Quelle est la solution idÃ©ale pour se protÃ©ger ?
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 6/5/2022 13:00:00

A lâ□□occasion de la JournÃ©e Internationale du Mot de Passe, qui a eu lieu ce jeudi 5 mai, les entreprises comme les particuliers sont encouragÃ©s Ã repenser la sÃ©curisation de leurs mots de passe. Lâ□□idÃ©al est de trouver le meilleur rapport entre sÃ©curitÃ© et efficacitÃ©.

Voici le commentaire de Regis Alix, Senior Principal Solutions Architect de Quest Software - fournisseur mondial de logiciels de gestion des systÃ¨mes et de sÃ©curitÃ©

Â« Un mot de passe de plus de 24 caractÃ¨res incluant des minuscules, majuscules, chiffres et caractÃ¨res spÃ©ciaux changÃ© frÃ©quemment, mais sans rÃ©gularitÃ© peut Ãªtre considÃ©rÃ© comme sÃ»r. Ã□videmment, de telles caractÃ©ristiques rendent les mots de passe impossibles Ã mÃ©moriser et inaccessibles Ã de nombreux utilisateurs qui ne veulent pas passer des heures Ã gÃ©rer cette complexitÃ©.

Ils chercheront Ã augmenter leur efficacitÃ© en simplifiant leurs mots de passe parfois Ã lâ□□extrÃªme. Â« Password Â» et Â« 123456 Â» demeurant les plus couramment utilisÃ©s. Tous ne sont pas aussi simples, mais une autre erreur est frÃ©quemment commise : la rÃ©utilisation.

Pensant bien faire, un utilisateur peut Ãªtre tentÃ© de crÃ©er un mot de passe moyennement complexe et de lâ□□utiliser sur un grand nombre de ressources, sites, applications, etc.

Bien entendu, si une fuite intervient sur une des ressources, un attaquant pourrait obtenir le mot de passe correspondant et tenter de lâ□□utiliser ailleurs (password spraying : tentative de connexion en utilisant des mots de passe simples, contextuels (Printemps2022!) ou encore issus listes dâ□□identifiants piratÃ©s au prÃ©alable en vente sur le dark web). Plus le mot de passe est rÃ©utilisÃ©, plus les chances quâ□□Ã un attaquant de parvenir Ã accÃ©der Ã une nouvelle ressource sont grandes.

Lâ□□idÃ©al est de trouver le meilleur rapport entre sÃ©curitÃ© et efficacitÃ©. Des mots de passe moins sÃ©curisÃ©s, mais plus faciles Ã retenir associÃ©s Ã une authentification multifacteurs (MFA) sont acceptables pour certains environnements. La mise en place dâ□□une architecture Zero Trust peut venir complÃ©ter ce principe de faÃ§on Ã compartimenter au maximum les autorisations au cas oÃ¹ un compte soit corrompu.

Enfin, des Ã©diteurs comme Microsoft travaillent Ã la mise en place dâ□□authentification Â« sans mot de passe Â», mais cette mÃ©thode est encore loin de se dÃ©mocratiser. Les applications de gestion de mots de passe, solutions pratiques, mais qui ne font que dÃ©caler le problÃ¨me (il faut un mot de passe pour y accÃ©derâ□¦) ont encore de beaux jours devant elles. Â»Â