Comment Boursorama Banque protège ses clients des fraudeurs

Face à la multiplication des tentatives de fraude touchant le secteur bancaire, Boursorama Banque a su s’armer pour protéger au mieux ses clients, tout en préservant l’expérience utilisateur.

Leader de la banque en ligne, Boursorama Banque a bâti son succès sur une offre bancaire complète et une stratégie tarifaire très compétitive. Avec plus de 4 millions de clients accédant à près de 1000 fonctionnalités en ligne, la lutte contre la fraude s'est imposée comme un chantier majeur.

La lutte contre la fraude s'est assortie de deux exigences supplémentaires : protéger la confidentialité des données et préserver une expérience client fluide. Pour participer à cette mission, Boursorama Banque a choisi IBM Security® Trusteer® solution.

Les clients de services bancaires en ligne sont de plus en plus exposés aux tentatives d'escroquerie. Les barrières de sécurité ont beau se renforcer avec des méthodes telles que l'authentification à double facteur, les méthodes des pirates se renouvellent

sans cesse. Le phishing représente plus de la moitié des cas : les clients reçoivent un email qui imite celui de leur établissement bancaire. Cet email pointe en fait vers un site internet frauduleux qui va subtiliser les accès des clients lorsqu'ils tentent de se connecter. Les pirates peuvent aussi passer des appels téléphoniques : ils utilisent des informations personnelles glanées sur internet afin d'étayer un discours convaincant et persuader les clients de dévoiler leurs codes d'accès ou d'effectuer des opérations qui ouvrent les portes de leurs comptes ou de leurs ordinateurs personnels aux pirates... Une étude publiée par l'Institut National de la Statistique et des Etudes Economiques (INSEE) fin 2021 indique ainsi que 35 % des internautes européens ont été exposés à du phishing et 30 % ont découvert un logiciel malveillant sur leur équipement d'accès à internet.

Boursorama Banque propose environ

1,000

fonctionnalités en ligne, qui doivent toutes être contrôlées

Les alertes basées sur l'identification d'appareils blacklistés représentent

97%

des fraudes avérées

Avec plus de quatre millions de clients, Boursorama Banque a donné la priorité à la lutte contre la fraude et la protection des intérêts de ses clients. C'est un enjeu qui impacte les opérations (équipe de gestion des fraudes),

les finances (coût des transactions frauduleuses non détectées) et l'image de l'entreprise auprès des clients et partenaires.

La mise en œuvre de dispositifs de lutte contre la fraude est un processus complexe : avec près de 1000 actions de gestion de compte accessibles en ligne chez Boursorama Banque, la surface de surveillance est très importante. Pour des raisons de confidentialité, Boursorama Banque ne permet pas à la solution anti-fraude d'accéder aux données personnelles des clients – l'analyse se fait donc sur des critères techniques ou comportementaux captés au moment des connexions. En outre, les délais doivent être très courts – à la fois pour ne pas gêner les clients qui consultent légitimement leurs comptes et pour contrer rapidement toute tentative de fraude !

"Beaucoup de solutions travaillent à partir du rapprochement des données via le prisme du client. IBM Security Trusteer travaille via le prisme des fraudeurs et de leur mode opératoire. Et cela se révèle très efficace."

Pierre Blanchier, RSSI, Boursorama Banque

Un modèle unique d'analyse des fraudes

Boursorama Banque a choisi IBM Security Trusteer, une solution permettant de détecter les fraudes tout au long du parcours client. Plus de 500 organisations de premier plan font confiance à IBM Security Trusteer pour sécuriser les accès de leurs clients.

La solution analyse chaque connexion aux services de Boursorama Banque afin de leur attribuer un indice de suspicion. Plus l'indice est haut, plus la connexion est susceptible d'être frauduleuse.

Pour cela, IBM Security Trusteer combine plusieurs types de données : des informations issues de bases de threat intelligence qui référencent les appareils de fraudeurs ou les services de hosting souvent utilisés par les pirates, les caractéristiques techniques de la connexion en cours

(hardware, système, navigateur…), le comportement lors de la connexion (vitesse de la souris, demande de réinitialisation du mot de passe, etc.) et beaucoup d'autres variables. En recoupant toutes ces données, la solution peut identifier des modes opératoires suspects et donc, faire remonter une alerte.

IBM Security Trusteer peut par exemple détecter la provenance d'une carte SIM. Lorsqu'elle est différente du pays de l'IP alors l'indice de confiance est dégradé. IBM Security Trusteer permet aussi de détecter les extensions suspectes installées sur les navigateurs, les applications de smartphones infectées par un code malicieux ou les systèmes jailbrakés plus exposés aux attaques.

«Il faut souligner que Boursorama Banque fait le choix de ne communiquer à IBM aucune information sur l'utilisateur, sa géolocalisation ou les données saisies – ceci pour garantir la confidentialité. IBM Security Trusteer sait s'en affranchir et c'est d'ailleurs un point différenciant par rapport à d'autres concurrents,» souligne Pierre Blanchier, RSSI de Boursorama Banque.

Boursorama Banque examine ensuite les alertes identifiées. C'est une cellule interne dédiée, basée en France, qui étudie plus précisément ces incidents, détermine si la fraude est avérée et prend les mesures qui s'imposent.

"Boursorama Banque ne communique aucune information sur l'utilisateur, sa géolocalisation ou les données saisies – ceci pour garantir la confidentialité. IBM Security Trusteer sait s'en affranchir"

Pierre Blanchier, RSSI, Boursorama Banque

Sauvegarde de l'expérience client

La réduction de la fraude est bien entendu le principal objectif de la solution. Mais pour Boursorama Banque, trois aspects clés lui permettent de se démarquer par rapport aux autres acteurs bancaires, soumis à la même pression des fraudeurs.

Réduction des «faux positifs»
Chaque alerte étant examinée par un collaborateur humain, la multiplication des faux positifs peut être très pénalisante en termes financiers et de ressources humaines. «Nous avons travaillé main dans la main avec IBM pour améliorer le taux de réussite et réduire significativement les faux positifs,» indique David Godat, DSI de Boursorama Banque. «De fait, nous savons que pour certains types d'alertes, nous avons un taux de fraude avérée qui peut monter jusqu'à 97%,» confirme Pierre Blanchier, RSSI de Boursorama Banque. Par ailleurs, les alertes qui bénéficient d'un haut degré de confiance ouvrent la voie à l'automatisation de leur traitement et « c'est un des chantiers des équipes de Boursorama Banque,» complète David Godat.

Anticipation
On entend souvent dire que les fraudeurs ont toujours un train d'avance. Solution utilisée par un grand nombre d'établissements bancaires, IBM Security Trusteer surveille des millions de sessions chaque jour dans le monde et mutualise les informations sur les modes opératoires des escrocs. De sorte que l'intégration rapide des nouvelles techniques et données dans les modèles de reconnaissance d'IBM Security Trusteer coupe l'herbe sous le pied des fraudeurs.

Sauvegarde de l'expérience client

En travaillant sur le mode opératoire, c'est-à-dire sur le comportement des fraudeurs au moment de la connexion, IBM Security Trusteer permet de raccourcir le délai d'identification et de réaction. L'escroc peut être identifié extrêmement rapidement, avant même qu'il ait pu aller au bout de sa fraude. La réaction immédiate de Boursorama Banque rend la tentative absolument indolore pour le client, à qui on évite le stress d'un compte bloqué ou l'attente de la régularisation d'une opération frauduleuse.

Boursorama Banque
La banque qu'on a envie de recommander.

Au sujet de Boursorama Banque

Boursorama Banque, filiale de Société Générale, est un acteur pionnier et leader sur ses trois activités principales : la banque en ligne, le courtage en ligne et l'information financière sur Internet. Boursorama Banqueoffre une large gamme de produits et services pour répondre aux besoins bancaires des clients : Banque au quotidien, crédits (immobilier, à la consommation, renouvelable), épargne de précaution, assurance-vie, bourse, assurances.

Composants de la solution

- IBM Security® Trusteer®