

Les DSI ajoutent Â« gestion des identitÃ©s Â» Ã leur vocabulaire

SÃ©curitÃ©

PostÃ© par : JPilo

PubliÃ© le : 11/12/2014 11:00:00

Lorsque les DSI parlent de sÃ©curitÃ©, ils utilisent souvent des termes comme Â« pare-feu Â» et Â« antivirus Â». Luc Caprini, Directeur Europe du Sud de Ping Identity explique les raisons pour lesquelles lâ€™environnement technologique actuel requiert un autre langage.

Les entreprises modernes sont plus ouvertes que jamais, mais cela ne signifie pas quâ€™elles sont plus sÃ©curisÃ©es. De leur cÃ´tÃ©, les entreprises tirent parti du cloud en se focalisant sur leurs compÃ©tences internes et en externalisant ce quâ€™elles peuvent Ã des prestataires tiers. Du cÃ´tÃ© du client, les employÃ©s Ã©quipÃ©s de pÃ©riphÃ©riques demandent de plus en plus un accÃ©s flexible et fluide aux donnÃ©es en tout lieu.

Lorsquâ€™un DSI envisage la sÃ©curitÃ©, il pense probablement Â« pare-feu Â» et Â« antivirus Â». Bien que ces technologies de sÃ©curitÃ© restent pertinentes, lâ€™environnement technologique Ã©voluant vers le cloud et le mobile oblige Ã prÃ©senter les DSI Ã considÃ©rer un nouvel ensemble de solutions. Les professionnels de la sÃ©curitÃ© doivent veiller Ã ce que le langage de chaque DSI intÃ©gre le concept dâ€™identitÃ©.

Lâ€™identitÃ© est le nouveau pÃ©rimÃ¨tre

Lâ€™approche classique de la sÃ©curitÃ© dâ€™entreprise sâ€™est axÃ©e sur la protection des utilisateurs au moyen de pare-feu comme pÃ©rimÃ¨tre de sÃ©curitÃ©. Aujourdâ€™hui, la vague du mobile, du cloud et du SaaS submerge les entreprises, ainsi que les demandes dâ€™accÃ©s de partenaires et de clients, cette approche cesse alors dâ€™Ãªtre viable.

Les entreprises doivent Ã prÃ©senter valider les utilisateurs sur la base de lâ€™identitÃ© et de certaines caractÃ©ristiques comme le rÃ´le, les droits dâ€™accÃ©s, le lieu et le pÃ©riphÃ©rique, indÃ©pendamment de lâ€™origine de la demande et oÃ¹ rÃ©sident les donnÃ©es. Ainsi, les pÃ©rimÃ¨tres de sÃ©curitÃ© classiques cÃ©dent le pas Ã un environnement virtualisÃ© dans lequel les identitÃ©s fÃ©dÃ©rÃ©es faÃ§onnent un nouveau cadre.

Le Cloud facilite la gestion des identitÃ©s

Les DSI disposent dâ€™ormais dâ€™outils modernes de gestion des identitÃ©s pour permettre une authentification sur tous les terminaux mobiles, depuis nâ€™importe oÃ¹. Ils peuvent ainsi configurer les processus dâ€™authentification en tout lieu, puis les associer Ã des utilisateurs dans un rÃ©fÃ©rentiel hÃ©bergÃ© nâ€™importe oÃ¹, et enfin les attribuer Ã une application on-premise ou cloud.

Ils peuvent intÃ©grer les systÃªmes internes actuels de gestion des identitÃ©s et les annuaires dâ€™utilisateurs finaux Ã des services IAM dans le cloud. Cela permet aux entreprises dâ€™externaliser ces services IAM pour les groupes dâ€™utilisateurs et les applications non stratÃ©giques tout en gÃ©rant les identitÃ©s et droits critiques en interne. Des fonctions comme lâ€™authentification multifacteur existent maintenant en tant quâ€™extensions dans le cloud, permettant ainsi une intÃ©gration facile et Ã©conomique.

Lâ€™expÃ©rience utilisateur de lâ€™authentification doit Ãªtre cohÃ©rente entre tous les canaux

De nombreuses entreprises investissent lourdement dans un systÃªme de sÃ©curitÃ© qui fonctionne pour les applications Web, mais pas nÃ©cessairement pour celles mobiles. Les nouvelles normes dâ€™identitÃ© comme OpenID Connect et OAuth 2.0 offrent une expÃ©rience cohÃ©rente

pour l'authentification des utilisateurs entre les applications Web et mobiles.

OpenID Connect permet de centraliser l'authentification des utilisateurs pour superviser leurs activités en toutes circonstances. Vous pouvez ainsi appliquer complètement les outils de sécurité déjà mis en place. Les utilisateurs bénéficient d'une expérience similaire en tout lieu. En outre, les mêmes normes peuvent servir à sécuriser un accès à des applications via des API orientées identité.

Une expertise approfondie n'est plus nécessaire

A l'origine, l'utilisation de l'authentification unique Single Sign-On (SSO) requerrait une certaine expertise car il était nécessaire de comprendre le langage SAML (Security Assertion Markup Language) ou faire appel à un spécialiste. Aujourd'hui, il existe l'option « assistant » qui permet maintenant à quiconque de se connecter rapidement en toute conformité.

Conformité et facilité d'utilisation vont de pair

Mettre en place un haut niveau de sécurité au sein de l'entreprise est devenue une condition sine qua non pour répondre aux exigences de conformité externes et réglementaires. S'assurer que les collaborateurs s'authentifient aux applications en toute sécurité permet à l'entreprise de protéger ses ressources au sein de l'entreprise.

Les bénéfices sont multiples : les employés risquent moins de mettre en péril l'entreprise en utilisant leurs identifiants professionnels dans le Cloud, l'entreprise renforce la sécurité des informations en contrôlant tout accès d'un employé à une application cloud. Enfin, les utilisateurs gagnent du temps en gestion des mots de passe et disposent d'un accès optimal aux applications.

La gestion des identités et des accès évolue sous l'effet des tendances du Cloud et du mobile. En comprenant ces nouvelles réalités, les DSI vont améliorer leur prise de décisions au bénéfice de leurs entreprises aujourd'hui et demain.