# MODE SaaS : COMMENT SECURISER L'ACCES A L'INFO ?

*Par Hervé STREIFF - Responsable conformité et sécurité de l'information - LOCARCHIVES*

**Comment combiner l'utilisation d'un portail web de gestion des archives en mode SaaS avec le niveau de sécurité exigé par une politique de centralisation des identités et des accès aux documents ?**

Dans un monde informatique de plus en plus ouvert sur l'extérieur, les entreprises souhaitant développer la mobilité de leurs collaborateurs recourent souvent à des solutions en ligne pour la consultation, le stockage et le partage de documents. En effet, d'après le rapport « State of It » de Spiceworks (mai 2014), dans la région EMOA, 56% des entreprises ont déjà adopté le Cloud[1].

**Les solutions « en mode SaaS » : définition et avantages**

Techniquement parlant, il s'agit de solutions en mode SaaS (Software as a Service), c'est-à-dire que le logiciel n'est pas installé sur le poste de travail des collaborateurs, mais est mutualisé pour un ensemble d'entreprises sur une plate-forme technique exploitée par un sous-traitant.

Pour l'entreprise, le choix d'une solution SaaS présente plusieurs avantages (coût, simplicité de gestion et évolutivité), mais aussi un inconvénient important : **une application SaaS accessible en ligne sort des murs de protection que la DSI de l'entreprise a érigés contre les intrusions extérieures.**

**L'existence d'un risque sur la sécurité des données**

Dans le cas d'un logiciel de gestion et de consultation des archives, cette faille potentielle dans la sécurité des données peut mettre en danger la confidentialité des documents sensibles de l'entreprise : contrats commerciaux, brevets de R&D, dossiers RH ou médicaux… La faille peut même être aggravée par le télétravail et le « Bring Your Own Device » qui encouragent l'utilisation de smartphones, de tablettes et d'ordinateurs personnels à des fins professionnelles. Ces terminaux ne sont en effet pas aussi bien sécurisés que les postes de travail de l'entreprise. Or, d'après l'étude Verizon Data Breach Investigation (juillet 2011), le vol des droits d'accès apparaît comme le moyen le plus utilisé pour accéder illégalement aux réseaux des entreprises[2].

Dès lors, **comment renforcer la sécurité des documents sensibles stockés en ligne ?**

**Solution n°1 : Optimiser vos moyens d'authentification et d'administration traditionnels**

90 % des mots de passe pourraient être piratés en quelques secondes ou en quelques heures à l'heure actuelle, d'après une étude mondiale réalisée par Deloitte[3]. **La sécurité offerte par le filtre du login et du mot de passe peut être améliorée par l'opérateur du système d'archivage grâce à une gestion renforcée des authentifications utilisateurs.** Ainsi, l'opérateur doit proposer un système d'archivage qui n'est pas en mesure de connaître le mot de passe des utilisateurs, ni de les stocker dans une base données accessible. Son système d'archivage doit en conserver seulement un « hash », une empreinte partielle et codée, dans une zone sécurisée non connectée à Internet.

L'archiveur doit également proposer à son client des règles de sécurité draconiennes. **Une bonne politique de révocation des mots de passe prévoit ainsi que ceux-ci devront être périodiquement renouvelés, ne pourront être remplacés à l'identique, et seront supprimés en cas de départ d'un collaborateur.** Le gestionnaire consciencieux contraint aussi l'utilisateur à choisir un mot de passe suffisamment robuste par sa longueur et sa complexité.


© 2015 LOCARCHIVES

**Mots de passe : 3 conseils à communiquer aux utilisateurs**
1- Utiliser des mots de passe professionnels et personnels différents
2- Utiliser un mot de passe complexe tout en étant mémorisable : minimum 8 caractères, association de caractères alphabétiques et numériques, minuscules et majuscules, intégration de caractères spéciaux
3- Ne jamais communiquer son mot de passe car l'utilisateur engage ainsi sa responsabilité professionnelle

**Solution n°2 : Rajouter un dispositif d'authentification forte**

Le gestionnaire de la plateforme d'archivage peut renforcer la sécurité grâce à l'association du login et du mot de passe avec **un « token », une clé électronique qu'il faut avoir pour finaliser l'identification**. Cette pratique est en nette progression. En effet, d'après la 2014 Global Annual Authentication Survey de SafeNet, 56% des entreprises envisagent une adoption de l'authentification forte pour la majorité de leurs utilisateurs d'ici 2016[4].

Autrefois intégré à un objet physique comme un badge électronique, le « token » peut aujourd'hui prendre la forme d'une clé logicielle**. Dans sa version la plus innovante, cette clé logicielle est dynamique : elle génère un mot de passe à usage unique appelé One Time Password (OTP)**. Par ailleurs, il est désormais possible de convertir le terminal d'un utilisateur en « token » ; poste de travail, smartphone et tablette, transformés en « token », fournissent alors un code valable une minute afin de permettre la connexion.

Cette solution logicielle garantit aujourd'hui le même niveau de sécurité qu'un « token » physique. Elle permet une expérience utilisateur plus simple et une gestion quotidienne plus économique que des badges électroniques.

**Solution n°3 : Relier l'application SaaS au système de gestion des identités interne**

Cette solution associe la sécurité de la plateforme d'archivage avec celle de l'entreprise, en permettant à la plateforme d'interroger le système de gestion des identités de l'entreprise lorsqu'un utilisateur se connecte.

Cette solution a un avantage majeur : elle permet à l'entreprise d'**avoir la main sur la gestion des identités et des utilisateurs lors de la demande d'accès à la plateforme d'archivage.** De plus, cette association garantit la cohérence entre les utilisateurs de la plateforme et ceux du SI de l'entreprise.

Les profils-utilisateurs peuvent être directement créés ou supprimés par la DSI à l'arrivée ou au départ de collaborateurs, sans que cela nécessite de passer par l'archiveur. Ainsi, un collaborateur qui vient de quitter l'entreprise se verra automatiquement privé d'accès à la plateforme d'archivage.

Cependant, ce niveau de sécurité a un prix. L'entreprise doit avoir atteint un nombre critique d'utilisateurs pour être amorti car un tel projet doit être réalisé sur mesure du fait de la multitude de protocoles à interfacer.

**Au-delà des solutions techniques, penser au facteur humain**

Mot de passe difficilement violable, clé physique ou logicielle, couplage entre le SI et le Saas… Différentes solutions technologiques de sécurisation des documents sensibles stockés en ligne existent aujourd'hui.

Cependant, **pour être totalement efficaces, ces sécurités doivent être acceptées par les collaborateurs de l'entreprise**. Dans le cas contraire, ces derniers peuvent être tentés de mettre en place des stratégies de contournement, comme le fameux post-it antisèche collé sur le clavier du poste de travail.

**Mal informé, l'utilisateur sera toujours le maillon faible d'un système de sécurité informatique**. C'est pourquoi il est nécessaire de faire preuve de pédagogie auprès des collaborateurs - qui n'ont souvent pas la culture de la sécurité informatique - en rappelant l'existence des règles de sécurité et l'importance de leur respect et ce, quelle que soit la solution choisie. La confidentialité des documents sensibles de l'entreprise est à ce prix.

1. http://www.silicon.fr/state-of-it-cloud-byod-recrutements-95867.html
2. https://www.loginpeople.com/wp-content/uploads/2012/10/loginpeople_theddna_FR.pdf
3. http://www2.deloitte.com/content/dam/Deloitte/ca/Documents/technology-media-telecommunications/ca-fr-tmt-des-perspectives-a-lavant-garde.pdf
4. http://www.synetis.com/2014/05/22/les-entreprises-adoptent-en-lauthentification-forte/


© 2015 LOCARCHIVES