GouvernÃ© par lâ□□identitÃ© numÃ©rique : SÃ©curitÃ© impÃ©rative
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/8/2021 15:00:00

Selon le rapport de lâ□□Observatoire de la sÃ©curitÃ© des moyens de paiement 2020, publiÃ© par la Banque de France, les paiements en ligne effectuÃ©s en 2020 au moyen dâ□□une carte bancaire franÃ§aise ont reprÃ©sentÃ© un montant de prÃ¨s de 150 milliards dâ□□euros, vÃ©ritable terreau fertile pour les fraudeurs.

Dans les opÃ©rations dâ□□e-commerce, les paiements Ã distance ont enregistrÃ© une hausse de la fraude de 16,4 % par rapport Ã 2019, laquelle repose sur deux facteurs : lâ□□augmentation des achats en ligne stimulÃ©e par la pandÃ©mie de Covid-19, et la multiplication des attaques menÃ©es par les acteurs malveillants.

Pour Duncan Godfrey, VP Security Engineering chez Auth0, Ã cette Ã©poque de transition oÃ¹ les entreprises traditionnelles commencent Ã ressembler davantage Ã un ensemble dâ□□applications tournÃ©es vers le consommateur â□□ de sorte quâ□□elles ne peuvent pas se permettre dâ□□ignorer les enjeux de sÃ©curitÃ© associÃ©s Ã la gestion des identitÃ©s et accÃ¨s des clients â□□ lâ□□identitÃ© devrait figurer en tÃªte des prioritÃ©s des RSSI.

Â« DerriÃ¨re chaque opÃ©ration se cache un utilisateur humain ou une machine, et les organisations doivent aujourdâ□□hui constamment vÃ©rifier leur authenticitÃ©, et sâ□□assurer quâ□□ils sont bien ceux quâ□□ils prÃ©tendent Ãªtre. Ces identitÃ©s numÃ©riques sont omniprÃ©sentes, et elles regroupent un ensemble dâ□□attributs qui dÃ©finissent un utilisateur particulier dans le contexte dâ□□une fonction assurÃ©e par une application particuliÃ¨re.

Le plus souvent, une protection est nÃ©cessaire. Dans le domaine de la gestion des identitÃ©s et des accÃ¨s (IAM), celle qui concerne plus spÃ©cifiquement les clients (CIAM) est axÃ©e sur la gestion des identitÃ©s des consommateurs qui doivent accÃ©der Ã des sites web, Ã des services dâ□□e-commerce et Ã dâ□□autres applications en ligne.

Il est compliquÃ© de gÃ©rer la CIAM. Câ□□est un fait. Non seulement parce que les applications sont susceptibles dâ□□Ãªtre exposÃ©es Ã des attaques Ã grande Ã©chelle sur internet, mais aussi en raison des tenants et aboutissants de la gestion des identitÃ©s des clients. Les consommateurs forment un groupe hÃ©tÃ©rogÃ¨ne, et il nâ□□est pas simple de faire la diffÃ©rence automatiquement entre un utilisateur un peu perdu et un attaquant avancÃ©.

En outre, la sÃ©curisation des identitÃ©s des clients est encore compliquÃ©e par lâ□□incapacitÃ© gÃ©nÃ©ralisÃ©e du secteur Ã protÃ©ger les donnÃ©es. Compte tenu de la frÃ©quence des compromissions de mots de passe et de lâ□□accÃ¨s Ã des outils dâ□□attaque automatisÃ©s, le mot de passe traditionnel est dÃ©sormais un moyen de protection obsolÃ¨te.

Aujourdâ□□hui, nous ne pouvons pas ignorer lâ□□Ã©vidence : lâ□□identitÃ© numÃ©rique contrÃ´le lâ□□accÃ¨s Ã des applications et des services de plus en plus nombreux. Ã terme, elle aura une incidence sur tous les aspects de la vie moderne, voire les rÃ©gira, ce qui fera de lâ□□authentification et de lâ□□autorisation des facteurs essentiels pour maintenir la confiance et la sÃ©curitÃ©.

Les conclusions de lâ□□observatoire font largement Ã©cho Ã nos propres observations. PremiÃ¨rement, les enregistrements frauduleux constituent un danger qui peut coÃ»ter cher. Bien

que les taux varient selon les secteurs dâ□□activitÃ©, environ 15 % de toutes les tentatives dâ□□enregistrement dâ□□un nouveau compte peuvent Ãªtre attribuÃ©es Ã des bots.

Plus quâ□□une simple nuisance, les comptes fantÃ´mes contrÃ´lÃ©s par des cybercriminels reprÃ©sentent un problÃ¨me avec un coÃ»t Ã©levÃ© et un impact nÃ©gatif sur les applications et leurs utilisateurs, tout en gÃ©nÃ©rant des consÃ©quences plus importantes, comme le blanchiment dâ□□argent. DeuxiÃ¨mement, le "credential stuffing" reprÃ©sente une menace de grande ampleur. Une attaque de ce type peut en effet Ãªtre Ã lâ□□origine de plus de 90 % des tentatives de connexion dans un secteur spÃ©cifique, un jour donnÃ©.

Les paiements en ligne et la crÃ©ation de comptes continueront Ã se dÃ©velopper, et les identitÃ©s ne cesseront de se multiplier, tout comme les tentatives de fraude. Pour dissuader les cybercriminels, il est indispensable de perturber lâ□□Ã©conomie des attaques en dÃ©veloppant des services dâ□□identitÃ© selon une approche flexible, fondÃ©e sur la sÃ©curitÃ© dÃ¨s la conception et la dÃ©fense en profondeur.

Dans cette optique, les Ã©quipes IT peuvent dÃ©ployer des mesures dÃ©fensives en amont du processus dâ□□authentification, et tout au long de celui-ci, et mettre en place des pratiques sÃ»res de gestion des sessions pour renforcer leur dÃ©fense.

Dans notre monde numÃ©rique en pleine Ã©volution, dans lequel la CIAM joue un rÃ´le de plus en plus important, il devient primordial de promouvoir lâ□□authentification multi-facteurs (MFA) tout en limitant les frictions et en prÃ©servant la sÃ©curitÃ© des utilisateurs.

Quâ□□il sâ□□agisse de lâ□□authentification progressive, de la MFA adaptive ou des mÃ©thodes biomÃ©triques compatibles avec le standard WebAuthn pour les connexions sans mot de passe, le dÃ©ploiement de capacitÃ©s dâ□□authentification constitue un atout prÃ©cieux dans la lutte contre les violations de donnÃ©es, la prise de contrÃ´le de comptes, le "credential stuffing", le vol dâ□□identitÃ©, les abus de confidentialitÃ© ou encore la fraude Ã la carte de crÃ©dit. Â»