La quête éperdue du mot de passe parfait

TECHNOLOGIE Les récentes attaques de «SIM swapping» ont démontré les faiblesses de la double authentification combinant mot de passe et code reçu par SMS. Les internautes doivent opter pour des méthodes plus sûres pour accéder à leurs comptes en ligne

ANOUCH SEYDTAGHIA
@Anouch

Le directeur de Twitter qui se fait pirater son compte... Twitter. L'incident, qui n'a duré que quelques minutes, aurait pu prêter à sourire. Mais la mésaventure subie par Jack Dorsey il y a une semaine est en réalité dramatique pour la sécurisation des services en ligne. Ce piratage aura des conséquences directes pour des centaines de millions d'internautes qui tentent de protéger leurs comptes sur internet. L'on croyait que taper un mot de passe, puis un code reçu par SMS sur son téléphone, était suffisant. Or c'était un leurre. Et la fin de cette illusion va tous nous obliger à changer nos pratiques sur internet.

Commençons par comprendre en détail ce qui est arrivé à Jack Dorsey. En l'espace de vingt minutes, le directeur de Twitter a tout simplement perdu le contrôle de sa carte SIM et donc de son numéro de téléphone. Un pirate a réussi à transférer ce numéro sur sa propre carte SIM et ainsi à se faire passer pour lui. Et comme le réseau social permettait d'envoyer des tweets directement par SMS – une fonction stoppée depuis cet incident –, le pirate a pu publier, sur le compte de Jack Dorsey, des messages sexistes, racistes et antisémites ainsi que des menaces d'attaque à la bombe.

Victimes de choix

Le transfert de numéro d'une carte SIM à une autre, appelé «SIM swapping», a déjà fait des victimes de choix aux Etats-Unis, dont l'actrice Jessica Alba et des utilisateurs de cryptomonnaies. Pour y parvenir, les pirates contactent un opérateur de téléphonie mobile, se font passer pour leur victime et demandent un transfert de numéro. Peu regardants, les employés des opérateurs s'exécutent et l'usurpation d'identité peut avoir lieu.

Avec parfois des conséquences désastreuses. On le voit depuis plusieurs mois, de plus en plus de services – e-mail, e-banking, réseaux sociaux, etc. – exigent une authentification dite à double facteur. Non seulement un mot de passe est requis, mais aussi ensuite un code envoyé par SMS. Cela permet de s'assurer que même si un pirate possède votre mot de passe, il n'y a aucun risque qu'il possède aussi physiquement votre smartphone. Mais avec le «SIM swapping», ce type d'authentification à double facteur devient totalement inefficace.

«L'authentification à double facteur avec un SMS, autrefois considérée comme forte, ne l'est plus»

STEVEN MEYER, DIRECTEUR DE LA SOCIÉTÉ DE SÉCURITÉ INFORMATIQUE ZENDATA

Aux Etats-Unis, ce type de piratage est aisé. «Là-bas, vous pouvez acheter une carte SIM et ensuite faire migrer votre ancien numéro de téléphone sur la nouvelle carte juste en appelant la hotline. Ce qui est très pratique lorsque vous perdez ou cassez votre smartphone, car en quelques minutes vous pouvez recommencer à l'utiliser», explique Steven Meyer, directeur de la société de cybersécurité ZENData, à Genève. Pour lui, le «SIM swapping» est plus difficile en Europe, les procédures étant plus sécurisées. «Mais ce n'est pas pour autant que ce n'est pas faisable en Suisse, poursuit-il. Il suffit d'aller dans un magasin d'opérateur avec une fausse procuration et une photocopie de la pièce d'identité du propriétaire pour mettre le numéro sur une nouvelle carte SIM. Certes, la présence physique d'une personne rend l'opération plus compliquée, mais pas impossible.»

Les opérateurs se veulent rassurants. «Nous contrôlons l'identité des clients en posant diverses questions personnelles et ils doivent présenter une pièce d'identité. Néanmoins, il ne peut y avoir de certitude à 100%», avance une porte-parole de Swisscom. Sunrise dit n'avoir jamais constaté de cas de «SIM swapping» et précise que «pour l'échange d'une carte SIM ou le transfert d'un numéro sur une nouvelle carte, il faut au moins une identification claire du client conformément aux exigences légales». Salt affirme avoir pris des mesures pour prévenir le «SIM swapping» et affirme qu'«au téléphone, en plus de l'identification, une demande de changement de SIM implique un envoi postal d'une nouvelle carte à l'adresse du client».

Authentification à risque

Peu de risques en Suisse, donc, mais des risques suffisants pour bouleverser notre façon d'accéder à nos comptes en ligne. La combinaison mot de passe+ code reçu par SMS doit tout simplement disparaître. «Cette authentification, autrefois considérée comme forte, ne l'est plus, poursuit Steven Meyer. En plus, le SMS est aussi utilisé pour récupérer un compte pour lequel on aurait oublié le mot de passe (Gmail, PayPal, etc.) et, dans ce cas, l'attaquant n'a même pas besoin de voler votre mot de passe pour faire son attaque.» Le spécialiste note que, dans certains cas, lorsque tous les mots de passe sont synchronisés avec le navigateur Chrome, le pirate peut accéder à tous les mots de passe via un simple SMS...

Du coup, que faire? Steven Meyer fournit plusieurs conseils. D'abord, utiliser toujours un mot de passe long: il ne doit pas forcément comprendre des caractères spéciaux, des majuscules ou des chiffres, mais faire au moins 13 caractères. Il doit bien sûr être unique et ne jamais être utilisé pour deux services différents. Il est aussi conseillé d'utiliser un gestionnaire de mots de passe, tels 1Password, LastPass, Dashlane ou KeePass, à employer tant sur son smartphone que sur son ordinateur.

L'authentification à deux facteurs est, en parallèle, fortement recommandée. Pas via un SMS, on l'a vu, mais via des méthodes plus sécurisées. Fin août, Microsoft publiait une étude indiquant que chaque jour, plus de 300 millions de tentatives de connexion frauduleuses visent ses plateformes Et dans le cas d'une d'utilisation d'une méthode d'authentification à double facteur, moins de 0,1% des attaques se soldent par un succès.

Pas le choix

Steven Meyer recommande ainsi une application d'authentification utilisable sur son smartphone, tel Google Authenticator, qui donnera un mot de passe unique. Une application tierce peut aussi être utilisée: par exemple UBS impose, pour la validation d'achats par carte de crédit, une validation via son application baptisée Access. Certaines applications permettent aussi de s'authentifier grâce au scan de QR codes. Enfin, des clés physiques qui se branchent sur les ordinateurs offrent un haut niveau de sécurité.

De toute façon, les consommateurs n'auront pas le choix: ils devront changer leurs pratiques. Ce mois-ci devait entrer en application, au niveau européen, la directive DSP2, qui impose notamment aux banques de mettre en place une authentification à deux facteurs via deux éléments dans ces trois catégories: quelque chose que l'on sait (un mot de passe), que l'on possède (un appareil) et quelque chose que l'on est (une donnée biométrique). Cette obligation devait débuter le 14 septembre pour les achats en ligne d'une valeur supérieure à 30 euros, mais plusieurs pays viennent de repousser son entrée en vigueur à 2022. Quoi qu'il en soit, la pression sur les marchands en ligne va s'accroître pour qu'ils imposent davantage de sécurité à leurs clients.

99,9%
Selon Microsoft, l'authentification à deux facteurs permet de déjouer 99,9% des attaques.

Mais ce sont surtout les géants du web qui poussent pour davantage de sécurité. Microsoft insiste ainsi pour que des protocoles tels que WebAuthn et CTAP2 soient déployés de manière massive, permettant même de supprimer les mots de passe. Dans ce cas, l'emploi de clés de sécurité FIDO2 permet de garantir le chiffrement de bout en bout des informations d'identification.

Mais il faudra plusieurs années avant que ces protocoles soient adoptés par tout le monde. D'ici là, les pirates auront encore épinglé de nombreuses victimes. ▬

PRATIQUE

Les conseils de base pour sécuriser ses comptes

- Utiliser un mot de passe d'au moins 13 caractères. Ne l'utiliser que pour un seul service
- Employer un gestionnaire de mots de passe (pour smartphone et ordinateur)
- Utiliser une application d'authentification sur son smartphone, tel Google Authenticator.

LT

(MIRJANA FARKAS POUR LE TEMPS)

Aux Etats-Unis, des scandales à répétition

SÉCURITÉ La faiblesse des systèmes de protection de certains établissements financiers américains est montrée du doigt

En Europe, rares sont les clients de banques à voir leurs données volées ou leur compte piraté. Il y a certes eu, il y a quelques jours, ce client de la néo-banque Revolut qui s'était fait voler 30000 francs après avoir cliqué sur un lien frauduleux envoyé par SMS. Mais c'est une exception. Par contre, aux Etats-Unis, la sécurité des institutions financières semble beaucoup plus faible. «Il y a là-bas un réel problème, détaille Steven Meyer, directeur de la société de cybersécurité ZENData, à Genève. On ne parle pas là des grandes banques ni des multinationales, mais de plus petites structures qui sont très en retard dans les meilleures pratiques, telles que l'utilisation du protocole de sécurité TLS (HTTPS). Ces établissements imposent aussi parfois une limite dans la longueur des mots de passe et ne requièrent pas d'authentification forte, par exemple. Il y a un progrès rapide, ces dernières années, chez ces petites banques, car elles ont été la cible d'attaques. Mais on lit encore régulièrement des analyses ou témoignages plutôt alarmants.»

Aux Etats-Unis, le numéro de sécurité sociale est souvent utilisé comme identifiant national et même comme mot de passe

Ajoutons que, aux Etats-Unis, le numéro de sécurité sociale, de neuf chiffres, est très souvent utilisé comme un identifiant national et même un mot de passe, ce qui aboutit à des piratages massifs. En 2017, Equifax, organisme spécialisé dans la cote de crédit, s'était fait dérober les informations sensibles de 143 millions de ses clients. Elle a été condamnée à payer une amende record de 700 millions de dollars. Et cet été, la banque Capital One s'est fait dérober les noms, adresses e-mail, numéros de sécurité sociale, dates de naissance et même numéros de téléphone de 106 millions de ses clients américains et canadiens. En cause, un piratage informatique réalisé par une seule personne, qui a été arrêtée depuis. Cette femme aurait réussi à pénétrer très facilement des systèmes informatiques dont le niveau de sécurité était insuffisant. ▬ A. S.