Les rÃ©seaux sociaux, Â« faille insidieuse Â» des cyberattaques
Internet
PostÃ© par : JerryG
PubliÃ©e le : 18/11/2013 14:00:00

Les cyberattaques sont plus sophistiquÃ©es que jamais et les techniques de hacking ne cessent dâ□□Ã©voluer, de se renouveler. Aujourdâ□□hui, force est de constater que la menace ne provient plus exclusivement de lâ□□extÃ©rieur. Au sein dâ□□une organisation, les utilisateurs sont Ã la fois victimes et potentiels Â« cybercriminels Â» notamment dans le cadre de leur usage des rÃ©seaux sociaux.

Les bonnes pratiques de lâ□□usage des rÃ©seaux sociaux au bureau Afin de rÃ©duire les risques dâ□□attaques et de renforcer la sÃ©curisation des donnÃ©es, les entreprises doivent former les employÃ©s aux bonnes pratiques de lâ□□usage des rÃ©seaux sociaux au bureau ; de nombreux utilisateurs ont un comportement Ã risque par manque de sensibilisation et/ou parce quâ□□ils ne mesurent pas les dangers quâ□□ils font prendre aux organisations.

Pourtant, les menaces les plus importantes proviennent surtout des sites professionnels tels que LinkedIn ou Viadeo, qui sont des sources intarissables dâ□□informations Ã trÃ¨s forte valeur ajoutÃ©e sur les entreprises pour les hackers.

Ceux-ci ont accÃ¨s en Â« libre-service Â» Ã un trÃ¨s grand nombre dâ□□informations sur lâ□□activitÃ© de lâ□□entreprise qui leur permettent de rÃ©cupÃ©rer des donnÃ©es sensibles. Les rÃ©seaux sociaux professionnels sont, en effet, le point dâ□□entrÃ©e Ã des informations sur les employÃ©s, leur rÃ´le dans lâ□□entreprise, leurs fonctions quotidiennes, voire les nombreuses informations sur les outils de sÃ©curitÃ© utilisÃ©s et les problÃ©matiques auxquelles ils ont Ã©tÃ© exposÃ©s.

Les hackers utilisent actuellement lâ□□ensemble des vecteurs Ã leur disposition : ils peuvent Ã©galement pirater des informations professionnelles via un terminal personnel lorsque lâ□□employÃ© utilise ses propres outils (BYOD) ou travaille de chez lui Ã partir de son ordinateur personnel.

Aujourdâ□□hui, les brÃ¨ches de sÃ©curitÃ© sont progressives et permettent aux pirates de sâ□□introduire dans les systÃ¨mes informatiques de la maniÃ¨re la plus discrÃ¨te possible pour collecter le maximum dâ□□informations et accÃ©der petit Ã petit aux donnÃ©es les plus critiques.

Le Community Manager, danger insoupÃ§onnÃ© Le Community Manager a un rÃ´le clÃ© dans une entreprise puisquâ□□il gÃ¨re son image et sa prÃ©sence sur les rÃ©seaux sociaux. Il ne sâ□□agit pas tant de ses privilÃ¨ges (qui sont finalement peu Ã©levÃ©s) que de son impact sur lâ□□image et la communication officielle de lâ□□entreprise sur les mÃ©dias sociaux. Le dÃ©tournement de ce type de compte est aujourdâ□□hui une cible privilÃ©giÃ©e de groupes cherchant Ã nuire Ã lâ□□image dâ□□une sociÃ©tÃ© ou Ã profiter de sa notoriÃ©tÃ© pour passer des messages non sollicitÃ©s ou diffuser des informations confidentielles.

Par ailleurs, lorsquâ□□un salariÃ© quitte lâ□□entreprise, il doit rendre ses clÃ©s, son badge mais

les employeurs ne pensent pas nÃ©cessairement Ã changer ses mots de passe. Or, un Community Manager ou autre employÃ© mÃ©content qui quitte lâ□□entreprise emportant avec lui identifiants et mots de passe pourrait Ã©galement lui nuire sans difficultÃ©s â□□ tout salariÃ© dâ□□une entreprise est susceptible de conserver ses donnÃ©es de connexion aprÃ¨s son dÃ©part de la sociÃ©tÃ©.

Prenons lâ□□exemple rÃ©cent de lâ□□affaire PRISM, il ressortirait que l'ancien analyste de la NSA, **Edward Snowden**, aurait accÃ©dÃ© Ã des informations extrÃªmement confidentielles grÃ¢ce aux identifiants de connexion de plusieurs de ses collÃ¨gues, qu'il aurait convaincu de lui fournir en prÃ©textant un travail qu'il devait faire, en tant qu'administrateur du systÃ¨me informatique. Ce type de comportements peut avoir des consÃ©quences catastrophiques sur lâ□□Ã©conomie dâ□□une entreprise et engendrer des dommages collatÃ©raux durables (perte de clients, impact sur le cours des actions en bourse pour les sociÃ©tÃ©s cotÃ©es, retrait dâ□□investisseurs/business angelsâ□¦).

De lâ□□importance dâ□□appliquer et transmettre les bonnes pratiques. Les cyberattaques sont une rÃ©alitÃ© pour tous et les entreprises comme les employÃ©s doivent prendre conscience que chaque individu est une porte dâ□□accÃ¨s aux donnÃ©es sensibles dâ□□une sociÃ©tÃ©. Pour ce faire, les organisations peuvent appliquer plusieurs rÃ¨gles simples et peu coÃ»teuses afin de renforcer la sÃ©curisation des informations :

ï□□ Sensibiliser les utilisateurs au fait que le risque existe et quâ□□ils doivent adopter un comportement de mÃ©fiance vis-Ã -vis dâ□□informations en provenance de lâ□□extÃ©rieur, mais Ã©galement de lâ□□intÃ©rieur â□□ le fait de partager un simple mot de passe avec un collÃ¨gue, peut aussi Ãªtre considÃ©rÃ© comme un comportement Ã risque.

ï□□ Identifier la source et le parcours des hackers afin de paralyser lâ□□attaque et le retrait de donnÃ©es sensibles.

ï□□ Mettre en place des solutions de dÃ©tection pour alerter les personnes responsables de lâ□□entreprise quâ□□un compte sensible est en cours dâ□□utilisation (peut-Ãªtre frauduleuse) afin de favoriser une intervention rapide.

ï□□ Identifier et sÃ©curiser les comptes Ã privilÃ¨ges au sein des entreprises, premiÃ¨res cibles des attaquants puisque souvent mÃ©connus et nÃ©gligÃ©s.

En conclusion, pour parer au maximum Ã ces Â« failles humaines Â», employÃ©s et entreprises doivent redoubler de vigilance pour un usage plus rÃ¨glemente des rÃ©seaux sociaux professionnels et privÃ©s**, confirme Olivier Prompt**, Regional Sales Engineer, Northern Europe & Africa chez Cyber-Ark Software.