Tribune – Quand l'identité devient un service : la voie de l'IDaaS

Aujourd'hui on n'utilise pas un mais des réseaux. Les périmètres métiers se sont multipliés et l'accès à l'information est possible depuis une multitude de terminaux mobiles ou fixes, personnels ou professionnels, à partir desquels chacun se connecte aux applications d'entreprises selon ses besoins. Bienvenue dans la nouvelle informatique distribuée.

Au final, quel élément reste commun à tout cela ? Quelle donnée reste et restera toujours le « plus petit dénominateur commun » aux périmètres, usages, applications ou terminaux ? L'identité. Elle est le pivot unique, invariable, autour duquel vont – et doivent – s'articuler l'ensemble des ressources et droits propres à chaque collaborateur.

Ce constat n'est pas nouveau. C'est même sur son fondement que sont nées des solutions comme Microsoft Active Directory, il y a plus de 20 ans. Devenues standard de facto, ces solutions restent nécessaires mais pas suffisantes.

Etendre le SSO

En effet, les sources d'identité se sont multipliées, ces dernières années. Aujourd'hui, nous utilisons un couple login/password pour s'identifier sur son poste de travail. Pourtant, c'est souvent par ces identifiants Facebook que l'on se connecte sur un grand nombre de plates-formes qui n'ont pourtant aucun lien avec ce réseau social. Enfin, c'est un simple profil LinkedIn, personnel mais à vocation professionnelle qui nous suit d'entreprise en entreprise.

Dans ce contexte, l'authentification unique Single Sign On ou SSO, permet de diffuser à ces différents programmes une identité de manière sécurisée et authentique.

Longtemps, le SSO a été pensé comme une sorte d'appliance locale, un coffre-fort de stockage des identifiants. Or cette vision initiale ne permettait pas d'étendre le SSO à des organisations tierces, externes à l'entreprise – surtout lorsque cette dernière ne faisait pas reposer sa propre solution de SSO sur les standards du marché. Il était alors impossible de l'étendre aux partenaires externes de l'entreprise. Qui plus est, ce stockage centralisé, ce 'coffre-fort', ne rassurait pas les utilisateurs quant à sa propre inviolabilité.

De nouvelles approches

De nouvelles approches ont donc vu le jour. Dans le domaine du grand public, un standard comme OpenID a été développé. C'est un protocole aujourd'hui particulièrement répandu qui permet à des utilisateurs de naviguer d'un site à un autre en ne s'authentifiant qu'une seule fois.
Dans le monde professionnel, le SSO ne peut plus être vu comme une initiative purement propre à l'entreprise. Pour pouvoir l'étendre plus facilement à ses partenaires extérieurs, des politiques de 'Identity as a Service' (IDaaS) ont vu le jour. Elles ne se substituent pas aux pratiques locales : elles les complètent. Ce n'est pas non plus une pratique de rupture : elle se situe dans la droite ligne

des ‘Software as a Service’, ou SaaS, auquel 40% des entreprises ont déjà recours. Les DSI sollicitent d’ailleurs ce procédé : une fois l’identité sous contrôle, ils sont plus en confiance pour déployer des solutions métiers qui s’étendent à plusieurs organisations, internes comme externes.

Au final, l’ouverture d’une entreprise vers son environnement proche ou lointain, ce que l’on a souvent appelé « l’entreprise étendue », a considérablement été ralentie ces dernières années par la crainte de ne pas maîtriser les éléments qui en sortaient ou y entraient. Dès lors que l’identité de ces éléments est non seulement connue mais maîtrisée, il est possible de leur délimiter un cadre précis d’exercice. Aujourd’hui, un SSO hybride, alliant une politique d’implémentation locale et d’IDaaS, représentent probablement l’avenir de l’authentification unique – celle qui permettra aux entreprises de s’ouvrir sans crainte vers l’extérieur.

Andi Hindle, directeur du développement International de Ping Indentity

---

Voir aussi
Silicon.fr étend son site dédié à l’emploi IT
Silicon.fr en direct sur les smartphones et tablettes