Comment sécuriser des données privées stockées et accessibles dans le nuage (cloud)

Principes concernés
Assurer la confidentialité et la sécurité, Comprendre l'écosystème existant

Introduction

En mettant en œuvre des sauvegardes, des politiques et des procédures adaptées, les données privées peuvent être stockées et accessibles en toute sécurité à partir de serveurs en nuage d'une tierce partie.

Termes clés:

- Les sauvegardes administratives se réfèrent aux politiques organisationnelles, procédures et à la tenue à jour de mesures de sécurité qui visent à protéger la confidentialité des informations, des données et de l'accès. Exemples : groupes d'accès, plans de gestion des risques et formation et gestion des effectifs.
- La sécurité dorsale se rapporte aux procédures et sauvegardes du côté du serveur (dans le cas de services en nuage d'une tierce partie) appliquées par les prestataires de services en nuage.
- Les services en nuage sont des installations gérées par des tiers qui stockent les données (par ex. Google Drive et G Suite, Dropbox, prestataires de courrier électronique comme Gmail et Outlook.com, Amazon S3, société d'hébergement sur le Web, etc.)
- Les données comprennent l'information des utilisateurs (par ex., données des patients), l'information programmatique (par ex. pour le suivi et évaluation), l'information numérique (par ex. documents textes, tableurs, présentations, graphiques) et communication numérique (par ex. courrier électronique, messagerie instantanée).
- Le chiffrement est une opération de traduction des données dans un autre code qui exige ensuite une clé numérique privée pour rendre ces données à nouveau lisibles.
- La sécurité frontale se réfère aux procédures ou sauvegardes

"Rappelez-vous que les mesures de sécurité techniques sont aussi bonnes que leurs utilisateurs humains. La technique de sécurité doit fonctionner dans le contexte où il est implémenté."

CLAYTON SIMS
Dimagi

mises en place par l'utilisateur qui restreignent l'accès aux applications et aux données auxquelles les utilisateurs se connectent.

- Les sauvegardes physiques restreignent l'accès aux terminaux, appareils et tablettes portables liés aux réseaux du nuage ou utilisés pour le recueil et la gestion de données. Par exemple, les contrôles d'accès aux postes de travail et aux appareils.
- Les sauvegardes techniques sont le matériel, le logiciel ou les mécanismes de procédures dédiées à la sécurité. Exemples : authentification en deux étapes et chiffrement.
- Des services tiers en nuage payants sont offerts par un organisme externe comme Google, Microsoft Corporation ou Amazon.com. Exemples d'application de stockage sur le nuage: Dropbox, Microsoft OneDrive et Google Drive.
- L'authentification en deux ou multiples étapes demande à l'utilisateur de fournir deux ou trois éléments d'authentification avant de recevoir l'autorisation d'accès : en général, un élément connu de l'utilisateur (par ex. un mot de passe) plus un autre élément (par ex., un code d'accès) L'authentification en plusieurs étapes peut inclure une authentification biométrique comme une empreinte digitale.

Description

La sécurisation des données, des appareils et des outils est cruciale pour protéger la confidentialité des données de l'utilisateur et s'assurer que les données organisationnelles ne sont pas compromises [http://digitalprinciples.org/resource/principe-8-assurer-la-confidentialite-et-la-securite]. De plus, les réglementations nationales et internationales se rapportant à la sécurité et la confidentialité des données (surtout concernant l'infrastructure de santé et les données personnelles) préoccupent de plus en plus de nombreuses organisations. Ces réglementations comprennent : la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, le Règlement général de l'Union européenne pour la protection des données et le Règlement de protection des données de la Coopération économique pour l'Asie-Pacifique [http://digitalprinciples.org/resource/principe-2-comprendre-lecosysteme-existant].

"Notre parti pris collectif est la minimisation des données. Mais les données valent des milliards de dollars de capitalisation boursière. Avouons cela. Il est naïf de penser que les groupes vont minimiser. Si c'est le cas, comment gérons-nous, définissons-nous, contrôlons-nous et utilisons-nous les données, surtout si nous voulons avoir une conversation sérieuse avec le secteur privé?."

WILLIAM HOFFMAN
World Economic Forum

[1] Kuo AM. Opportunities and Challenges of Cloud Computing to Improve Health Care Services. *J Med Internet Res.* 2011 Sep 21;13(3):e67. doi: 10.2196/jmir.1867. Disponible sur https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/.

[2] Yunchuan S, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks.* 2014 Jan 1;10(7). doi: 10.1155/2014/190903. Disponible sur http://journals.sagepub.com/doi/full/10.1155/2014/190903#.

Comment sécuriser des données privées stockées et accessibles dans le nuage (cloud)

Les services d'informatique en nuage (cloud computing) sont offerts par un service d'hébergement qui stocke et traite les données de l'utilisateur final tout en offrant des services de gestion de données sur Internet. Le stockage sur le cloud réduit le besoin de ressources financières et humaines au sein de l'organisation consacrées à la sauvegarde des données et au maintien de l'accès au serveur. Un service de cloud facilite la gestion des données et les applications à l'intérieur d'un réseau relié par l'intermédiaire d'appareils portables, d'ordinateurs et de tablettes.[1]

Toutefois, ces réseaux peuvent poser d'importants problèmes pour la sécurité frontale dans l'environnement de l'informatique en nuage. De multiples mesures de sécurité mises en place par les utilisateurs à divers niveaux doivent être instaurées pour restreindre l'accès, vérifier l'identité de l'utilisateur, préserver l'intégrité des données et protéger la confidentialité des données individuelles, Aller sur le cloud, c'est l'occasion de standardiser, répliquer et déployer des procédures robustes de sécurisation des données sur l'ensemble des réseaux.

Les organisations qui stockent leurs données par l'intermédiaire d'un service d'informatique en nuage tiers bénéficie de cadres de sécurité exhaustifs mis en œuvre par les prestataires de services en nuage réputés. À la différence des organisations d'utilisateurs ordinaires, les services en nuage tiers emploient des milliers de personnes pour la sécurité et appliquent des mesures de sécurités qui sont sophistiquées et bien financées. Pour encore mieux protéger l'intégrité et la confidentialité de données très sensibles dans le cloud, les utilisateurs doivent mettre en œuvre des mesures frontales de sécurité techniques, administratives et physiques.

Le présent guide décrit les mesures à prendre pour promouvoir une sécurité frontale moderne et robuste lors de l'utilisation de services tiers d'informatique en nuage. Alliées aux protocoles de sécurité exhaustifs mis en œuvre par les prestataires de services en cloud, ces pratiques offrent une couche supplémentaire de protection pour les données privées. Ces recommandations sont résumées à partir de références existantes, notées dans la section Ressources.

> "Considérez que toute information partagée par SMS non crypté peut être interceptée par les télécoms ou d'autres parties, telles que des agences gouvernementales, et toute information partagée via un shortcode peut être accessible par des agrégateurs tiers et des sociétés de marketing."
>
> PETER MICEK
> Access Now

Comment sécuriser des données privées stockées et accessibles dans le nuage (cloud)

FIGURE 1 : SAUVEGARDES TECHNIQUE, ADMINISTRATIVES ET PHYSIQUES POUR LA CONFIDENTIALITÉ DES DONNÉE ET LEUR INTÉGRITÉ

SAUVEGARDE	DE QUOI S'AGIT-IL?	Considérations	EXIGENCES
Authentification en deux ou en plusieurs étapes	Un élément que vous connaissez (par ex. un mot de passe) plus un autre élément (par ex. un téléphone portable avec un code d'accès). L'authentification en plusieurs étapes inclut un élément attaché à votre personne (biométrique)	Difficile à appliquer sur le terrain, peut être cher, tout dépend de la solution choisie.	Appliquez des mots de passe renforcés pour la première couche de protection. Utilisez un système de connexion unique basée sur le cloud (par ex Okta, OneLogin or Microsoft Azure Active Directory) pour gérer l'authentification sur les services en nuage.
Chiffrement	Opération de traduction des données dans un autre code qui exige ensuite une clé numérique privée pour rendre ces données à nouveau lisibles.	Les principaux fournisseurs de services en nuage chiffrent les données des utilisateurs en transit vers leur serveur et stockées sur ce dernier. Le chiffrement côté client, soit quand un utilisateur ajoute une seconde couche de chiffrement avant que les données ne soient stockées sur le cloud, n'est possible que pour les applications de cloud où les données sont stockées sous forme de fichiers, et non sous forme de registres (par ex. application non SaSS telles que Box ou Amazon Web Services). Outils de chiffrement [https://www.syncany.org] et GNU Privacy Guard [https://gnupg.org/].	Créez des clés de chiffrement pour les appareils, les données et les courriers électroniques. Développez et appliquez des pratiques de gestion au moyen de clés de chiffrement.
Groupe d'accès	Les utilisateurs sont regroupés en fonction de privilèges particuliers, selon leur rôle (par ex. accès en lecture, ou lecture/écriture).	Les utilisateurs peuvent demander des autorisations d'accès aux données et à la gestion des données qui ne sont pas adaptées à leur situation d'utilisateurs. La révocation de l'accès (par ex. désactiver l'accès lorsque quelqu'un quitte un programme ou ne doit plus avoir accès à celui-ci) exige un contrôle et des actions. Le transfert de droits d'accès par les utilisateurs, un problème significatif avec les systèmes de documents tels que Dropbox, peut entraîner un accès non autorisé en cas de gestion inadaptée.	Pour la majorité des utilisateurs, l'autorisation minimale est le défaut. Documentez les cas d'utilisation liés aux autorisations d'accès et de gestion des données pour les besoins de la transparence et pour obtenir l'appui des utilisateurs.

Processus

1. **Appliquez des principes de confidentialité des données** adaptées au niveau de sensibilité et de confidentialité des données stockées dans le cloud. Cette mesure peut être adoptée en appliquant des principes plus contraignants

pour des données très sensibles afin de protéger l'identité et l'information confidentielle. Les sauvegardes administratives (par ex. évaluation et gestion des risques, restrictions d'accès), les sauvegardes techniques (par ex. chiffrement des données, authentification par les utilisateurs) et les sauvegardes physiques (par ex. garder les appareils dans une salle fermée à clé) peuvent toutes servir à protéger des données très sensibles ou privées. (Voir Figure 1)

2. **Mettez en œuvre des sauvegardes de l'intégrité des données** pour protéger ces dernières de toute élimination, modification, fabrication ou dissémination non autorisée. Cette étape est cruciale en raison de l'interopérabilité des appareils et des systèmes lorsqu'ils utilisent des services en nuage. Authentifier l'identité des utilisateurs et fournir à ces derniers des niveaux d'accès aux données adaptées et des autorisations sur la base de leurs fonctions, l'accès par défaut étant le niveau d'autorisation le plus bas. (Voir Figure 1)

3. **Créer et documenter les politiques de sécurité des données de l'organisation.** La sécurité de l'information exige des sauvegardes administratives, techniques et physiques. Ces sauvegardes s'appliquent lors d'activités soit dans l'environnement de l'informatique en nuage soit dans un environnement traditionnel basé sur un serveur. Toutefois, lors de l'utilisation de services en nuage, les ressources qui étaient auparavant dédiées à la maintenance et à la sauvegarde du serveur peuvent désormais être employées à développer, documenter, soutenir et contrôler les processus de gestion de la sécurité.

4. **Procédez à une analyse de risque du réseau et mettre sur pied une stratégie de gestion des risques.** Chargez certaines personnes de la sécurité et de la gestion des risques. Organisez des séances de sensibilisation et de formation à la sécurité pour les utilisateurs de données, en vous assurant que le personnel comprend bien comment respecter les plans et procédures de contingence en cas d'urgence et d'incident de sécurité. Examinez les exigences en matière de localisation des données et envisagez quels adversaires éventuels (par exemple, des acteurs gouvernementaux) pourraient avoir accès aux données en raison

PROCESSUS

CONSEILS ET RESSOURCES

Privacy Recommendations for Information and Communication Technologies for Health and Development (Adapted from Global Pulse http://www.unglobalpulse.org/sites/default/files/Data%20Privacy%20and%20Security%20in%20ICT4D%20-%20conference%20report%20layout%20-%20FINAL.pdf)

1. Intégrez des mécanismes proactifs de confidentialité dans la conception des initiatives.
2. Soyez transparents avec les personnes dont l'information est collectée quant à l'utilisation de leurs données.
3. Faites en sorte que l'utilisation des données personnelles recueillies soit spécifique, juste et justifiée.
4. Réduisez à l'essentiel la quantité et le détail des données recueillies.
5. Appliquez les principes au temps de stockage et à la destruction des données.

d'obligations juridiques liées aux activités dans le pays, de traités d'assistance juridique mutuelle ou de demandes de données, ou par un accès physique au stockage des données ou au chiffrement dorsal [https://transparencyreport.google.com/user-data/overview].

5. **Contrôlez l'application et menez des audits de conformité.** Effectuez des audits périodiques pour repérer les failles de sécurité et contrôler la conformité. Créez et appliquez des politiques de gestion du personnel et une discipline liée aux violations de la sécurité ; décidez de la responsabilité de votre organisation en la matière. L'apprentissage se fait par l'action et non par des mots : offrez une formation professionnelle adaptée correspondant au niveau des données traitées.

6. **Adoptez les meilleures pratiques pour les données très sensibles et privées** afin de mieux protéger l'identité et les informations confidentielles des personnes dont les données seront stockées dans le cloud. Reportez-vous aux directives nationales pour le recueil et le stockage de données privées, notamment si ces politiques autorisent le stockage de ces données dans le cloud. Les réglementations nationales et internationales offrent aussi des directives sur les bonnes pratiques [http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm], [http://www.eugdpr.org/] et [https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection].

Résultats

Ces résultats sont révélateurs et ont été recueillis auprès des organismes de développement numérique qui ont suivi les étapes décrites dans ce guide.

- Des principes de sécurité modernes et solides sont déployés en utilisant l'infrastructure de sécurité du prestataire de services en nuage.
- Les ressources destinées aux activités du serveur de l'entreprise et à la maintenance sont réorientées sur la mise à jour et le maintien de sauvegardes de sécurité solides via des services basés sur le cloud.

> "Il y a souvent confusion entre consentement, compréhension, et choix. Ces trois concepts ne sont pas la même chose. Les gens peuvent être submergés par l'information. Même lorsque les gens comprennent, parfois le consentement n'est pas un choix à moins qu'il y ait des alternatives valables."
>
> — KATHY JOE
> ESOMAR

Comment sécuriser des données privées stockées et accessibles dans le nuage (cloud)

- Les bonnes pratiques de recueil et de protections des données privées sont appliquées, notamment le fait de s'enquérir si les réglementations nationales et régionales permettent que les données sensibles (par ex., données du patient) soient stockées et accessibles via le cloud.

Erreurs courantes

- **Politiques relatives la résidence des données.** Les politiques et les réglementations de certains pays peuvent décourager ou interdire le stockage de données dans des services en nuage offshore. Les Directives de l'OCDE de 2013 sur la confidentialité offrent des orientations sur des problématiques telles que la propriété des données lorsque ces dernières sont transférées hors des frontières [http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm]. Les réglementations nationales et internationales peuvent aussi limiter le stockage de données de patients ou de données privées par le biais de services en nuage.
- **Insuffisances des infrastructures.** Un bande passante Internet insuffisante ou instable peut ralentir les services du cloud ou les rendre peu fiables pour les utilisateurs finaux. Avant de mettre en œuvre des services en nuage, les organisations doivent évaluer la connectivité du réseau dans le contexte où les utilisateurs auront besoin d'accéder au service.
- **Financement et ressources.** Les services en nuage exigent un accès à des fonds continus et stables pour éviter la déconnexion des services et la perte des données. Le développement, la mise en œuvre, la maintenance et l'évaluation de la confidentialité et des mesures de sécurité, tout cela a un coût. Les organisations doivent examiner si elles ont accès à des financements stables et réservés au financement des services en nuage et des mesures de sécurité.
- **Évolution rapide de la technologie et de l'environnement.** Les utilisateurs doivent détenir un savoir-faire technique de haut niveau et une forte sensibilité pour s'adapter aux changements de l'environnement de l'informatique en nuage. Former les utilisateurs, attirer et retenir des effectifs techniquement

"UÀ moins que nous réagissions rapidement, il va y avoir un scandale. Quelqu'un aura sa base de données exposée avec beaucoup d'informations sensibles. [Les organisations de développement] et les consultants ont des tonnes de données sensibles, [et ces données sont stockés sur] des ordinateurs portables. C'est une information privée très intime. Nous sommes catégoriques sur le fait que nos informations personnelles soient protégées, mais tout le monde a droit à ces protections. La question est donc de savoir comment doter les organisations des politiques, des pratiques et des normes qui permettent ces protections, en particulier lorsque l'on passe des outils analogiques au outils numériques."

MALIHA KHAN
Consultant indépendant

sophistiqués ont des implications sur le financement.

- **Sécurité dorsale et risques de confidentialité.** Les prestataires de stockage sur le cloud disposent d'un certain niveau d'accès aux données (bien que fortement restreint), ce qui peut susciter un manque de confiance dans la sécurité et la confidentialité des données chez les utilisateurs. Les atteintes à la sécurité sont également possibles à la suite de cyberattaques du prestataire de service dans le cloud ou de violation de sécurité en interne.

RESSOURCES

FIELD IMPLEMENTATION GUIDANCE:

Conducting Mobile Surveys Responsibly: A Field Book for WFP Staff, World Food Programme (WFP). http://documents.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp292067.pdf

Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect. http://www.girleffect.org/media/3052/gem-girl-safeguarding-policys_19-05-16.pdf

Responsible Data Management, Oxfam. http://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management

GUIDES TECHNIQUES:

Audit Trail and Node Authentication, Integrating the Healthcare Enterprise (IHE). http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

Cloud Computing Toolkit, HIMSS. http://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit

Doing It Right: Cloud Encryption Key Management Best Practices, TechTarget Network. http://searchcloudsecurity.techtarget.com/tip/Doing-it-right-Cloud-encryption-key-management-best-practices

Enabling Privacy: Data Segmentation, HealthIT.gov. https://www.healthit.gov/providers-professionals/ds4p-initiative.

IT Infrastructure Handbook: De-identification, IHE. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf.

IT Infrastructure Technical Framework Supplement: Data Segmentation for Privacy, IHE. http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DS4P_Rev1.0_PC_2014-03-14.pdf.

INTRODUCTIONS ET HISTORIQUE:

Cloud Computing in Health White Paper, Canada Health Infoway. https://www.infoway-inforoute.ca/en/component/edocman/545-cloud-computing-in-health-white-paper-full/view-document?Itemid=0.

Comment sécuriser des données privées stockées et accessibles dans le nuage (cloud)

Cross-Enterprise User Assertion (XUA), IHE. http://wiki.ihe.net/index.php/Cross-Enterprise_User_Assertion_(XUA).

Data Protection, Privacy, and Security for Humanitarian & Development Programs, World Vision International. http://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs

Improving Data Privacy & Security in ICT4D: A Workshop on Principle 8 of the Digital Development Principles, United Nations Global Pulse. http://www.unglobalpulse.org/sites/default/files/Data%20Privacy%20and%20Security%20in%20ICT4D%20-%20conference%20report%20layout%20-%20FINAL.pdf

A Primer on the Privacy, Security, and Confidentiality of Electronic Health Records, MEASURE Evaluation. https://www.measureevaluation.org/resources/publications/sr-15-128-en

Quality, Research and Public Health (QRPH) White Paper: Using IHE Profiles for Healthcare — Secondary Data Access, IHE. https://www.ihe.net/uploadedFiles/Documents/QRPH/IHE_QRPH_WP_Healthcare_Secondary_Data_Access.pdf

Responsible Data Policies – Terms, Policies and Frameworks. MERLTech. https://drive.google.com/file/d/0B6RRlwWznhZqalBVS3FlTEVZVmc/view

RÈGLEMENTATION ET POLITIQUE:

African Union Convention on Cyber Security and Personal Data Protection. https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

European Union General Data Protection Regulation (EU GDPR). http://www.eugdpr.org/

Guidance on HIPAA & Cloud Computing, U.S. Department of Health and Human Services (HHS). https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

"Il y a toujours un point de vue que la technologie va tout resoudre. Mais on comprend de plus en plus que la technologie s'accompagne de véritables défis et de dilemmes éthiques." Ella Duncan, Search for Common Ground."

ELLA DUNCAN

Search for Common Ground