La cybersÃ©curitÃ© de demain, au-delÃ du mot de passe
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/10/2021 13:00:00

A lâoccasion du mois europÃ©en de la cybersÃ©curitÃ©, qui vise Ã sensibiliser les utilisateurs aux cybermenaces et aux habitudes Ã prendre pour sâen protÃ©ger, il convient de faire le point sur les risques qui perdurent. Le plus connu de tous : le mot de passe.

Lâ□□ANSSI a dâ□□ailleurs rÃ©cemment mis Ã jour son guide dÃ©diÃ© Ã lâ□□authentification multifacteur et aux mots de passe. Ces derniers ont leurs preuves avec la sÃ©curitÃ© pÃ©rimÃ©trique, mais ne sont plus aptes Ã protÃ©ger efficacement les donnÃ©es personnelles ou professionnelles. En effet, ces identifiants sont trop souvent mal utilisÃ©s et gÃ©rÃ©s, et ne reprÃ©sentent plus un niveau de sÃ©curitÃ© suffisant face aux techniques des cybercriminels.

Selon JÃ©rÃ´me Colleu, IngÃ©nieur Avant-Vente chez CyberArk, la maniÃ¨re dont les utilisateurs prouve que leur identitÃ© est clÃ©, alors que la frontiÃ¨re entre les sphÃ¨res privÃ©e et professionnelle sâ□□estompe :

Â« Il existe six raisons pour se dÃ©barrasser une fois pour toute des mots de passe, et laisser place Ã des moyens dâ□□authentification plus adaptÃ©s face Ã la sophistication des cybermenaces actuelles.

Des mots de passe faibles. Chaque utilisateur possÃ¨de en moyenne 85 mots de passe entre ses comptes personnels et professionnels. Par consÃ©quent, lorsquâ□□un identifiant expire et doit Ãªtre renouvelÃ©, de nombreuses personnes remplacent simplement un chiffre par un autre, annulant ainsi l'objectif de la rÃ©initialisation obligatoire.

En outre, alors que les Ã©quipes IT continuent de faire campagne pour des mots de passe complexes et uniques, beaucoup dâ□□employÃ©s ne suivent pas ce conseil. Et mÃªme lorsque des identifiants forts sont en place, des habitudes risquÃ©es - telles que l'enregistrement des identifiants dans les navigateurs, le recours Ã des feuilles Excel ou des post-it â□□ restent communes.

Des vols rÃ©guliers de mot de passe et d'identifiants. Il est facile pour les attaquants de voler ou de dÃ©chiffrer les identifiants via des mÃ©thodes courantes, telles que le phishing et l'usurpation d'identitÃ©. Un rapport rÃ©cent de Verizon rÃ©vÃ¨le ainsi que pas moins de 80 % des violations peuvent Ãªtre liÃ©es Ã des identifiants volÃ©es ou rÃ©cupÃ©rÃ©s avec une attaque par force brute.

Une perte de productivitÃ© pour les employÃ©s. Chaque fois quâ□□un utilisateur ne peut accÃ©der Ã un compte ou Ã une ressource de travail, il perd un temps prÃ©cieux. De mÃªme que lâ□□Ã©quipe d'assistance informatique, qui devra probablement rÃ©initialiser le mot de passe ou rÃ©tablir lâ□□accÃ¨s en question. On estime ainsi quâ□□une entreprise de 1 000 employÃ©s dÃ©pense environ 495 000 $ par an Ã rÃ©soudre des problÃ¨mes liÃ©s au mot de passe.

Seulement une premiÃ¨re ligne de dÃ©fense. Des gestionnaires de mots de passe sont pertinents pour mÃ©moriser les mots de passe personnels sans recourir Ã un stockage dans le navigateur. Cependant, ils ne sont pas infaillibles, surtout les mÃªmes identifiants sont utilisÃ©s dans la sphÃ¨re professionnelle.

De plus, ils ne procurent pas une protection adÃ©quate dans les environnements d'entreprise, oÃ¹ les utilisateurs bÃ©nÃ©ficient de diffÃ©rents niveaux d'accÃ¨s au systÃ¨me informatique. Les gestionnaires de mots de passe ne peuvent pas en effet gÃ©rer qui accÃ¨de Ã quelles ressources sensibles et pour combien de temps ; et les Ã©quipes informatiques en parallÃ¨le nâ□□ont quâ□□une visibilitÃ© limitÃ©e sur les Ã©vÃ©nements liÃ©s aux accÃ¨s ; ce qui crÃ©e des failles de sÃ©curitÃ© et une exposition aux risques.

Les mÃ©thodes d'authentification sans mot de passe. Beaucoup dâ□□utilisateurs ressentent une "fatigue de la sÃ©curitÃ©", du fait dâ□□authentification rÃ©pÃ©tÃ©e tout au long de la journÃ©e, ce qui les conduit Ã rechercher des moyens de contourner ou d'ignorer les systÃ¨mes d'authentification.

Les utilisateurs sont dÃ©sormais enclins Ã essayer de nouvelles mÃ©thodes sans mot de passe pour protÃ©ger Ã la fois leurs comptes personnels et les donnÃ©es sensibles de leur entreprise. Ainsi, selon une Ã©tude de Ponemon, une majoritÃ© de professionnels de la sÃ©curitÃ© informatique et d'utilisateurs professionnels (55 %) prÃ©fÃ©reraient une mÃ©thode de protection des comptes qui n'implique pas de mots de passe

Les avancÃ©es technologiques. Des innovations, telles que le machine learning, minimisent les dÃ©sagrÃ©ments courants liÃ©s aux mots de passe en Ã©liminant les demandes de connexion excessives.

En outre, les outils d'authentification unique (SSO) aident les employeurs Ã surmonter les dÃ©fis de sÃ©curitÃ© associÃ©s aux mots de passe traditionnels et Ã automatiser les processus d'octroi d'accÃ¨s manuel, qui peuvent ralentir les Ã©quipes IT. Ces derniers peuvent alors analyser le contexte de l'utilisateur et de l'appareil pour dÃ©terminer si la demande d'accÃ¨s est lÃ©gitime.

Le systÃ¨me sait, par exemple, si l'utilisateur tente d'accÃ©der Ã une base de donnÃ©es qui ne doit pas Ãªtre accessible dans le cadre de ses activitÃ©s quotidiennes, ou si un appareil se trouve dans une ville diffÃ©rente de l'habitude. Si le contexte est anormal, le systÃ¨me enclenche des contrÃ´les, comme une demande de rÃ©authentification ou l'ajustement du niveau d'accÃ¨s. L'analyse permet de minimiser les frictions en mettant en place des barriÃ¨res uniquement lorsque cela est nÃ©cessaire, en fonction d'un score de risque.

En tant que citoyen numÃ©rique, chaque utilisateur a la responsabilitÃ© de protÃ©ger sa part du cyberespace. Beaucoup dâ□□identitÃ©s sont encore vÃ©rifiÃ©es avec un mot de passe ; pour consulter le solde d'un compte bancaire, faire des achats en ligne ou accÃ©der Ã des applications et systÃ¨mes liÃ©s au travail. Cependant, les cybercriminels profitent des vulnÃ©rabilitÃ©s inhÃ©rentes Ã leur mauvaise utilisation, afin de rapidement et facilement voler des informations. Â»