Cyberrisques

Données sensibles dans le nuage

Les nouvelles technologies amènent leur lot de problèmes. Les capacités peuvent être initialement mal comprises, faisant naître des risques imprévus. C'est notamment le cas lorsqu'on confie des données sensibles à l'environnement infonuagique.

En raison du potentiel d'accès à des ressources informatiques peu coûteuses, hautement disponibles et flexibles, la migration des données vers l'environnement infonuagique est inévitable. Tant les fournisseurs de ces services que leurs abonnés doivent faire preuve de vigilance face à ces nouveaux risques. Les abonnés ont la responsabilité de choisir des fournisseurs qui observent des niveaux de sécurité appropriés aux types de données qu'ils leur confient. Les abonnés doivent également évaluer le degré de contrôle qui leur sera accordé au chapitre de l'autorisation des comptes d'utilisateur et de la définition des rôles, ainsi que la manière dont les données seront protégées, tant au repos qu'en cours de transmission. Il incombe aux fournisseurs de préciser le plus clairement possible comment ils traiteront et protégeront les données des clients.[1]

Pour atténuer le risque lié à la transmission de données sensibles dans un environnement infonuagique, il importe d'abord de s'assurer que les abonnés et les fournisseurs sont d'accord sur la protection offerte.

L'infonuagique ne peut atteindre son plein potentiel que s'il existe un équilibre entre la volonté de fournir les services avec souplesse et la nécessité d'isoler les ressources des abonnés de façon à garantir la sécurité adéquate des données. L'environnement de la base de données et les techniques d'isolation des données utilisées revêtent une importance essentielle lorsque des données sensibles sont traitées dans un environnement infonuagique.

Comme le précise le National Institute of Standards and Technology, les modèles « multi-instances » et « multi-locataires » sont des exemples d'environnements de bases de données infonuagiques. Les modèles multi-instances permettent un « système de gestion de base de données unique fonctionnant sur une instance de machine virtuelle pour chaque consommateur d'infonuagique ».[1] Ce modèle permet à l'abonné de contrôler les principales caractéristiques de sécurité, telles que la définition et l'autorisation du rôle de l'utilisateur.

Le modèle multi-locataires est un « environnement prédéfini pour le consommateur d'infonuagique qui est partagé avec d'autres locataires, généralement en étiquetant les données à un identifiant de consommateur ».[1] Pour offrir un environnement de base de données sécurisé, ce modèle dépend du fournisseur d'infonuagique. Le chiffrement sécurisé des données stockées n'est généralement pas offert dans ces bases de données partagées.

En recourant aux services d'un fournisseur de stockage infonuagique, un abonné pourrait être victime d'une atteinte à la confidentialité de ses données de deux façons, soit à la suite d'un incident de sécurité subi par lui-même, soit à la suite d'un incident de sécurité subi par le fournisseur.

Une récente cyberattaque visant Capital One en 2019 démontre à quel point la vulnérabilité du système de l'abonné permet d'accéder aux données stockées dans l'infonuagique. Alors qu'elle stockait les renseignements personnels des utilisateurs et les coordonnées bancaires dans le système d'infonuagique d'Amazon Web Services, Capital One a été victime d'une compromission de son infrastructure, ce qui a entraîné un accès non autorisé à ces renseignements.[2] Ce n'est pas le système d'Amazon Web Services qui a été attaqué. Cet événement a touché environ 100 millions de personnes aux États-Unis et quelque 6 millions au Canada.[3]

Le système iCloud d'Apple, qui permet aux utilisateurs d'Apple de sauvegarder les données de leur compte telles que photos, courriels, contacts, calendriers et autres, a été attaqué en 2014. À la suite de cette cyberattaque, les photos personnelles de nombreux utilisateurs, dont des acteurs d'Hollywood, ont été rendues publiques. En raison de la notoriété des personnes atteintes, l'attaque a fait l'objet d'une vaste couverture médiatique, mettant ainsi la question de la sécurité des données infonuagiques à l'avant-plan des préoccupations du grand public et soulignant l'importance de renforcer les comptes infonuagiques au moyen de mesures de sécurité supplémentaires.[4]

Les questions suivantes sont fournies dans le but de permettre une analyse des risques et des mécanismes de contrôle liés au traitement des données sensibles stockées dans un environnement infonuagique :

- Comment les données sensibles sont-elles protégées, tant en cours de transmission qu'au repos?
- Si on a recours au chiffrement, qui du fournisseur ou de l'abonné gère les clés de chiffrement?
- Les employés du fournisseur ont-ils accès aux données non chiffrées des clients?
- Comment est contrôlé et surveillé l'accès des employés du fournisseur aux données des abonnés?
- Quelles capacités d'authentification, d'autorisation et de gestion des accès des utilisateurs sont offertes? Qui du fournisseur ou de l'abonné contrôle ces fonctions?
- Dans les contrats avec les abonnés, quels mécanismes de contrôle de sécurité précis le fournisseur accepte-t-il de mettre en place? Sur son site Web? Dans sa publicité?

Ces questions ne sont nullement exhaustives, mais elles serviront de point de départ à un dialogue informatif avec vos clients au sujet de ce nouveau secteur de risque.

Pour de plus amples renseignements, prière de parcourir le site cnacanada.ca.

1 Guidelines on Security and Privacy in Public Cloud Computing (2011) En anglais seulement. Tiré de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
2 Guest Post: What the Capital One Hack Means for Board of Directors (2019) (En anglais seulement) Tiré de https://www.dandodiary.com/2019/08/articles/cyber-liability/guest-post-what-the-capitalone-hack-means-for-board-of-directors/
3 Capital One (2019) (En anglais seulement) Tiré de https://www.capitalone.com/facts2019/
4 Forbes (2014) (En anglais seulement) Tiré de https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/#d1ca2192de72