Les Echos

11/12/2012 08:00

Les fraudeurs aussi apprécient le multicanal !

Une multiplication de cas de fraudes multicanal

Les fraudeurs aujourd'hui savent utiliser les différents canaux de communication pour réaliser leurs méfaits. De multiples cas ont déjà été recensés : utilisation du call center pour faire changer l'email de contact puis récupération des mots de passe par ce nouvel email par l'interface web, interception de courrier pour capter les informations permettant de s'authentifier lors d'un appel au call center…

Les fraudeurs sont aussi particulièrement attentifs au cycle de vie des entreprises : l'été est ainsi une période où les tentatives de fraudes se multiplient. Les conseillers habituels ne sont pas là, les remplaçants sont des stagiaires ou des personnes provenant d'autres secteurs ou entités. Connaissant moins la clientèle et parfois ayant été moins formés, ils sont plus vulnérables en cas de tentative d'ingénierie sociale.

Les entreprises prennent cependant la mesure de ces fraudes et s'équipent en conséquence. Les solutions de détection de la fraude (détection de transaction suspicieuse, scoring…) se mettent progressivement au multicanal avec parfois des difficultés inhérentes à la construction en silo de différents systèmes les supportant. Une solution additionnelle peut être la mise en place d'authentification unique multicanal, elle permet de centraliser toutes les opérations d'accès et donc de détecter les tentatives sur plusieurs fronts à la fois.

Du multicanal au multientreprises pour des fraudes encore plus efficaces

Mais aujourd'hui, les fraudeurs vont encore plus loin : les fraudes sont non seulement multicanaux, mais aussi multientreprises ! Le cas récent d'un journaliste de Wired, Mat Honan, le montre clairement. Celui-ci a vu ses comptes personnels sur internet attaqués. Ses données personnelles ont ensuite été accédées puis altérées (publication de tweets infamant en son nom), voire détruites (effacement à distance de son compte Gmail et de ses différents portables, téléphones et tablettes). Au-delà de cet évènement grave à titre personnel (en particulier quand nous connaissons notre dépendance à tous ces services), il est intéressant d'étudier comment l'attaque a eu lieu.

Le fraudeur a su jouer entre les services clients d'Amazon et d'Apple pour récupérer de manière croisée des informations normalement confidentielles. En particulier, il a joué du service client d'Amazon pour ajouter une fausse carte bancaire en s'authentifiant grâce à l'adresse postale de la victime, puis modifier l'adresse email de contact en s'appuyant sur le faux numéro de carte, puis déclarer sur le site web le mot de passe perdu.

Avec cet accès à l'espace client d'Amazon, il a eu connaissance des 4 derniers chiffres de la «vraie» carte bancaire du journaliste. Une fois cet élément obtenu, il s'en est servi auprès du call center d'Apple, où ces 4 chiffres servent à prouver son identité et donc à modifier le mot de passe de sa victime ! Une fois ce «sésame» obtenu, les méfaits sont simples à réaliser. Suite à cet incident largement médiatisé, des mesures ont été prises, mais tous les services

de relation client peuvent être concernés par ces attaques croisées !

Une nécessaire collaboration entre entreprises dans le futur ?

Pour lutter contre ces scénarios avancés, peu de moyens sont disponibles à l'échelle de l'entreprise. Il est difficile de savoir quelles sont les informations qui vont être confiées par ailleurs et comment ces informations seront protégées pour chaque service. D'autant plus que les clients privilégient souvent la facilité d'accès et utilisent les mêmes mots de passe et questions secrètes sur tous les différents sites, sans compter la somme d'informations révélées sur les réseaux sociaux !

Des normes et de bonnes pratiques pourraient être partagées entre les différents acteurs à l'échelle internationale pour éviter que des informations puissent être recoupées trop facilement. La sensibilisation des clients sera également importante. Mais au final, une réflexion de fond doit être entamée pour améliorer la sécurité de l'authentification des clients et des initiatives autour de l'authentification forte déjà entamées doivent être poursuivies dans le futur pour réduire ces risques de fraudes.