement et commencer dès à présent à évaluer leurs politiques de sécurité, avant que la proposition de loi ne soit approuvée par le Parlement et le Conseil européen.
Où en sont les entreprises européennes en termes de sécurité des données et quelles mesures doivent-elles prendre afin d'être conformes ? A l'heure actuelle, les pare-feu, les antivirus, le filtrage de contenu et la détection des menaces sont les principaux outils utilisés pour se prémunir des vols de données. Ces mesures sont, cependant, insuffisantes, les hackers pouvant franchir aisément ce premier périmètre de sécurité. Dès lors, l'adresse IP des entreprises ou encore les informations de leurs clients peuvent être compromises, comme ce fut le cas avec Volkswagen et la conception de sa Passat.
D'après le Breach Level Index réalisé pour l'année 2015 par Gemalto, plus de 707,5 millions de dossiers clients ont été volés ou perdus à la suite de 1 673 cyberattaques menées de par le monde. Un chiffre qui devrait faire l'effet d'un véritable électrochoc pour les responsables informatiques, d'autant que, fait encore plus inquiétant, 4 % des infractions ont impliqué des données sécurisées (chiffrées partiellement ou en totalité).
Les clients confient des données confidentielles, et ils doivent donc être assurés et convaincus de leur sécurité. Si le lien de confiance avec le client vient à être brisé, il peut être très difficile pour les entreprises de le renouer.
Une de nos récentes études a révélé que plus de la moitié des individus interrogés (57 %) ne traiterait jamais, ou très peu probablement, avec une société ayant perdu des données personnelles suite à une cyberattaque.

Pourquoi ce règlement apparaît aujourd'hui comme une nécessité ?
La sécurité a toujours été un sujet d'actualité, mais suite aux récentes attaques, comme celle de Talk Talk, et le fait que de plus en plus de données personnelles sont collectées en ligne, assurer leur sécurité et maintenir une relation de confiance avec les clients n'a jamais été aussi primordial. A l'heure actuelle, les entreprises européennes ne sont pas tenues de signaler les brèches de données dont elles peuvent faire l'objet, et, de fait, grand nombre d'entre elles ne le font pas. Une fois la nouvelle réglementation en vigueur, elles seront dans l'obligation de révéler ces violations, sous peine de se voir infliger une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. C'est pourquoi elles doivent dès à présent opérer un changement de stratégie.
Cependant, il ne s'agit pas là d'un fait nouveau. Cette pratique est déjà en place depuis plusieurs années aux Etats-Unis. C'est pourquoi nous entendons davantage parler des cyberattaques ayant lieu outre-Atlantique que celles se produisant près de chez nous.

Quels sont les principaux enseignements à en tirer ?
Au lieu de se concentrer uniquement sur la protection du périmètre de sécurité, les entreprises devraient plutôt adopter une approche segmentée, protégeant les données à tous les niveaux et barrant le passage aux hackers qui auraient franchi le 1er palier de défense. Cela signifie également que la priorité doit porter sur les données elles-mêmes et sur le fait qu'elles ne puissent être consultées ou utilisées par des personnes non autorisées. Protéger les données par des solutions de chiffrement de bout en bout, d'authentification et des contrôles d'accès permet d'ajouter un niveau de sécurité supplémentaire. En mettant en place des outils de chiffrement, les données subtilisées n'ont plus aucune valeur pour toute personne non autorisée. L'accès peut être sécurisé en utilisant des clés permettant aux personnes habilitées de consulter les informations. Ainsi, en cas d'attaque, les entreprises sont certaines de garantir la sécurité des données de leurs clients.

Informer les clients
Une fois ces mesures sécuritaires mises en place, il est important d'en informer les clients et de les rassurer quant à la pertinence des processus instaurés pour protéger leurs données. Si les entreprises peuvent démontrer qu'elles sont prêtes à se dépasser et à mettre toute leur énergie dans cette démarche, elles seront perçues comme innovantes et dignes de confiance.
La sécurité est un effort mutuel. S'il est important d'informer les clients sur le travail qui est fait pour assurer leur sécurité, il est tout aussi primordial qu'ils sachent comment se protéger eux-mêmes. De plus, s'adresser à un utilisateur averti permettra de lui proposer un meilleur service client.
L'adoption du nouveau règlement européen sur la protection des données donne aux entreprises la possibilité de prendre les devants et montrer dès à présent à leurs clients qu'elles prennent ce sujet très au sérieux. Elles ne doivent pas seulement se soucier d'être conformes ou pas, mais comprendre qu'il s'agit là d'une nécessité essentielle à leur réussite. Les utilisateurs sont de plus en plus conscients qu'ils confient des données sensibles aux entreprises, leur demandant, de fait, d'en être responsables. La montée en puissance de cette prise de conscience doit aller de pair avec un niveau d'exigence plus élevé vis-à-vis des structures hébergeant ces informations. Ne pas prendre ce sujet au sérieux pourrait non seulement être préjudiciable en cas d'attaque, mais également nuire à la confiance instaurée avec les clients. Perdre ce lien les incitera à se tourner vers des concurrents jugés plus fiables… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nouveau règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès | Solutions Numériques*