Cyber-criminalitÃ© : L'authentification un facteur de sÃ©curitÃ©.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 24/1/2019 13:00:00

Les violations de donnÃ©es, le phishing, et lâ□□Ã©laboration de rÃ©glementations favorisent lâ□□adoption rapide de lâ□□authentification forte. Selon le rapport 2019 de Javelin Strategy & Research sur l'Ã©tat actuel de l'authentification forte, le recours Ã l'authentification sÃ©curisÃ©e par cryptographie a triplÃ© depuis 2017

Alors que les violations de donnÃ©es et les attaques par phishing, de plus en plus sophistiquÃ©es, continuent d'alimenter les compromissions de comptes en ligne et les pertes financiÃ¨res, le rapport 2019 de Javelin Strategy & Research, sur lâ□□Ã©tat de lâ□□authentification forte, indique que les entreprises intensifient leurs efforts, et investissent dans des processus plus rÃ©sistants.

Le rapport, sponsorisÃ© par lâ□□Alliance FIDO, analyse lâ□□Ã©tat des pratiques en termes dâ□□authentification des clients et des employÃ©s dâ□□entreprises amÃ©ricaines, et tire les conclusions sur le rÃ´le jouÃ© par lâ□□authentification forte dans la protection des comptes, mais aussi dans la sÃ©curisation de lâ□□accÃ¨s aux donnÃ©es importantes et aux systÃ¨mes critiques.

Voici les principales conclusions et recommandations du rapport :

â□¢ Le recours Ã lâ□□authentification forte a considÃ©rablement augmentÃ© depuis 2017. Â

Le nombre d'organisations recourant Ã l'authentification forte basÃ©e sur la cryptographie Ã clÃ© publique a triplÃ© depuis 2017 en ce qui concerne l'authentification du consommateur.

Elle a augmentÃ© de prÃ¨s de 50 % pour l'authentification en entreprise sur la mÃªme pÃ©riode.

Cette mÃ©thode dâ□□authentification prÃ©sente lâ□□avantage de ne pas Ãªtre sensible au phishing, aux attaques de lâ□□homme du milieu (ou Â« man-in-the-middle Â»), ou Ã toute autre attaque ciblant les identifiants â□□ ce qui nâ□□est pas le cas des mots de passe et mots de passe Ã usage unique (OTP), qui y sont vulnÃ©rables.

â□¢ La rÃ©glementation accÃ©lÃ¨re le passage Ã l'authentification forte. PrÃ¨s de 70 % des entreprises estiment Ãªtre soumises Ã une forte pression rÃ©glementaire pour proposer une authentification forte Ã leurs clients.Â

Cette statistique est notamment liÃ©e Ã lâ□□entrÃ©e en vigueur de la directive DSP2, ainsi quâ□□Ã la rÃ©glementation en matiÃ¨re de protection des donnÃ©es dans les Ã□tats de lâ□□Union EuropÃ©enne et aux Ã□tats-Unis, comme par exemple en Californie.

â□¢ Le non-recours aux systÃ¨mes d'authentification forte prÃ©sente un risque sous-estimÃ© pour les entreprises et leurs clients. Bien que les cybercriminels ciblent une grande variÃ©tÃ© dâ□□informations confidentielles, les deux tiers des entreprises utilisent uniquement des mots de passe pour authentifier leurs employÃ©s.Â

Elles estiment en effet que ces derniers sont suffisants pour le type de donnÃ©es quâ□□elles protÃ¨gent.

â□¢ Toutes les mesures dâ□□authentification forte ne sont pas Ã©gales. Selon Javelin, lâ□□adoption de solutions d'authentification forte qui sont basÃ©es sur des normes et qui utilisent une sÃ©curitÃ© cryptographique, telle que celles proposÃ©es par lâ□□Alliance FIDO, peut aider les entreprises Ã rÃ©duire les coÃ»ts liÃ©s au respect de la rÃ©glementation, aux attentes des clients, et Ã des systÃ¨mes de fraude de plus en plus sophistiquÃ©s.

â□□ Il est temps de mettre un terme aux OTP. Alors que les cybercriminels utilisent l'ingÃ©nierie sociale, le portage tÃ©lÃ©phonique et les malwares pour compromettre les authentificateurs OTP, Javelin recommande de les dÃ©laisser, au profit dâ□□une authentification forte sÃ©curisÃ©e par cryptographie.

Le rapport inclut des Ã©tudes de cas de Google, Tradelink et Visa, qui s'appuient toutes sur l'authentification FIDO pour renforcer la protection des comptes de leurs clients et de leurs employÃ©s.

Â« Lâ□□augmentation du recours Ã lâ□□authentification forte est somme toute assez logique. En effet, malgrÃ© lâ□□augmentation des violations de donnÃ©es, des attaques par phishing, et des pressions dans le domaine rÃ©glementaire, les coÃ»ts financiers, associÃ©s Ã la mise en Å□uvre de lâ□□authentification forte ont, eux, diminuÃ©, explique Al Pascual, vice-prÃ©sident et directeur de la recherche, chez Javelin Strategy & Research.

Ce qui est moins encourageant, câ□□est que les sociÃ©tÃ©s nâ□□adoptant pas ces solutions pensent que les mots de passe seuls constituent une sÃ©curitÃ© suffisante. Elles doivent comprendre que mÃªme les donnÃ©es Ã faible risque peuvent avoir une valeur non nÃ©gligeable pour les fraudeurs, et les exposer Ã un contrÃ´le rÃ©glementaire.Â

Il est nÃ©cessaire pour elles de planifier dÃ¨s maintenant leur passage Ã une authentification forte, sous peine de demeurer une cible de choix pour les cybercriminels. Â»

Â« Les entreprises reconnaissent enfin que les mots de passe et OTP ne fournissent pas une protection suffisante contre les menaces actuelles, confie Brett McDowell, directeur exÃ©cutif de lâ□□Alliance FIDO.Â

Nous espÃ©rons que cette Ã©tude contribuera Ã mieux faire connaÃ®tre les nouvelles capacitÃ©s d'authentification reposant sur la cryptographie, conformes aux normes industrielles de lâ□□Alliance FIDO et du W3C, et dÃ©sormais largement disponibles sur les principales plateformes d'applications internet et mobiles.

Ces fonctionnalitÃ©s permettent aux applications de lier les informations dâ□□identification du compte au pÃ©riphÃ©rique physique de lâ□□utilisateur, de sorte quâ□□elles ne peuvent pas Ãªtre rÃ©cupÃ©rÃ©es via des attaques par phishing.Â

Les plateformes regroupent ces fonctionnalitÃ©s de sÃ©curitÃ© dans des expÃ©riences plus pratiques pour les utilisateurs, leur permettant dâ□□utiliser leur empreinte, leur visage, ou leur clÃ© de sÃ©curitÃ© pour se connecter Ã tous leurs sites internet et applications favoris. Â»

Le rapport complet de Javelin Strategy & Research.