Authentification sans mot de passe
Internet
PostÃ© par : JerryG
PubliÃ©e le : 29/1/2024 13:00:00

A l'occasion de la 18Ã¨me JournÃ©e internationale de la protection des donnÃ©es, cÃ©lÃ©brÃ©e chaque annÃ©e le 28 janvier, Fabrice de VÃ©sian, Sales Manager France chez Yubico, explique comment les organisations et les particuliers peuvent amÃ©liorer leurs pratiques en matiÃ¨re de sÃ©curitÃ© des donnÃ©es grÃ¢ce Ã l'authentification sans mot de passe :

Â« Le phishing reste la mÃ©thode d'attaque la plus rÃ©pandue en raison de son coÃ»t relativement faible et de son taux de rÃ©ussite Ã©levÃ©, et les progrÃ¨s de l'IA ne font dÃ©sormais qu'accentuer ce problÃ¨me. Malheureusement, les organisations ne font pas assez pour mettre Ã niveau les outils et les mÃ©thodes de cybersÃ©curitÃ© utilisÃ©s pour protÃ©ger leur personnel et leurs clients.Â

Alors que le taux d'attaques sophistiquÃ©es par phishing continue d'augmenter, la JournÃ©e de la protection des donnÃ©es met en Ã©vidence le besoin critique d'une authentification moderne et rÃ©sistante Ã ces attaques pour rester en sÃ©curitÃ©, aussi bien de la part des entreprises que des particuliers.

Il est clair que les noms d'utilisateurs et les mots de passe traditionnels ne suffisent plus Ã assurer la sÃ©curitÃ© des donnÃ©es, mais ils restent malheureusement l'une des formes d'authentification les plus utilisÃ©es dans le monde au sein des entreprises. Ceci expose non seulement les donnÃ©es personnelles des employÃ©s Ã des tentatives de phishing, mais aussi celles de lâ□□organisation. Cela peut entraÃ®ner d'importants dommages financiers et de rÃ©putation.

L'authentification de base par nom d'utilisateur et mot de passe est trop facile Ã contourner pour les cybercriminels, ce qui permet un accÃ¨s non autorisÃ© aux comptes en ligne et aux donnÃ©es personnelles. Une fois le mot de passe volÃ©, ils peuvent passer outre de nombreuses formes d'authentification multi-facteur (MFA), telles que les codes de passe Ã usage unique (OTP) par SMS.Â

De mÃªme, l'authentification basÃ©e sur une application mobile reste une mÃ©thode faillible. Elle apporte en effet un certain nombre de contraintes sur les organisations et les utilisateurs qui doivent changer rÃ©guliÃ¨rement leur mot de passe malgrÃ© tout, espÃ©rer avoir du rÃ©seau et de la batterie, et ajoute beaucoup plus d'Ã©tapes qu'une authentification sans mot de passe.

Une protection fiable contre les cybermenaces modernes nÃ©cessite une mÃ©thode d'authentification moderne et rÃ©sistante au phishing, telle que les clÃ©s de sÃ©curitÃ© matÃ©rielles, qui peuvent mettre fin aux attaques en exigeant que l'on insÃ¨re dans l'appareil quelque chose que l'on possÃ¨de (une clÃ© de sÃ©curitÃ©) et que lâ□□on saisisse quelque chose que lâ□□on connaÃ®t (un mot de passe), puis que l'on touche physiquement l'appareil pour avoir accÃ¨s aux comptes. L'utilisation de cette mÃ©thode d'authentification est essentielle pour protÃ©ger les donnÃ©es personnelles contre des cyberattaques. Â»