Sécurité Informatique

PAYS : France
PAGE(S) : 6-7
SURFACE : 100 %
PERIODICITE : Bimensuel

► **6 juin 2017 - N°483**

protection

Houari Yahia, Elcimaï Financial Software : « Le contrôle comportemental continu est la clé dans la lutte contre la fraude bancaire »

Filiale du groupe Elcimaï, Elcimaï Financial Software est un éditeur de logiciel spécialisé dans la dématérialisation et la gouvernance des flux. Il est présent dans de grands groupes bancaires européens. Dans cette interview, Houari Yahia, Product Manager chez Elcimaï Financial Software explique le rôle clé de l'innovation dans la lutte contre la fraude.

Il a été fortement question de cybersécurité lors de la dernière élection présidentielle. Y voyez-vous une tendance ?

Aujourd'hui, la cybersécurité touche l'ensemble des secteurs d'activité, y compris la politique. Nous l'avons constaté durant la dernière présidentielle et les « hacks » subis par l'équipe de campagne d'Emmanuel Macron. Selon une étude de l'éditeur Symantec, la France est dans le top 10 des pays où la cybercriminalité est la plus active. La France est également à l'origine de plus de 9,9 millions d'attaques réseaux et connaît un grand nombre d'attaques ciblées qui concernent à plus de 57% les PME, et à 28,9% les entreprises de plus de 1 500 employés. Les secteurs d'activité les plus touchés sont l'industrie, la banque-finance-assurance et les services. Face à ces chiffres vertigineux et à l'explosion des différentes formes de cybercriminalité (« fraude au président », « social engineering », « phishing »...), il devient indispensable d'offrir des solutions répondant efficacement à ces problématiques.

Comment en est-on arrivé à une telle situation ?

Hier, l'accès à l'agence bancaire n'était possible que du mardi au samedi, avec des heures d'ouverture bien précises. Une fois le sas de sécurité passé et après avoir présenté sa pièce d'identité au guichet, vous pouviez enfin accéder aux services disponibles en agence (retrait CB ou chéquier, passage d'un ordre de bourse, opération de virement, ...). Bien que ces prestations existent toujours en agence, il est bien loin le temps où l'on se bousculait devant le guichet. Les banques en ligne, de plus en plus banalisées, ont révolutionné les usages. Les services bancaires, désormais accessibles à toute heure et partout dans le monde, offrent un gain de temps et une totale autonomie au client.

Ces avantages soulèvent cependant des interrogations en termes de sécurité. Les campagnes d'informations sont-elles suffisantes ? Les banques investissent en permanence dans la lutte contre la cybercriminalité mais le facteur humain, lui, est plus complexe à gérer. Les campagnes d'informations peuvent aider à réduire le risque mais cela est bien souvent insuffisant tant les techniques de fraude se sont multipliées.

Qu'entendez-vous par là ?

Je dis simplement que le « social engineering » ou le « phishing » multi-canal n'existent pas qu'au cinéma... Voici un cas concret : Un escroc prend contact avec l'entreprise, par mail ou téléphone, afin de demander à l'in-

Sécurité Informatique

PAYS :France
PAGE(S) :6-7
SURFACE :100 %
PERIODICITE :Bimensuel

► 6 juin 2017 - N°483

terlocuteur de se connecter à un site « frauduleux » identique à celui de la banque. L'escroc fait exécuter un ordre de virement de 1€, en prétextant des tests de compatibilité. Le fichier est alors récupéré, le montant modifié et le virement émis à destination de la vraie banque, grâce aux codes d'accès précédemment saisis. Cet exemple démontre bien que trop souvent le maillon faible est l'humain.

L'authentification serait-elle le maillon faible ?

La question posée est comment identifier un client se connectant à sa banque en ligne ? La connaissance client allait de soi en agence. Avec la banque en ligne, il faut recourir à la connaissance comportementale pour authentifier le client, et mieux, l'identifier. Contrairement au client se présentant en agence physique, l'accès virtuel ne peut garantir à 100% que le client se connectant est bien celui autorisé. À défaut de pouvoir identifier le client, il convient donc de dresser un profil (« scoring »), en s'appuyant sur ses habitudes, couplées à un moyen d'authentification. Il ne faut pas se leurrer, il n'existe aujourd'hui pas de solution miracle pour éradiquer la cybercriminalité. En revanche, la combinaison de critères d'authentification peut aider à réduire considérablement les risques de fraudes.

Quelles solutions de sécurité sont à la disposition des banques ?

Les acteurs de l'écosystème bancaire appliquent des standards communs d'authentification et, par un usage récurrent, deviennent familiers et rassurants pour le client final. Vous l'aurez compris, l'authentification multi-facteurs ne doit pas être une entrave au parcours client. Celle-ci doit être la plus transparente possible pour le client final, afin de lui offrir une expérience optimale, et pour se faire le contrôle comportemental continusemble être la solution la plus adaptée. En complément du moyen d'authentification utilisé (login/mot de passe, clavier virtuel, la carte ou la clé OTP, le certificat USB, la biométrie ou le QR Code), la connaissance du matériel habituellement utilisé par le client, de ses lieux de connexion, jours/horaires, de son adresse IP, de ses montants habituels ainsi que de ses bénéficiaires sont autant d'informations permettant de « scorer » efficacement un client. Evidemment, celui-ci ne doit être sollicité qu'en cas de doute. Un code unique, permettant de compléter son authentification et/ou sa transaction, peut être envoyé via SMS afin de s'assurer que la personne se connectant est bien celle attendue. Utilisées individuellement, chacune de ces solutions est faillible, il n'y a pas de débat. En revanche, la combinaison de ces solutions renforcera la sécurité client. La sécurité constitue plus que jamais un enjeu stratégique pour l'ensemble de l'écosystème (client, banque, éditeur, prestataire). Dans ce domaine, il conviendra d'innover toujours plus rapidement, sans faire abstraction du dilemme : confort client versus sécurité. •