PME et authentification : comment dÃ©passer les risques
Internet
PostÃ© par : JPilo
PubliÃ©e le : 9/6/2023 14:00:00

Les petites entreprises ont tendance Ã sous-estimer la probabilitÃ© dâ□□Ãªtre la cible dâ□□une attaque, pensant que les cybercriminels sâ□□en prennent plutÃ´t aux grands groupes, du fait de quantitÃ©s importantes de donnÃ©es lucratives stockÃ©es par ces organisations.

En rÃ©alitÃ©, toutes les entreprises sont victimes de cyberattaques Ã la mÃªme frÃ©quence, indÃ©pendamment de leur taille : le rapport de 2023 de Netwrix en matiÃ¨re de sÃ©curitÃ© hybride rapporte ainsi que 65 % des grands groupes ont Ã©tÃ© victimes dâ□□un incident de sÃ©curitÃ© au cours des 12 derniers mois, un chiffre similaire pour les organisations de toutes tailles (68 %).

Selon Pierre-Louis Lussan, Country Manager Southern Europe & Belux chez Netwrix, les Petites et Moyennes Entreprises (PME) devraient investir dans des solutions clÃ©-en-main, afin de faire face Ã la sophistication accrue des cybercrimes ciblant une surface dâ□□attaque grandissante : les comptes utilisateurs.

Â« Un compte, quel quâ□□en soit lâ□□utilisateur â□□ salariÃ©, partenaire ou prestataire avec un accÃ¨s lÃ©gitime â□□ peut devenir un point dâ□□accÃ¨s au rÃ©seau pour les cybercriminels dÃ¨s lors quâ□□il est compromis.

Ces derniers disposent de nombreux subterfuges pour compromettre les mots de passe ; dont notamment recourir Ã des databases dâ□□identifiants volÃ©s ou tenter de les deviner. NÃ©anmoins, les petites organisations rencontrent des difficultÃ©s pour se prÃ©munir contre les compromissions de comptes, Ã cause de ressources humaines et budgÃ©taires limitÃ©es.

Il est ainsi possible dâ□□exiger une authentification multi-facteurs (MFA) qui renforce la sÃ©curitÃ© en imposant une seconde Ã©tape dâ□□authentification Ã la suite de la saisie du nom dâ□□utilisateur et mot de passe. Cependant, des attaques appelÃ©es "Pass-the-Cookie" ont vu le jour : utilisant les cookies du navigateur pour contourner la MFA, elles permettent aux cybercriminels dâ□□accÃ©der aux services cloud et Ã dâ□□autres ressources informatiques.

Par consÃ©quent, il est indispensable de continuer Ã exiger des mots de passe robustes et uniques pour tous les comptes, afin de limiter les risques de compromission.

Cependant, mÃ©moriser des identifiants complexes et en grand nombre est impossible, raison pour laquelle les organisations doivent fournir un outil facile dâ□□utilisation pour les employÃ©s crÃ©ant des mots de passe robustes, les stockant de faÃ§on sÃ©curisÃ©e, et qui complÃ¨te automatiquement et systÃ©matiquement le mot de passe adÃ©quate Ã lâ□□authentification sur les divers systÃ¨mes et sites web.

Tout le monde y gagnera : les gestionnaires de mots de passe amÃ©liorent la sÃ©curitÃ©, tout en permettant aux utilisateurs dâ□□Ãªtre plus efficaces et productifs en ne perdant pas de temps lors de lâ□□authentification.

En outre, un gestionnaire de mots de passe optimal simplifie Ã©galement le quotidien des Ã©quipes informatique et de sÃ©curitÃ©, qui sont alors nettement moins sollicitÃ©es par les utilisateurs au sujet de leurs mots de passe.

Ces Ã©quipes gagnent Ã©galement du temps et peuvent se concentrer sur des tÃ¢ches Ã plus forte valeurs ajoutÃ©es, car ces outils automatisent la rÃ©initialisation des mots de passe. Enfin, ces technologies diminuant le risque de compromission de comptes, ces experts IT Ã©quipes consacreront moins de temps aux efforts de remÃ©diation ; une activitÃ© stressante et couteuse.

Ã□videmment, pour les PME, le manque de moyens financiers peut Ãªtre un frein Ã la sÃ©curisation de leurs environnements informatiques. Afin dâ□□accÃ©der Ã des services de gestion de mots de passe plus abordables, elles peuvent donc se tourner vers des solutions Ã tarification Ã plusieurs niveaux. Ceci leur permettra de dÃ©buter avec un nombre rÃ©duit de licences, avant dâ□□en acquÃ©rir de nouvelles grÃ¢ce aux avantages engrangÃ©s suite Ã cette adoption.

Les cybercriminels tentent de compromettre les identifiants de connexion des salariÃ©s dans les petites entreprises pour diverses raisons. Les PME ont, dâ□□une part, des informations sensibles qui peuvent Ãªtre volÃ©es et revendues sur le dark web.

Dâ□□autre part, elles constituent une porte dâ□□entrÃ©e vers les entreprises plus grandes avec lesquelles elles entretiennent des relations, en tant que client, fournisseur, ou encore prestataire de services. Il est par consÃ©quent essentiel que ces organisations instaurent des politiques de mots de passe strictes et quâ□□elles facilitent leur mise en Å□uvre par les salariÃ©s. Â»