Authentification sÃ©curisÃ©e avec n'importe quel appareil mobile
Internet
PostÃ© par : JulieM
PubliÃ©e le : 12/3/2013 13:00:00

Le monde de lâ□□informatique semble apprÃ©cier les acronymes Ã quatre lettres :Â WLAN, SNMP, HTML â□□ et le tout dernier BYOD (Bring Your Own Device) (Amenez votreÂ propre appareil). **AccÃ©der aux rÃ©seaux et aux donnÃ©es dâ□□entreprise Ã lâ□□aide Ã lâ□□aide de terminaux dâ□□utilisateurs privÃ©s** reste toutefois un problÃ¨me qui laisse perplexes de nombreux responsables IT et directeurs dâ□□entreprise.

Â« *Comment pouvons-nous permettre un accÃ¨s sÃ©curisÃ© pour les appareils mobiles sans mettre nos donnÃ©es en danger ?* Â» Utiliser une double couche de sÃ©curitÃ© qui implique lâ□□identification des utilisateurs au moyen dâ□□une authentification Ã deux facteurs sans jeton semble Ãªtre une approche appropriÃ©e. En effet, cette approche combine les coordonnÃ©es de connexion personnelles, qui reprÃ©sentent le premier facteur, puis un numÃ©ro d'identification dynamique reÃ§u par Smartphone, tablette ou autre dispositif mobile, comme second facteur.

Se servir dâ□□ordinateurs personnels et dâ□□autres dispositifs pour des raisons professionnelles est de plus en plus courant. Comme le rÃ©vÃ¨le la derniÃ¨re enquÃªte de lâ□□association BITKOM : 27 % de toutes les entreprises qui ont participÃ© Ã lâ□□enquÃªte se concentrent actuellement sur la question du BYOD qui est Â« La technologie et la tendance du marchÃ© la plus importante selon les sociÃ©tÃ©s ICT Â». En outre, on constate un intÃ©rÃªt considÃ©rable pour les applications mobiles (48 %) et la question de la sÃ©curitÃ© informatique en gÃ©nÃ©ral (33 %). Lorsquâ□□il sâ□□agit du principe de BYOD, deux exigences importantes sâ□□opposent : les employeurs souhaitent disposer de la plus grande flexibilitÃ© possible, avec une procÃ©dure de connexion simple, alors que les employÃ©s veulent absolument garantir la meilleure sÃ©curitÃ© possible pour les rÃ©seaux et les donnÃ©es.

Double couche de sÃ©curitÃ©

Depuis que les mesures de sÃ©curitÃ© informatique ont Ã©tÃ© Ã©laborÃ©es, et en particulier en ce qui concerne les processus dâ□□identification, les experts de sÃ©curitÃ© ont commencÃ© Ã combiner des mÃ©canismes multiples. Câ□□est le cas pour lâ□□authentification Ã deux facteurs.

Afin de permettre une identification sans ambiguÃ¯tÃ©, au moins deux de trois facteurs de sÃ©curitÃ© possibles sont requis et ces trois facteurs sont :

â¢ Un Ã©lÃ©ment que seul lâutilisateur connaÃ®t (par ex. mot de passe ou numÃ©ro dâidentification personnel) ;

â¢ Un Ã©lÃ©ment concret que seul lâutilisateur possÃ¨de (par ex. un tÃ©lÃ©phone mobile) ;

â¢ Quelque chose qui est connectÃ© intrinsÃ¨quement Ã lâutilisateur (par ex. lâiris de lâÅil).

On peut citer Ã titre dâexemple quotidien le retrait dâargent depuis un distributeur de billets : le client a besoin de sa propre carte bancaire et dâun numÃ©ro dâidentification personnel pour effectuer une transaction rÃ©ussie. Le problÃ¨me dans ce cas est que la carte bancaire (ou le jeton, en termes de terminologie de rÃ©seau dâentreprise) doit toujours Ãªtre portÃ©e par lâutilisateur. Outre ce problÃ¨me, les coÃ»ts liÃ©s Ã lâutilisation de jetons ne doivent pas Ãªtre sous-estimÃ©s par les sociÃ©tÃ©s. Dans ce contexte, les responsables doivent prendre en compte les coÃ»ts liÃ©s Ã lâacquisition initiale des jetons, ainsi que lâÃ©mission de remplacements en cas de perte ou de vol.

Exploiter les ressources existantes

Les solutions modernes vont encore plus loin et fonctionnent sur le principe de Â« BYOT Â» : Bring your own token (Amenez vos jetons personnels). PlutÃ´t que dâutiliser des outils supplÃ©mentaires, de telles applications se servent des dispositifs existants, tels que les outils dâaccÃ¨s, qui sont dans ce cas spÃ©cifique des appareils mobiles. Lâavantage de cette approche est que les Smartphones sont devenus de toute faÃ§on un compagnon presque constant pour la plupart des personnes dans leur vie quotidienne. Et au travail, presque tous les employÃ©s disposent Ã©galement de leur propre tÃ©lÃ©phone portable, tablette ou ordinateur portable avec eux.

Afin de permettre une identification sÃ©curisÃ©e et non ambiguÃ«, les solutions BYOT combinent un Â« facteur de numÃ©ro dâidentification Â» et un Â« facteur de coordonnÃ©es de connexion personnelles Â». Pour ce dernier, lâutilisateur dispose dâun nom dâutilisateur et mot de passe personnellement dÃ©finis, ainsi que dâune licence dâaccÃ¨s personnelle. Et pour le premier facteur, lâutilisateur reÃ§oit sur son appareil mobile un numÃ©ro dâidentification numÃ©rique valide une fois et gÃ©nÃ©rÃ© dynamiquement par SMS, e-mail ou par le biais dâune application. Par consÃ©quent, les sociÃ©tÃ©s nâont pas besoin d'installer de logiciel ou matÃ©riel supplÃ©mentaire sur les appareils, lorsque le personnel utilise non seulement des appareils dâentreprise, ainsi que des appareils privÃ©s pour accÃ©der aux donnÃ©es internes. Ceci permet dâÃ©viter que les employÃ©s ne ressentent un sentiment d'imposition causÃ© par lâobligation dâinstaller un logiciel supplÃ©mentaire sur leurs appareils privÃ©s.

Date dâexpiration intÃ©grÃ©e

Lorsque lâutilisateur saisit son numÃ©ro dâidentification au moment de la connexion, cette sÃ©quence de numÃ©ros spÃ©cifique expire dÃ¨s quâelle a Ã©tÃ© saisie et le systÃ¨me gÃ©nÃ¨re automatiquement un nouveau code et lâenvoie Ã lâappareil mobile de lâutilisateur. Le mÃªme principe sâapplique dans le cas des entrÃ©es incorrectes au moment de la connexion. Il est possible de dÃ©finir combien de connexions incorrectes sont autorisÃ©es avant que lâaccÃ¨s ne soit complÃ¨tement refusÃ©. Alternativement, les utilisateurs peuvent recevoir un numÃ©ro dâidentification rÃ©utilisable pendant une pÃ©riode prÃ©dÃ©finie et qui expire automatiquement avec une nouvelle combinaison de chiffres envoyÃ©e pÃ©riodiquement un jour avant que son utilisation ne soit requise. Ce remplacement des codes assure quâun numÃ©ro d'identification valide est toujours disponible et que les problÃ¨mes de transmission

sensible dans les rÃ©seaux de tÃ©lÃ©phone mobiles nâ□□empÃªchent pas lâ□□exÃ©cution rÃ©ussie de la procÃ©dure de connexion.

Authentification Ã deux facteurs en pratique

Une approche dâ□□authentification Ã deux facteurs, telle que dÃ©crite ici a Ã©tÃ© mise en Å□uvre par exemple chez T-Mobile. Dâ□□ailleurs la sociÃ©tÃ© a Ã©tÃ© le premier opÃ©rateur de tÃ©lÃ©phonie mobile Ã dÃ©ployer une solution qui utilise les tÃ©lÃ©phones mobiles pour lâ□□authentification Ã distance. Celle-ci permet au personnel de sâ□□identifier, quel que soit lâ□□emplacement, Ã lâ□□aide dâ□□un tÃ©lÃ©phone portable, dâ□□un mot de passe et dâ□□un numÃ©ro dâ□□identification gÃ©nÃ©rÃ© dynamiquement qui est envoyÃ© Ã l'appareil mobile de chaque personne. Ã□tant donnÃ© que chaque employÃ© est la seule personne Ã connaÃ®tre ses deux facteurs, les tierces parties nâ□□ont aucun moyen dâ□□accÃ©der au rÃ©seau et de voler des donnÃ©es. 15 000 employÃ©s en tout travaillent dÃ©sormais avec cet outil et les responsables ont remarquÃ© que ceci a causÃ© des Ã©conomies de temps et de coÃ»ts importantes, Ã©tant donnÃ© que l'acquisition onÃ©reuse de jetons matÃ©riels supplÃ©mentaires n'est pas requise. En outre, il nâ□□est nÃ©cessaire de mener des sÃ©ances de formation qui prennent beaucoup de temps.

SynthÃ¨se

Les sociÃ©tÃ©s qui utilisent lâ□□authentification Ã deux facteurs bÃ©nÃ©ficient dâ□□une double couche de sÃ©curitÃ©, Ã©tant donnÃ© que la procÃ©dure de connexion combine un nom d'utilisateur et un mot de passe dÃ©finis par l'utilisateur et un numÃ©ro d'identification gÃ©nÃ©rÃ© dynamique, plus une licence d'utilisateur. Par consÃ©quent, mÃªme si le mot de passe est dÃ©couvert par quelquâ□□un dâ□□autre, lâ□□accÃ¨s par une tierce partie reste bloquÃ© car les autres facteurs restent inconnus. Ces solutions sont Ã©galement intÃ©ressantes en termes de coÃ»t, car la sociÃ©tÃ© investit uniquement dans lâ□□application centrale et lâ□□acquisition onÃ©reuse de jetons supplÃ©mentaires nâ□□est pas nÃ©cessaire. **Une calculatrice disponible** peut Ãªtre utilisÃ©e pour dÃ©terminer les Ã©conomies approximatives rÃ©sultant du passage Ã une mÃ©thode dâ□□authentification sans jeton. Enfin, la configuration, la distribution, la rÃ©Ã©mission de jetons (dans le cas dâ□□une perte ou dâ□□un vol) et lâ□□assistance informatique ne sont plus requises.