Lâ□□identitÃ© est dÃ©sormais la clÃ© de voÃ»te de la sÃ©curitÃ© informatique
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 8/1/2014 13:00:00

Nul ne serait surpris dâ□□apprendre que les frontiÃ¨res traditionnelles de la sÃ©curitÃ© informatique nâ□□existent plus. La migration des applications vers le cloud, la mobilitÃ© universelle et lâ□□essor de lâ□□accÃ¨s tiers Ã des ressources sensibles sont des tendances sources de dÃ©fis pour les DSI du monde entier.

Les applications cloud et les appareils mobiles ont effacÃ© les contours de la sÃ©curitÃ© sur lesquels lâ□□entreprise se fondait depuis longtemps. Ces tendances Ã©mergent alors que les DSI sont censÃ©es gagner en efficacitÃ© et gÃ©nÃ©rer de la valeur ajoutÃ©e avec des rÃ©ductions dâ□□effectifs et une explosion du nombre dâ□□utilisateurs et dâ□□applications.

Que faut-il pour faire face Ã cette Ã©volution de la sÃ©curitÃ© ?

Il faut un ensemble de protocoles modernes pour la gestion des identitÃ©s adaptÃ©s Ã de nouveaux modÃ¨les de dÃ©veloppement Web. Cet ensemble moderne de protocoles repose sur des normes et des infrastructures orientÃ©es dÃ©veloppeur comme REST et JSON (JavaScript Object Notation).

Ces normes comprennent SCIM (System for Cross-Domain Identity Management), OAuth, OpenID Connect et lâ□□incontournable SAML (Security Assertion Markup Language). Ce jeu de protocoles sâ□□avÃ¨re nÃ©cessaire Ã une gestion Ã©volutive des utilisateurs et donc crucial pour tout mandat de conformitÃ©.

Approfondissons un peu le rÃ´le de chaque norme :

SCIM (System for Cross-Domain Identity Management)

Lâ□□accÃ¨s des utilisateurs aux applications est impossible sans crÃ©er une identitÃ© utilisateur.

Lâ□□entreprise se dÃ©bat avec des systÃ¨mes dâ□□attribution exclusifs friables car ils ne gÃ¨rent pas lâ□□Ã©volution des applications ou systÃ¨mes dâ□□exploitation.

Les premiers projets axÃ©s sur SPML (Service Provisioning Markup Language) ayant Ã©chouÃ© Ã cause de la complexitÃ©, SCIM offre un jeu de commandes simple pour crÃ©er, lire, actualiser et supprimer.

SCIM est une norme orientÃ©e dÃ©veloppeur qui exploite REST et JSON, remplaÃ§ant des mÃ©canismes dâ□□attribution propriÃ©taires ou manuels coÃ»teux.

Â

Les fournisseurs de services utilisent dÃ©jÃ SCIM 1.0, ainsi que des produits IAM. Lâ□□organisme de normalisation IETF a presque achevÃ© la dÃ©finition de la version 2.0 du protocole SCIM.

SAML (Security Assertion Markup Language)

CrÃ©Ã©e il y plus de 10 ans, SAML est la norme dâ□□identitÃ© la plus utilisÃ©e en entreprise. Il sâ□□agit de la mÃ©thode de fait pour lâ□□authentification Web et SSO des applications SaaS. Les entreprises lâ□□utilisent Ã©galement pour la connexion Ã diverses applications, comme celles intÃ©grÃ©es suite Ã une fusion ou acquisition.

La norme SAML sâ□□avÃ¨re pÃ©renne et offre une solution privilÃ©giÃ©e pour lâ□□authentification SSO Web, car un trÃ¨s grand nombre dâ□□applications et de systÃ¨mes dâ□□identification la gÃ¨rent.

En outre, elle permet lâ□□authentification SSO sans dÃ©pendre de noms dâ□□utilisateur et mots de passe, que lâ□□on peut facilement dÃ©rober et utiliser pour des transactions illicites et des atteintes Ã la sÃ©curitÃ© des donnÃ©es.

Enfin, elle permet lâ□□accÃ¨s Ã grande Ã©chelle en Ã©liminant les rÃ©initialisations de mot de passe dans lâ□□application cible. SAML demeure la norme rÃ©fÃ©rence pour lâ□□authentification utilisateur Web et SSO.

OAuth 2.0

Quid des applications mobiles natives, souvent dÃ©nuÃ©es de fonctionnalitÃ© Web ? Câ□□est lÃ quâ□□OAuth 2.0 entre en scÃ¨ne.
OAuth 2.0 est une norme permettant Ã des applications mobiles natives dâ□□accÃ©der Ã des ressources au nom de lâ□□utilisateur. Il sâ□□agit dâ□□un protocole orientÃ© API qui exploite REST et JSON.

Il est intÃ©grÃ© Ã de nombreuses applications SaaS comme Facebook, Google, Yahoo, Ã des infrastructures de cloud comme Windows Azure Active Directory et Ã des logiciels IAM modernes, notamment ceux quâ□□offre ma sociÃ©tÃ© Ping Identity.

Pour lâ□□entreprise, OAuth est un gage dâ□□accÃ¨s authentifiÃ© aux applications mobiles natives et gagne en adoption chez les dÃ©veloppeurs et Ã©diteurs dâ□□applications SaaS. La norme de base OAuth 2.0 est finalisÃ©e et approuvÃ©e par lâ□□IETF (Internet Engineering Task Force).

Alors quâ□□OAuth est la norme de fait de lâ□□authentification pour les applications hors Web, il manque un cadre pour lâ□□enregistrement flexible de ces applications, impÃ©ratif si elles ont accÃ¨s Ã des ressources dâ□□entreprise. En outre, OAuth exige une infrastructure Ã©largie de

gestion des identitÃ©s pour assurer une authentification unique des utilisateurs dans de nombreuses applications.

OpenID Connect

OpenID Connect vise Ã aider Ã relever les dÃ©fis que prÃ©sente OAuth. Reposant sur lâ□□architecture OAuth, ce protocole permet une identification Ã grande Ã©chelle en offrant un processus dâ□□enregistrement automatisÃ© pour les applications et un processus de recherche pour les systÃ¨mes dâ□□authentification.

Compte tenu de ses racines, OpenID Connect simplifie le flux dâ□□authentification OAuth comme aucun autre protocole.
La dÃ©finition de la norme est pratiquement terminÃ©e et fait Ã prÃ©sent lâ□□objet dâ□□un examen final par lâ□□OpenID Foundation, lâ□□approbation dÃ©finitive Ã©tant attendue vers le dÃ©but 2014.

Lâ□□adoption est dÃ©jÃ en cours. Le 23 octobre, Google a informÃ© ses partenaires du retrait progressif dâ□□OpenID 2.0 et OAuth 1.0 au profit dâ□□OpenID Connect. Ce changement va obliger les sites Web qui acceptent des ID Google pour la connexion Ã Ã©voluer vers la spÃ©cification. Salesforce et Microsoft figurent parmi les autres acteurs Ã gÃ©rer OpenID Connect et les Ã©diteurs de logiciels IAM appuient Ã©galement ce changement.

Lâ□□adoption du protocole le dirige vers le pÃ©rimÃ¨tre dâ□□infrastructure des opÃ©rateurs mobiles, les projets dâ□□identification soutenus par les pouvoirs publics en Europe et aux Ã□tats-Unis, ainsi que les dÃ©ploiements de clouds hybrides en entreprise.

Conclusion Patrick Harding, CTO de Ping Identity

Lâ□□adoption de ce jeu de protocoles dÃ©passe largement le cadre des environnements de laboratoire et de bÃªta test. Les fondations sont posÃ©es et le dÃ©ploiement Ã grande Ã©chelle sâ□□avÃ¨re omniprÃ©sent.
Les fournisseurs de services et les architectes en sÃ©curitÃ© dâ□□entreprise peuvent observer le rÃ´le vital de lâ□□identitÃ© dans un monde connectÃ© englobant chaque employÃ©, appareil et application.

Le seul moyen dâ□□adapter lâ□□accÃ¨s et la sÃ©curitÃ© Ã travers ce monde connectÃ© rÃ©side dans la normalisation. Le cloud, la mobilitÃ© et les rÃ©seaux sociaux transformant lâ□□entreprise moderne, lâ□□identitÃ© forme une base cruciale pour relever les dÃ©fis.