bsi.

...making excellence a habit.™

ISO/IEC27018

Sauvegarde des données personnelles dans le cloud

Livre blanc

HDS

Résumé

La protection des informations confidentielles n'a jamais été une préoccupation aussi importante. De nombreux organismes nationaux et internationaux, y compris l'Organisation Internationale de Normalisation (ISO), les États-Unis et l'Union Européenne, prennent des mesures pour répondre à cette problématique. L'une de leurs initiatives communes est la norme ISO/IEC27018 et les contrôles supplémentaires qui étendent l'ISO/IEC27001 pour sécuriser les informations détenues par les fournisseurs de services cloud (CSP).
Qu'est-ce que l'ISO/IEC27018 offre spécifiquement aux clients de services cloud, et pourquoi est-elle si importante ?

La violation des données en chiffres

2,803,036
- chaque jour

1,947
- chaque minute

116,793
- chaque heure

32
- chaque seconde

L'exposition potentielle des données personnelles est une des préoccupations internationales. Le nombre croissant de violations de sécurité de haut niveau a attiré l'attention de la population sur la façon dont leurs données individuelles doivent être protégées. Si vous regardez la liste des violations et le nombre de personnes qui en ont été victimes, vous pouvez voir l'ampleur du problème : le bureau américain de la Gestion des Données Personnelles qui compte plus de 21 millions d'employés a été volé, et l'attaque de Carphone Warehouse au Royaume-Uni a affecté plus de 2 millions de clients. Celles-ci ne représentent qu'une infime partie des attaques ayant eu lieu sur une période de trois mois en 2015. En effet, McAfee a estimé que 800 millions de données ont été perdues en 2013.

Pourtant, les entreprises dépensent encore plus pour leur sécurité. Selon les chiffres de Gartner, les dépenses mondiales de sécurité informatique devaient atteindre 76,9 milliards de dollars en 2015.

Alors que beaucoup de gens se font de fausses idées avec l'image du hacker socialement inadapté, la plupart des attaques venant de l'étranger sont menées par des organisations criminelles sophistiquées ou des organisations parrainées par l'État, ce qui rend particulièrement difficile la prise de mesures pour y faire face.
Il y a un risque plus dangereux encore, celui de l'employé qui, délibérément ou involontairement, quitte une entreprise en la laissant vulnérable aux attaques. Ceux-ci sont plus dangereux car ils ne sont souvent pas signalés ou sont couverts. Selon la recherche de PricewaterhouseCooper[3], 75% des organisations qui souffrent d'incidents de sécurité commis par leurs employés ne font pas appel à la justice et n'engagent pas de poursuites judiciaires. Cela signifie que les clients de ces organisations sont également vulnérables et que les entreprises qui recrutent ces personnes ne sont pas conscientes de leur passé, et pourraient être vulnérables à d'autres attaques.

Il n'est pas étonnant de voir tant d'inquiétude à propos de la façon dont les données personnelles sont protégées, tant de craintes à propos du cloud et tant de réticence à confier des données aux CSP.

C'est pour ces raisons que l'Union Européenne, par exemple, envisage de nouvelles réglementations sur la protection des données dans le but d'harmoniser la situation juridique à travers le continent. Quand il s'agit de l'Europe, il existe une variété de lois locales sur la protection des données, ce qui rend particulièrement difficile le fonctionnement des fournisseurs de services cloud. Le cloud traverse les frontières internationales, tandis que les lois régissant la sécurité des données sont principalement spécifiques au pays.

[1] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [2] http://www.gartner.com/newsroom/id/2828722
[3] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

Une partie de la problématique concerne également la façon dont les organisations détiennent des données - il y a une séparation juridique quand il s'agit de fournisseurs de services cloud. Ils détiennent des données pour le compte de leurs clients, mais le client a la responsabilité légale de ce qui arrive à ces données.

C'est là que les craintes concernant les CSP sont vraiment centrées : ces derniers parlent de leur expertise en sécurité, du montant qu'ils consacrent à la protection des données et des barrières physiques qu'ils mettent en place pour prévenir les violations, mais il reste une inquiétude sous-jacente : les CSP vont-ils traiter les données confidentielles de la même manière que leurs clients le feraient ?

Alors que l'Union Européenne tente d'introduire une certaine cohérence dans le domaine de la protection des données, les États-Unis doivent faire face à une situation différente.

Aux États-Unis, il n'existe aucune loi nationale encadrant l'utilisation des données personnelles. Les différentes politiques des États peuvent également causer une certaine confusion.
Ceci est exacerbé par diverses exigences réglementaires exigées par différentes industries.
Tous ces facteurs se conjuguent pour rendre difficile la formulation d'une politique de données cohérente. En août 2015, l'Institut National des Technologies de la Normalisation a conseillé aux agences fédérales « d'utiliser les normes internationales pertinentes pour la cyber sécurité, lorsqu'elles sont efficaces et appropriées, dans les activités de mission et d'élaboration de politiques[4] ». Les agences gouvernementales utilisent de plus en plus ces normes, et tendent à exiger de leurs entrepreneurs et des chaînes d'approvisionnement qu'ils se conforment également aux exigences de diverses normes.

ISO/IEC27000

L'ISO a développé une famille de normes pour la sécurité de l'information qui fournit un cadre aux entreprises pour élaborer des processus et des procédures afin de répondre aux préoccupations en matière de sécurité de l'information dans l'ensemble de l'organisation.

La principale norme de ce groupe est l'ISO/IEC27001, qui est la norme la plus reconnue pour la protection des informations sensibles contre la distribution inintentionnelle et l'accès non autorisé.

Avec ses 114 points de contrôle, l'ISO/IEC27001 peut atténuer les risques liés à la collecte, au stockage et à la diffusion de l'information en :

- Permettant aux organisations de se conformer à l'augmentation des réglementations gouvernementales et aux exigences spécifiques de l'industrie
- Fournissant les exigences pour un système de management de la sécurité de l'information efficace
- Faisant croître les organisations en sachant que toutes leurs informations jugées confidentielles resteront confidentielles

[4] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf

La norme **ISO/IEC27018**

Pour apaiser les craintes supplémentaires créées par le cloud, l'ISO a lancé une nouvelle norme, l'ISO/IEC27018, à l'automne 2014. Les fournisseurs de services cloud peuvent adopter cette norme pour rassurer leurs clients sur la sécurité de leurs données. La nouvelle norme, qui est une extension des normes ISO/IEC27001 et ISO/IEC27002, fournit des conseils aux organisations soucieuses de la façon dont leurs fournisseurs de services cloud transmettent des informations personnellement identifiables (PII).

C'est un champ de mines' juridique pour les organisations et c'est l'une des raisons pour lesquelles les discussions de l'UE ont été si longues, mais certaines définitions juridiques devaient d'abord être établies.

L'élément clé est le PII; c'est la définition sur laquelle toutes les discussions bloquent. Les informations personnelles ont été définies comme toute information qui (a) peut être utilisée pour identifier le principal PII auquel ces informations se rapportent, ou (b) pourrait être liée directement ou indirectement à un PII principal.

Cela soulève une autre question : que signifie un 'PII principal' ? C'est plus délicat car certains pays considèrent cette entité comme la personne concernée. De même, il existe un certain flou concernant le terme de 'contrôleur PII', parfois appelé un contrôleur de données, mais le point central est que le contrôleur PII est la personne qui détermine les fins pour lesquelles ces données sont traitées.

Que contient l'**ISO/IEC27018**

Il existe plusieurs lignes directrices dans la norme. Selon la définition ISO, ces lignes sont :

- D'aider le fournisseur de services de cloud public à se conformer aux obligations applicables lorsqu'il agit en tant que gestionnaire PII, ces obligations incombent directement ou indirectement au gestionnaire PII.
- Permettre au gestionnaire PII de services de cloud public d'être transparent sur les sujets importants afin que les clients du service cloud puissent sélectionner des services de traitement des données PII basés sur le cloud et bien gérés.
- Aider le client du service cloud et le gestionnaire PII de cloud public à conclure un accord contractuel.
- Fournir aux clients des services de cloud un mécanisme pour exercer les activités d'audit et faire le point sur les droits et responsabilités en matière de conformité dans les cas d'audits de données de services cloud individuels hébergés dans un cadre multi-parties, l'environnement du cloud peut être impraticable techniquement et peut augmenter les risques des contrôles de sécurité physiques et logiques déjà en place.

Alors que ce sont des principes de bases, si nous regardons les détails de ce que cela signifie et comment ils peuvent aider les clients, nous pouvons voir que pour la première fois, il existe un vrai cadre pour le traitement des données personnelles. La norme ISO/IEC27018 s'assure qu'un fournisseur de services cloud documente la façon dont le traitement des données personnelles est géré, les procédures mises en place et la façon dont il réagit aux demandes des clients. Elle peut également aider à élaborer des accords contractuels plus solides.

Cela peut également aider le fournisseur de services cloud. La norme aidera à définir comment les CSP peuvent former le personnel sur les PII, mettre en place une procédure de documentation, placer et fournir des lignes directrices à suivre. L'ISO/IEC27018 fournira également une réelle transparence afin que les données personnelles, et la façon dont elles sont gérées, ne soient pas uniquement des pensées après coup.

L'organisation doit s'interroger sur trois domaines lors de la mise en œuvre de la norme.

- Existe-t-il des exigences légales et réglementaires qu'une organisation doit respecter, y compris les règles et réglementations spécifiques à son secteur d'activité ?
- L'adhésion à la norme ISO/IEC27018 comporte-t-elle des risques pour l'organisation ?
- Est-ce-que l'adoption d'une telle norme va à l'encontre des politiques et de la culture d'une entreprise ?

Conclusion

Il y a peu de doute sur le fait que l'industrie du cloud a besoin de normes pour fournir une sécurité de l'information adéquate et efficace. Selon un sondage de TrustE, réalisé fin 2014, 92% des internautes britanniques s'inquiétaient de la protection de leur vie privée; contre 89% en 2013[5]. La plus grande préoccupation demeure la possibilité pour les entreprises de recueillir et de partager des données personnelles. Les consommateurs exigent de plus en plus des entreprises qu'elles deviennent plus transparentes quant à la collecte, l'utilisation et la protection de leurs données en ligne.

L'arrivée de l'ISO/IEC27018 aide à concentrer l'attention de l'industrie sur la mise en place d'une sécurité accrue pour protéger les PII. La norme a déjà été adoptée par certains grands fournisseurs de services cloud : Microsoft l'a incorporé dans Azure, Office 365, Dynamics CRM et Global Foundation Services et les deux services Amazon Web et Dropbox ont également obtenu la certification ISO/IEC27018. De nombreux autres CSP vont suivre. Les organisations transfèreront de plus en plus les informations vers le cloud pour bénéficier d'une plus grande flexibilité de la technologie et d'une diminution de la demande de ressources, mais le niveau d'adoption sera élevé lorsque la sécurité, en particulier les problèmes de confidentialité, sera résolue.

La prochaine réglementation européenne assurera qu'une nouvelle approche de la vie privée sera à l'ordre du jour. L'ISO/IEC27018 aidera à fournir un ensemble de lignes directrices pour les clients et les fournisseurs de services cloud.

Ce ne sera pas un substitut aux réglementations nationales et internationales, et son adoption à grande échelle ne signifiera pas que les fournisseurs suivront automatiquement les demandes légales, mais ce sera une étape importante.

Pour en savoir plus sur les solutions de BSI pour aider votre entreprise à protéger ses données

Rendez-vous sur :

www.bsigroup.fr

[5] https://www.truste.com/about-truste/press-room/british-customers-online-privacy-more-important/

Pourquoi choisir BSI ?

BSI a été à l'origine des normes de sécurité de l'information depuis 1995, ayant produit la première norme au monde, BS7799, devenue ISO/IEC27001, la norme de sécurité de l'information la plus populaire. Et nous n'avons cessé de nous attaquer aux problèmes émergents tels que la cyber sécurité et la sécurité dans le cloud.

Chez BSI, nous créons l'excellence en construisant le succès de nos clients à travers les normes. Nous permettons aux organisations de mieux performer, gérer les risques et atteindre une croissance durable.

Depuis plus d'un siècle, nos experts combattent les mauvaises pratiques pour intégrer l'excellence dans la façon dont les personnes et les produits évoluent.

Nous faisons de l'excellence une habitude.

Pour en savoir plus
rendez vous sur : bsigroup.fr

bsi.
bsigroup.fr