World Password Day : la fin du mot de passe comme identifiant unique

Auteur : Arnaud Gallut, Directeur des Ventes Europe du sud, Ping Identity

La troisième édition du World Password Day qui s'est déroulé le 2 Mai, avait pour objectif de mobiliser l'opinion publique sur la nécessité de disposer de mots de passe robustes. Le fait que les mots de passe sont aujourd'hui omniprésents dans la nouvelle économie numérique n'échappe à personne, et surtout pas aux cybers criminels, qui s'y attaquent en priorité, et savent d'une part qu'ils sont simples à usurper dans la grande majorité, et d'autre part qu'ils sont la porte d'entrée aux informations et aux ressources les plus précieuses. D'après le Data Breach Investigation Report 2017 de Verizon, 81% des cyber attaques réussies ont exploité des mots de passe insuffisamment robustes ou volés. La faible robustesse des mots de passe est de notoriété publique. Bien plus, d'après une récente enquête OVUM, 80% des utilisateurs conservent le même mot de passe pour différents comptes, et 46% des employés utilisent des mots de passe personnels pour leurs comptes professionnels. La raison est simple. Plus les mots de passe sont complexes et multiples, plus ils sont difficiles à mémoriser. Beaucoup d'organismes officiels, la CNIL en France par exemple, recommandent des bonnes pratiques pour limiter les risques, telles que des mots de passe d'au moins 12 caractères de 4 types différents, un mot de passe par compte, des mises à jour régulières, l'absence de tout lien entre le mot de passe et son propriétaire, ou encore l'utilisation d'un gestionnaire de mots de passe. Mais ces pratiques sont peu respectées car elles sont contraires aux attentes des utilisateurs, qui privilégient l'ergonomie et la simplicité d'accès.
Ceci étant dit, ne nous y trompons pas. Quelle que soit leur robustesse et les bonnes pratiques utilisées, les mots de passe n'offrent plus un niveau de sécurité suffisant pour protéger les données les plus sensibles. Dans l'immense majorité des cas, ils sont devenus simples à usurper, et n'importe quel cyber criminel sérieux, s'il y met les moyens, mettra moins d'une journée par y parvenir. Sans compter qu'il pourra se servir sur le 'dark web', où des milliards d'identifiants sont disponibles à un prix modique.

De nouveaux standards à la rescousse du mot de passe

Le W3C (World Wide Web Consortium) et la FIDO Alliance, à l'origine des standards les plus répandus d'Internet, ont récemment finalisé l'API WebAuthn, dont l'objectif avoué est de généraliser une authentification sans mot de passe (Passwordless). WebAuthn est disponible gratuitement et déjà supportée par tous les principaux navigateurs, ainsi que par Android et Windows 10. Il permet aux fournisseurs de services de remplacer le mot de passe par une validation de l'authentification de l'utilisateur sans transmettre de données sensibles en y procédant localement sur son poste de travail (tablette, périphérique ou smartphone). La validation de l'authentification s'effectue alors par des moyens tiers interfacés avec cette API, tels qu'une clé de sécurité USB ou une montre connectée par exemple. L'intérêt de cette API est de ne plus avoir de mot de passe à véhiculer sur les réseaux.

La biométrie, remède miracle ?

Beaucoup d'acteurs de l'industrie high tech prédisent la disparition totale des mots de passe comme méthode d'identification, et son remplacement notamment par des systèmes biométriques. Les systèmes de lecture d'empreintes digitales et de reconnaissance faciale se multiplient ainsi depuis plusieurs années, en particulier sur les terminaux mobiles. Toutefois, les solutions biométriques ne sont pas non plus immunisées contre les attaques. La technologie de lecture des empreintes digitales s'est certes grandement améliorée ces dernières années, mais n'est toujours pas infaillible. Elle peut notamment être prise en défaut par des solutions d'intelligence artificielle et de machine learning qui permettent de réaliser des empreintes 'passe partout'. Même chose pour les solutions de reconnaissance faciale, dont certaines peuvent être trompées à l'aide d'une simple photo d'identité.

Authentification multifacteur et SSO : le duo gagnant

La biométrie utilisée seule a donc elle aussi ses faiblesses. Cela ne veut pas dire qu'elle est inutile, mais simplement qu'elle souffre des même défauts qu'un mot de passe en tant qu'authentification unique. Que ce soit en utilisant un visage imprimé en 3D, en créant de fausses empreintes, ou en craquant simplement un mot de passe de secours trop faible, il est beaucoup plus facile pour un attaquant de s'emparer d'un compte utilisateur qui n'est pas protégé par au moins deux facteurs d'authentification.

L'authentification multifacteur, associant par exemple biométrie, mot de passe et terminal identifié, est ainsi seule capable d'offrir un niveau maximum de sécurité car elle impose à l'attaquant de prendre le contrôle de non pas un mais plusieurs facteurs. La solution idéale aujourd'hui est de l'associer à des solutions d'authentification unique, ou SSO (Single Sign On) qui permet à un utilisateur d'accéder à de nombreuses applications sans avoir à multiplier les authentifications. Il lui de s'authentifier en début de session, et il peut ensuite accéder à de nombreuses applications sans être contraint de devoir s'identifier sur chacune d'entre elles. On obtient ainsi une solution qui associe une grande simplicité d'utilisation, notamment pour des applications grand public, et un haut niveau de sécurité.