Insolite : SÃ©curitÃ© des rÃ©seaux sociaux, faites mieux que 123456!
Insolite
PostÃ© par : JPilo
PubliÃ©e le : 29/6/2012 13:00:00

Comme vous le savez, le rÃ©seau social LinkedIn a rÃ©cemment Ã©tÃ© victime de piratage. Une faille de sÃ©curitÃ© dans la version mobile du rÃ©seau serait enÂ cause dans le piratage de 6,5 millions de comptes. A ce jour, des centaines deÂ milliers de mots de passe ont Ã©tÃ© dÃ©cryptÃ©s.

Jan Valcke, PrÃ©sident et COO de VASCO Data Security, Ã©diteur leader spÃ©cialiste des solutions d'authentification forte, vous donne quelques conseils pour sÃ©curiser vos informations sur les rÃ©seaux sociaux.

Combien de comptes en ligne possÃ©dez-vous ? Vous ne le savez pas vraiment ? Comptez avec nous : au moins un compte e-mail ; un ou plusieurs comptes pour vous connecter Ã vos rÃ©seaux sociaux, des comptes pour faire du shopping, des jeux en ligne ou lire votre journal ; un autre compte pour votre club de sport local ou pour le forum de votre site prÃ©fÃ©rÃ©. Outre cela, vous avez aussi de multiples autres comptes dans votre environnement de travail : pour l'accÃ¨s Ã votre CRM, au webmail, aux diverses applications de l'entreprise, ou pour consulter les revues spÃ©cialisÃ©es auxquelles votre entreprise est abonnÃ©e. Dans ce contexte est-ce que le terme Â« protÃ©gÃ©(e) Â» est le terme le plus appropriÃ© pour dÃ©crire votre situation ?

Inventer des mots de passe est un Ã©ternel compromis

Si les mots de passe sont trop simples, il est facile pour les pirates de les dÃ©couvrir et de les intercepter. Toutefois, lorsque les mots de passe sont trop complexes, ils sont obliÃ©s ou couchÃ©s par Ã©crit sur un post-it (en gÃ©nÃ©ral pas trop loin de l'Ã©cran...). Un grand nombre de problÃ¨mes se posent aussi lorsque nous utilisons des mots de passe statiques. Tout d'abord, l'utilisateur moyen n'a guÃ¨re d'imagination quand il s'agit d'inventer un mot de passe. Les noms des enfants, des proches ou des animaux domestiques, les dates de naissance ou des combinaisons de touches simples sur le clavier, telles que 123456 sont cousues de fil blanc. De plus, les gens ont tendance Ã utiliser les mÃªmes mots de passe pour diffÃ©rents comptes. Une diffÃ©rence entre les applications privÃ©es et de travail est rarement faite. Pour les hackers, c'est un jeu d'enfant que d'intercepter ces mots de passe. Dans le but de contrer ce problÃ¨me, certaines entreprises contraignent leurs employÃ©s Ã changer de mot de passe aprÃ¨s une certaine pÃ©riode de temps (par exemple aprÃ¨s 30 jours). Cependant, ces mots de passe sont souvent obliÃ©s, impliquant une charge de travail supplÃ©mentaire pour les dÃ©partements informatiques dans le domaine de la gestion de mots de passe.

Un faux sentiment de libertÃ©

Nous pouvons nous plaire Ã penser que la cybercriminalitÃ© ne nous touchera jamais. Cependant, nous sommes en rÃ©alitÃ© plus vulnÃ©rables sur Internet que nous ne pouvons le croire. Jetons un coup d'Å□il, par exemple, sur les rÃ©seaux sociaux. Facebook, LinkedIn, Twitter : qui n'a pas au moins un compte sur ces rÃ©seaux de nos jours ? Un rÃ©seau social est un endroit idÃ©al pour rencontrer et garder contact avec nos amis, relations d'affaires ou avec des personnes qui habitent loin. Ces rÃ©seaux apparaissent comme des environnements agrÃ©ables et aimables oÃ¹ les informations peuvent Ãªtre partagÃ©es, que ce soit Ã des fins professionnelles ou dans un cadre privÃ©. Comme il n'y a pas de barriÃ¨re physique, les utilisateurs n'ont pas d'inhibition Ã y divulguer des dÃ©tails sur leur entreprise ou sur leur propre vie privÃ©e. Les utilisateurs ne sont pas conscients du fait qu'ils ouvrent les fenÃªtres en grand sur leur propre vie. Les pirates suivent l'argent et sont conscients des gains pouvant Ãªtre obtenus par l'exploitation d'informations publiÃ©es par les utilisateurs sur les rÃ©seaux sociaux. Les donnÃ©es-cibles sont aussi bien des informations personnelles que des informations de propriÃ©tÃ© intellectuelle ou des informations sur l'entreprise voire mÃªme des numÃ©ros de sÃ©curitÃ© sociale ou de cartes de crÃ©dit.

Internet, un monde cruel

Disposer d'un niveau de sÃ©curitÃ© adÃ©quat est nÃ©cessaire sur Internet car le rÃ©seau est parsemÃ© de dangers. Les attaques par dictionnaire, le hameÃ§onnage (phishing), les enregistreurs de frappe (keyware), les logiciels espions (spyware) et les attaques dites Â« de l'homme du milieu Â» (MITM, man-in-the-middle) sont les plus communes.

Tout d'abord, l'exÃ©cution par les pirates d'attaques par dictionnaire sont liÃ©es au fait que la plupart des internautes utilisent des mots de passe simples ou rÃ©utilisent leurs mots de passe pour diffÃ©rents comptes. L'idÃ©e est de passer outre les techniques de chiffrement en composant une liste limitÃ©e de mots de passe possibles. Ces listes sont adaptÃ©es au pays dans lequel l'attaque est exÃ©cutÃ©e ou aux intÃ©rÃªts de la victime.

Ensuite, le hameÃ§onnage est Ã©galement une technique courante pour obtenir illÃ©galement des mots de passe. Des escrocs envoient alors de faux e-mails Ã l'utilisateur pour le conduire Ã visiter un faux site web les incitant Ã fournir leur nom d'utilisateur et leur mot de passe.

Les criminels utilisent aussi des enregistreurs de frappe. Ces logiciels malveillants (malware) d'un genre un peu particulier enregistrent les touches frappÃ©es sur le clavier Ã l'insu de l'utilisateur afin de dÃ©tecter le mot de passe, qui est ensuite envoyÃ© au pirate sur le rÃ©seau. L'utilisateur est inconscient de tout prÃ©judice. Ce malware peut entrer dans l'ordinateur par le biais de n'importe quel fichier possible et souvent de faÃ§on dÃ©guisÃ©e.

Les logiciels espions (spyware) recueillent des informations sur l'utilisateur via sa connexion Internet. La caractÃ©ristique d'un logiciel espion est qu'il est souvent dÃ©livrÃ© de faÃ§on invisible avec un freeware qui peut Ãªtre tÃ©lÃ©chargÃ© Ã partir d'Internet. Une fois installÃ©, le logiciel espion surveille les activitÃ©s de l'utilisateur sur Internet et il envoie les informations Ã un tiers. Au cours des derniÃ¨res annÃ©es, on note une augmentation significative du nombre de logiciels espions capables de recueillir des informations sur les adresses Ã©lectroniques et mots de passe. Parfois, ces logiciels fonctionnent un peu comme des chevaux de Troie : les utilisateurs acceptent l'installation du virus sans le savoir sur leur ordinateur, en croyant avoir installÃ© un autre programme.

Enfin, les attaques dites Â« de l'homme du milieu Â» (MITM, man-in-the-middle) sont un moyen d'Ã©coute Ã©lectronique. Le pirate s'insÃ¨re dans une communication et est capable de lire les messages entre les deux parties, d'ajouter des choses ou de modifier le message. L'expÃ©diteur ne se rend pas compte que le lien entre lui et le rÃ©cepteur est compromis. Dans le cas d'une attaque de type MITM, l'authentification traditionnelle avec une combinaison de nom d'utilisateur et mot de passe statique n'est pas suffisante pour vÃ©rifier l'authenticitÃ© de la transaction. La communication complÃ¨te peut Ãªtre menÃ©e Ã travers un faux site Web, gÃ©rÃ© par le pirate (l'homme du milieu).

La solution ? Recourir Ã l'authentification forte

L'authentification forte apporte une rÃ©ponse aux problÃ¨mes prÃ©cÃ©dents. Chaque mot de passe statique est remplacÃ© par un mot de passe dynamique. L'authentification Ã deux facteurs implique que l'utilisateur dispose de deux Ã©lÃ©ments. D'une part, il doit savoir quelque chose - par exemple un code PIN - et d'autre part, il doit possÃ©der quelque chose, comme un dispositif matÃ©riel ou une application pour gÃ©nÃ©rer un mot de passe Ã usage unique (one-time password ou OTP). L'ouverture de session n'est possible que par la saisie de ce mot de passe Ã usage unique. Et ce mot de passe n'a qu'une validitÃ© limitÃ©e dans le temps, de quelques dizaines de secondes en gÃ©nÃ©ral. Tenter l'interception de ce type de mots de passe se rÃ©vÃ¨le donc Ãªtre un effort futile de la part des pirates.

Comment cela fonctionne ?

D'un point de vue technique, un mot de passe Ã usage unique (OTP) est le rÃ©sultat d'une opÃ©ration cryptographique combinant une clÃ© secrÃ¨te et un paramÃ¨tre variable. La clÃ© secrÃ¨te permet de s'assurer que les diffÃ©rents dispositifs gÃ©nÃ¨rent des mots de passe diffÃ©rents, puisque la clÃ© est diffÃ©rente pour chaque appareil. Le paramÃ¨tre variable, utilisÃ© comme second facteur, permet de s'assurer que chaque appareil gÃ©nÃ¨re un mot de passe OTP diffÃ©rent Ã diffÃ©rents moments, de sorte qu'un OTP diffÃ©rent puisse Ãªtre utilisÃ© Ã chaque connexion avec un mÃªme pÃ©riphÃ©rique. Trois types de paramÃ¨tres variables peuvent Ãªtre distinguÃ©s : le temps, le compteur et la demande d'identitÃ© (challenge).

Si le paramÃ¨tre appliquÃ© est le temps, l'heure et la date sont utilisÃ©es comme paramÃ¨tre variable. AprÃ¨s tout, ceux-ci sont uniques pour chaque gÃ©nÃ©ration OTP. Lorsque ce facteur temps est utilisÃ©, une durÃ©e de validitÃ© peut facilement Ãªtre dÃ©terminÃ©e cÃ´tÃ© serveur. Le dispositif d'authentification ou l'application d'authentification gÃ©nÃ¨re alors un mot de passe valide uniquement pendant une pÃ©riode de temps limitÃ©e (par exemple pendant 30 secondes).

Si le compteur est le paramÃ¨tre variable, le compteur est augmentÃ© d'une unitÃ© chaque fois que l'utilisateur appuie sur le bouton. Dans tous les cas, le dispositif d'authentification ou application et le serveur d'authentification sont synchronisÃ©s Ã chaque authentification rÃ©ussie.

Dans le cas du mode d'authentification dÃ©fi/rÃ©ponse (challenge-response authentication), utilisÃ© uniquement dans un contexte bancaire, l'utilisateur entre un numÃ©ro et reÃ§oit une rÃ©ponse sur ce point. Dans le mÃªme temps, le dÃ©fi est envoyÃ© au serveur pour empÃªcher qu'il soit utilisÃ© une seconde fois. L'opÃ©ration cryptographique est une opÃ©ration de chiffrement par bloc s'appuyant sur les protocoles 3DES ou AES.

Difficile ? Cher ? Pas du tout !

La question qui se pose est de savoir pourquoi l'authentification forte n'est pas encore gÃ©nÃ©ralement dÃ©ployÃ©e. La rÃ©ponse est que le dÃ©ploiement de l'authentification Ã deux facteurs est considÃ©rÃ© comme difficile et coÃ»teux. A tort. Avec d'autres, VASCO Data Security fournit un serveur d'authentification pouvant Ãªtre intÃ©grÃ© dans toutes les applications

existantes, quel que soit le modÃ¨le de donnÃ©es ou l'architecture, le tout sans achat de matÃ©riel ou de logiciel supplÃ©mentaire. La polyvalence de cette application permet de s'assurer que l'authentification forte est dÃ©ployÃ©e de faÃ§on rentable et sans trop de problÃ¨mes. Il est possible de relier le serveur aux applications Ã travers une API SOAP - une interface de programmation d'application. Un assistant d'installation guide l'utilisateur Ã travers le processus, Ã©tape par Ã©tape. Une installation en douceur et sans effort est ainsi garantie.

DiffÃ©rents packs et applications sont aussi disponibles sur le marchÃ©. Il existe des serveurs d'authentification plug-and-play qui simplifient le dÃ©ploiement de l'authentification Ã deux facteurs de faÃ§on substantielle. Certains fournisseurs offrent aussi une solution d'authentification prÃªte Ã l'emploi (off-the-shelf) qui inclue tous les logiciels et matÃ©riels nÃ©cessaires en un seul package clÃ© en main.

Pour ceux qui pensent que l'intÃ©gration et le maintien des systÃ¨mes de sÃ©curitÃ© posent trop de difficultÃ©s, il existe aussi une solution d'authentification dans le cloud. Chaque demande de connexion est simplement envoyÃ©e Ã un serveur de sÃ©curitÃ© hÃ©bergÃ© qui traite le processus d'authentification. En tant que client, vous n'avez pas plus Ã vous soucier de la disponibilitÃ© et de l'Ã©volution de la solution. Des solutions modernes telles que le DIGIPASS as a Service vont mÃªme un peu plus loin et offrent un package de service complet, comprenant l'installation et l'activation des dispositifs d'authentification. GrÃ¢ce Ã l'externalisation, le processus devient transparent pour l'utilisateur final. Le message, comme la conception du dispositif d'authentification, peuvent Ãªtre personnalisÃ©s conformÃ©ment aux souhaits du client. De cette faÃ§on, nous n'avons pas Ã rÃ©inventer la roue et pouvons nous concentrer sur nos activitÃ©s principales. La solution est prÃªte Ã utiliser, possÃ¨de une Ã©volutivitÃ© quasiment illimitÃ©e et seule la capacitÃ© utilisÃ©e doit Ãªtre payÃ©e.

Un concept innovant

Une autre solution pratique est MYDIGIPASS.COM. Cette plateforme hÃ©bergÃ©e destinÃ©e aux particuliers garantit un login sÃ©curisÃ© aux applications et services web grÃ¢ce Ã l'utilisation de l'authentification forte et rÃ©sout parfaitement la double question de la sÃ©curitÃ© et de l'ergonomie. Ce service simplifie la gestion de ses mots de passe par l'utilisateur final. La plateforme fournit un environnement d'authentification unique (SSO) : une fois qu'un utilisateur d'Internet a ouvert une session sur MYDIGIPASS.COM, il a accÃ¨s Ã chaque application qui est enregistrÃ©e sur la plateforme. Il n'a qu'Ã se connecter une fois avec son mot de passe fort et l'accÃ¨s sera accordÃ© Ã l'ensemble de ses applications. En outre, le service offre un emplacement central permettant Ã l'utilisateur de stocker, mettre Ã jour et partager ses informations d'identification. Imaginez combien de fois nous avons Ã inscrire notre nom, date de naissance ou adresse pour nous enregistrer et crÃ©er un compte sur un nouveau service. Ces tracas relÃ¨vent du passÃ© avec MYDIGIPASS.COM. L'utilisateur lui-mÃªme dispose d'un parfait contrÃ´le sur les informations qu'il souhaite partager. La plate-forme permet aussi aux utilisateurs de tÃ©lÃ©charger gratuitement une version mobile de l'application DIGIPASS qui gÃ©nÃ¨re de faÃ§on dynamique des mots de passe forts sur le tÃ©lÃ©phone de l'utilisateur final.