Découvrez l’accord qui autorise la surveillance des données informatique

	Découvrez l’accord qui autorise la surveillance des données informatique

Le Patriot Act est une loi antiterroriste qui a été adoptée par les Etats-Unis après le 11 septembre 2001. Promulguée dans l'urgence comme une loi d'exception, elle a été prolongée à deux reprises et est toujours en vigueur à l'heure actuelle. Le Patriot Act autorise l'administration américaine à accéder à tout moment et sans autorisation judiciaire aux données informatiques des entreprises ou des particuliers qui ont un lien, quel qu'il soit, avec les États-Unis. En pratique, cela peut poser de graves problèmes pour une entreprise ayant stocké ses données confidentielles ou celles de son client chez un hébergeur américain, même s'il s'agit d'une filiale localisée dans un pays différent.
Qu'en est-il alors des entreprises françaises ? Quelles solutions existent pour assurer la confidentialité des informations privées des entreprises ?

Le risque de fuite de l'information
Dans un environnement hyperconcurrentiel, les risques de divulgation d'informations confidentielles pèsent sur toutes les entreprises puisque chacune a une part de marché à défendre ou une image à préserver. Néanmoins, toutes ne sont pas forcément impactées par l'étendue du Patriot Act, cela va dépendre de leur système d'information (organisation, gérance, etc.). Aujourd'hui, le développement de logiciels et la gestion des systèmes d'informations sont souvent sous-traités partiellement ou totalement à des fournisseurs pour notamment réduire les coûts de gestion ou bien bénéficier du savoir-faire et l'expertise de spécialistes. Cependant, cette externalisation (en mode Saas ou autre) peut ouvrir la porte au Patriot Act en faisant le choix, délibérément ou par manque d'informations, d'un prestataire de services de nationalité américaine pour l'hébergement des données.
En outre, l'Agence Nationale de la Sécurité Américaine (NSA) bénéficie de l'accès direct aux informations stockées sur les serveurs américains, et même aux données des fournisseurs de services informatiques américains (et donc de leurs clients) dont les serveurs sont situés en dehors des Etats-Unis ! Rappelons qu'en mai 2014, Microsoft (société de droit américain relevant donc du Patriot Act) a été sommé de céder aux autorités américaines les informations privées d'un client, bien que celles-ci fussent hébergées en Irlande.

Qui des données issues d'Office 365?
Si l'on prend maintenant l'exemple des solutions Microsoft 365 (Outlook en accès web), les informations sont enregistrées et traitées par un serveur américain qui relève du Patriot Act. Les entreprises, en utilisant ces services, peuvent donc être espionnées et leurs informations sensibles exploitées. De plus, les autorités américaines qui n'ont aucune obligation d'informer les propriétaires des données consultées ni des modalités de conservation ! Ainsi, du moment où elles passent par un serveur américain, les données des entreprises ne sont plus considérées comme sécurisées et courent donc un risque non négligeable de confidentialité (au niveau de l'intelligence économique notamment). C'est un risque que l'on peut comparer au piratage informatique sauf que dans le cas Patriot Act, il s'agit d'une intrusion légale.

Assurer la confidentialité des données privées
Dans ce contexte, trois étapes apparaissent essentielles pour permettre aux entreprises de ne pas être sujette à cette éventuelle fuite de l'information, et pour s'assurer le contrôle sur l'accès aux données :
• **Faire le tri**
Dans un premier temps, il appartient aux entreprises de catégoriser leurs données, afin de cibler et de trier les informations sensibles, celles-ci pouvant revêtir de nombreux aspects : secret des affaires, communication financière et stratégique, brevets, éléments de recherche et développement, débats des conseils d'administration, mais aussi tout ce qui relève des échanges électroniques du quotidien.
• **Sensibiliser les collaborateurs**
Pour prévenir le risque d'être confronté au Patriot Act, on note aussi l'importance de la communication au sein même de l'entreprise pour informer et responsabiliser les collaborateurs à la sécurité des données. Cette sensibilisation peut éviter une soumission par négligence au Patriot Act, comme c'est le cas lors des échanges par email via des services de messagerie grand-public (webmails) qui sont très populaires, mais souvent américains. Ainsi, former ses employés aux enjeux de la confidentialité des données et aux conséquences que peuvent avoir certains de leurs actes virtuels, c'est protéger le capital informationnel de l'entreprise tout en instaurant de bonnes pratiques en matière de sécurité informatique.
• Être vigilant
Une fois les données catégorisées et les collaborateurs sensibilisés, l'entreprise doit être très attentive aux conditions de stockage de l'information dite sensible.
Le meilleur moyen de se protéger du Patriot Act américain consiste à être vigilant quant à l'origine de l'hébergeur et du serveur. Une vérification de toute la chaîne de fournisseurs – et pas uniquement du serveur – s'impose donc pour s'assurer que les données ne sont pas concernées par cette loi américaine.
Ainsi il faut que l'entreprise privilégie les opérateurs européens dont les serveurs sont situés sur le territoire européen. Dans le cas d'une entreprise française, il est bien évidemment préférable de choisir des prestataires à caractère souverain dont les serveurs sont localisés en France.
En effet, pour protéger l'information sensible de l'entreprise, la France et les acteurs européens créent des certificats (par exemple le Label Cloud Confidence ou le Label Cyber Sécurité France) dans l'idée de labéliser les services qui respectent le principe de conservation de l'information dans le cadre juridique européen.
Enfin, d'autres mesures classiques existent pour protéger ses informations privées : chiffrement des données, engagement de confidentialité, audits systématiques pour tester régulièrement la sécurité des logiciels utilisés, etc. Tous ces moyens de protection témoignent d'une véritable prise de conscience de la part des entreprises de la valeur critique de leurs données et de la nécessité de les protéger.
Par Nadim Baklouti, Directeur R&D Leading Boards (solution de dématérialisation des Conseils d'Administration), et Gaetan Fron, Directeur DiliTrust (service de datarooms électroniques).

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.informatiquenews.fr/le-patriot-act-et-la-securite-des-donnees-des-entreprises-francaises-nadim-baklouti-et-gaetan-fron-euqity-31046