SINGLE SIGN ON.

L'authentification unique sort de son isolement

- Le SSO n'est plus seulement cette technologie de confort au retour sur investissement assuré.
- Un projet d'authentification unique s'inscrit désormais dans un chantier plus large de gestion des identités et des accès, parfois couplé à une authentification forte.

Imaginer qu'un utilisateur puisse mémoriser 6 à 7 mots de passe différents, tout en assurant le renouvellement régulier, est une utopie. Ce constat a naturellement conduit à l'émergence, et au succès, des solutions de SSO (Single Sign On ou authentification unique) en entreprise dès le début des années 2000. Cette technologie assure la maîtrise et la fiabilisation des processus d'authentification primaire et secondaire. Dans un premier temps, une authentification primaire est faite de l'utilisateur, puis une authentification secondaire suit, de manière transparente, pour l'accès aux différentes ressources du système d'information (SI). Une politique de mots de passe forts au niveau de l'authentification primaire suffit alors au renforcement de la politique de contrôle d'accès.

Vers une diminution des coûts

Ce qui explique que le SSO soit souvent couplé à un projet d'authentification forte, type PKI. Selon Stéphane Vinsot, directeur de l'offre IAM (Identity & Access Management ou gestion des identités et des accès) de l'éditeur Evidian, les deux technologies se complètent, au sens où *« le SSO est un outil de continuité de service de la fonction d'authentification forte. Il est intéressant de déployer des cartes à puce, mais que se passe-t-il quand la carte a été oubliée ? Le SSO prend en compte ces problématiques organisationnelles, en offrant des modes d'authentification de secours »*. Citons les mécanismes de questions-réponses ou de mot de passe temporaire.

Défendre le SSO comme complémentaire d'autres briques de sécurité est une évolution récente. Cette technologie autorise une gestion centralisée de l'accès tout en diminuant les coûts par la réduction des temps d'ouverture de session, et la diminution du recours au help desk.

Ce dernier point a longtemps été le motif du succès de la technologie. Un projet de SSO plaisait aux entreprises pour deux raisons : le retour sur investissement était assuré et l'utilisateur y gagnait en simplicité d'accès. Cela a contribué à isoler le SSO, les projets étant principalement poussés pour satisfaire ces deux objectifs, légitimes, sans s'inscrire dans une vue globale de l'architecture de sécurité. Ainsi, Francis Crégoire, directeur de projet d'Arismore, prévient : *« Le SSO n'est pas la bonne solution pour rationaliser le système d'information. On apporte à l'utilisateur une fonction pratique, mais on ne rationalise pas les bases utilisateurs, car les solutions ne font que rejouer le couple identifiant-mot de passe. »*

Sur le plan organisationnel, le SSO est un projet d'intérêt

Certes, le SSO est toujours perçu comme un projet à part entière, mais il s'inscrit désormais dans un cadre assez précis. *« C'est une première étape de l'IAM pour nombre d'entreprises qui ne souhaite pas se lancer sur des projets dont elles ne voient pas la fin »*, assure Stéphane Belloni, Product Marketing et Business Development Manager d'Ilex, lequel propose une offre verticale sur le marché de la santé. Cependant, Sébastien Lapique, ingénieur d'affaires Infrastructure et sécurité chez Euriware note que *« moins de projets d'IAM débutent par le SSO »*, tout en précisant que la place du SSO n'est pas négligeable. *« Quelle action a été déclenchée dans le système d'information ? Qui a accédé à quoi et qui s'est authentifié ? Ce sont autant de questions auxquelles le SSO sait parfaitement répondre désormais »*, détaille Sébastien Lapique. La raison en est que les solutions ont su intégrer des fonctions d'audit et de reporting, à commencer par l'horodatage de toutes les actions d'authentification. Au chapitre de l'évolution des offres, il faut ajouter l'amélioration des scripts d'auto-apprentissage des procédures d'authentification auprès des diverses ressources, et une meilleure gestion de l'authentification pour des applications Java. En outre, sur un plan organisationnel, le SSO est un projet d'intérêt. Antoine Gérardin, manager Sécurité chez Dimension Data insiste sur ce point : *« Le SSO est forcément structurant car le mettre en œuvre implique de travailler avec plusieurs entités de l'entreprise et nécessite un référentiel commun. »* ■


DR

2 QUESTIONS À...

Bruno Vincent,
associé et cofondateur d'ITekia, cabinet de conseil en système d'information

Quelle importance revêtent les référentiels dans la mise en place d'un SSO ?

« Primordiale ! Avant de se lancer dans un projet de SSO, il est essentiel de veiller au contenu et à la qualité des données d'identité présentes dans les référentiels. Un système de SSO devra au minimum disposer d'une table de correspondance assurant le lien entre diverses identités par lesquelles des applications reconnaissent respectivement l'utilisateur. Si l'entreprise a déjà un annuaire mutualisé d'authentification (LDAP), il suffira de baser le SSO sur ce référentiel aux identifiants uniques. »

Active Directory tient-il une place particulière dans les référentiels de SSO ?

« Oui, parce que ce référentiel est bien souvent l'un des plus fiables en termes d'exactitude de données d'identité. Mais aussi depuis Windows 2000, Active Directory fournit, au travers du protocole Kerberos, un service de jetons de SSO. Néanmoins, bien que Kerberos supporte un nombre croissant de langages et de produits du marché, son intégration reste encore complexe. »