Kaspersky®
Fraud Prevention

Protection proactive contre la fraude en ligne et sur mobile

Kaspersky Fraud Prevention Cloud analyse l'ensemble de paramètres et d'actions à partir de tous les appareils de l'utilisateur utilisés pour accéder aux comptes.

Il prend des décisions en fonction de la réputation générale des appareils et des comptes dans la durée.

Il permet de détecter efficacement les fraudes complexes au niveau des comptes, mais aussi d'améliorer constamment la précision de la détection.

L'accroissement de la surface d'attaque et la nécessité d'une approche de prévention de la fraude multicanal axée sur les comptes

Les appareils des clients que vous ne contrôlez pas se trouvent au-delà de votre périmètre de sécurité et sont probablement insuffisamment protégés (voire pas du tout). Ils accèdent toutefois couramment à vos applications bancaires numériques sensibles et sont autorisés à effectuer plusieurs activités à haut risque. Puisque la plupart des utilisateurs se servent de divers canaux pour accéder aux applications bancaires, il devient difficile d'être sûr que votre établissement financier dispose de stratégies de protection adéquatement établies pour chacune d'entre elles.

En outre, les fraudeurs s'attaquent souvent à un canal afin de faciliter la fraude dans des canaux multiples (par exemple : attaquer des données d'identification bancaire plutôt faiblement sécurisées pour se connecter à une application de services bancaires en ligne afin de pirater le compte). Cela nous amène inévitablement à conclure qu'il est nécessaire de protéger le compte dans sa globalité, en plus de l'appareil et du canal individuel. Cette stratégie requiert une approche multicanal axée sur les comptes.

Kaspersky Fraud Prevention Cloud est capable de détecter les attaques ciblant les comptes d'utilisateurs ou les sessions bancaires, telles que :

- Piratage de compte
- Fraude via de nouveaux comptes
- Phishing / pharming
- Robots / carding / vérifications croisées
- Attaques à l'aide d'outils d'administration à distance
- Attaques dites de l'homme dans le navigateur

Kaspersky Fraud Prevention Cloud combine 4 technologies de prévention de la fraude dotées d'algorithmes de machine learning :

- **La détection de programmes malveillants sans client** vérifie si la machine du client est infectée par des programmes malveillants sans que l'utilisateur ait besoin d'installer de logiciel supplémentaire. Ces données sont utilisées pour l'authentification selon le risque, pour le modèle de machine learning et pour déterminer la légitimité des transactions.
- **Biométrie comportementale.** Elle analyse l'interaction du client unique avec son appareil (lorsqu'il déplace la souris, touche et balaye rapidement l'écran, par exemple) afin de détecter si l'appareil est entre les mains d'un utilisateur légitime ou non. Cette technologie détecte les robots et les outils d'administration à distance.
- **L'analyse comportementale** examine ce sur quoi l'utilisateur clique et la façon dont il agit pendant la connexion et la session. Elle s'intéresse également aux schémas de navigation et temporels, ainsi qu'à d'autres aspects. Cette analyse permet de construire des profils à comportement normal et de détecter tout comportement suspect ou anormal.
- **L'analyse de l'appareil et de l'environnement** profite de la présence mondiale de Kaspersky Lab pour identifier les « bons » appareils et utiliser ces connaissances pour authentifier l'utilisateur. En fonction de l'identification générale de l'appareil, de l'adresse IP et de la réputation de l'emplacement, tout attribut considéré comme une activité frauduleuse est également détecté de manière proactive et identifié comme suspect ou lié à la fraude.

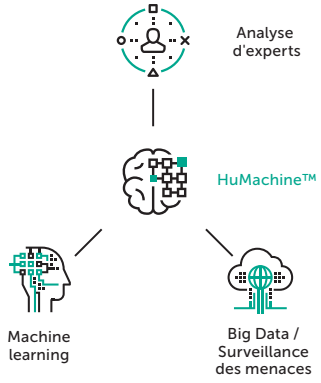
Les méthodes de machine learning, qui sont à la base du système, améliorent les technologies clés en activant des composants supplémentaires pour détecter la fraude :

L'authentification selon le risque permet d'accéder activement au niveau de risque lorsqu'un utilisateur se connecte au système. En fonction de cette évaluation et des diagnostics en temps réel de Kaspersky Fraud Prevention Cloud, votre organisation peut décider de la façon dont la transaction doit être traitée par la suite : permettre l'accès, demander une authentification supplémentaire ou restreindre les services disponibles. La détection des fraudes franchit un nouveau palier en réagissant en temps réel et en évitant les étapes d'authentification supplémentaires pour les clients légitimes.

La détection continue des anomalies de la session effectue une évaluation continue des risques de la session en fonction de l'analyse du comportement de l'utilisateur, de la réputation de l'appareil, des données biométriques et plus encore. Considérablement renforcés, les systèmes internes de surveillance des transactions peuvent détecter les menaces et automatiser plus rapidement, augmentant ainsi le taux de détection. Les transactions à risque peuvent faire l'objet d'une attention toute particulière et d'un traitement manuel, alors que les autres sont traitées automatiquement sans délai.

Kaspersky Fraud Prevention Cloud ne remplace pas votre solution de surveillance interne. Au lieu de cela, il la complète en fournissant à vos équipes de façon continue des données nécessaires pour détecter une activité frauduleuse en temps réel avant que la transaction n'ait lieu. Cela permet à vos systèmes actuels de bénéficier d'un contexte supplémentaire proactif pour prendre des décisions de façon plus précise et rapide, ainsi que de l'utilisation intelligente et adaptative de l'authentification à étapes.

Pour en savoir plus, contactez-nous sur : kfp@kaspersky.fr



Solutions de sécurité Kaspersky Lab pour les entreprises : **https://www.kaspersky.fr/enterprise-security**
Actualités des cybermenaces : **www.viruslist.fr**
Actualités de la sécurité informatique : **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.fr