API dans le paiement, à la recherche de l'équilibre entre ouverture et sécurité

Grégory Boulanger, Product Owner, Limonetik

Même si le terme est devenu très populaire, et encore plus particulièrement dans l'écosystème financier, les Application Programming Interface (API) ne sont pas nées de la dernière pluie. Véritable moteur de la FinTech, elles sont au coeur de la transformation numérique des acteurs du paiement. De fait, on accorde aujourd'hui plus d'importance aux API en raison de la criticité qui les entoure et de leur propension à permettre aux entreprises d'évoluer plus rapidement.

Les API gouvernent-elles le monde du paiement ?

L'idée d'une API est de faire communiquer entre elles deux applications tout en restant transparente pour les utilisateurs finaux. L'API est la possibilité pour deux logiciels d'interagir, d'échanger des informations.

Souvent comparées à des Lego, leur architecture de plus en plus construite en micro-services permet de créer de nouveaux usages mieux segmentés et donc plus simples à faire évoluer et à maintenir. Les API demandent un travail de réflexion et d'implémentation conséquent au démarrage mais qui apportera au fil du temps un réel gain à l'entreprise.

Dans le monde du paiement, les API se trouvent aujourd'hui au centre de toutes les attentions. Elles sont notamment la condition de ce qu'on appelle l'Open Banking. En effet, les banques, acteurs majeurs du monde du paiement, doivent désormais rendre accessibles les mouvements liés aux opérations effectuées sur les comptes de leurs clients.

Favorisées par l'entrée en vigueur de la directive européenne relative au paiement (DSP2), les API, en ouvrant les systèmes bancaires au monde extérieur, permettent d'offrir de nouveaux services tels que :

- accéder aux soldes et aux mouvements bancaires de manière centralisée,
- interroger la banque d'un client pour effectuer un règlement,
- permettre les virements instantanés.

Les API, un nouveau prisme stratégique

La DSP2 a transformé l'univers bancaire ; un monde devenu ouvert dans lequel la norme de communication est l'API. Celles-ci permettent de gagner du temps en termes de mise en marché d'une solution. Un projet qui auparavant pouvait durer plusieurs années pour passer en production peut être réduit désormais à quelques mois grâce à la norme d'API définie.

L'Open Banking, qui a émergé avec la DSP2, offre de nombreux avantages. C'est notamment la facilité pour un tiers à se connecter à une banque sans devoir développer *n*systèmes de connexion à *n*banques différentes. Grâce à la DSP2 il n'y a donc plus qu'un seul système normé qui permet d'accéder aux informations dans toutes ses banques partenaires. Un vrai gain de productivité et

d’efficacité pour les tiers.

Les API permettent d’accélérer toutes les modifications dans un monde interconnecté. En sus, la DSP2 contraint les établissements bancaires à ouvrir leurs systèmes d’information (SI). Les API sont le bras armé de la DSP2 qui vise à promouvoir le commerce et le paiement en ligne. En effet, la directive européenne apporte des solutions à l’évolution du monde du paiement notamment avec l’explosion des marketplaces et des services de suivi bancaire.

L’APIsation oui, mais pas sans unesécurité renforcée

Le sujet à suivre en 2019 sera inévitablement l’évolution des API du point de vue de la sécurité.

Les API étant la clé des échanges, elles sont en particulier soumises aux attaques des pirates du Web. Affronter la cybercriminalité galopante n’est pas simple. Il est primordial de trouver un équilibre entre un monde ouvert, empli d’API, et un monde de sécurité. Penser une *security by design*dans le monde du paiement est incontournable. Il serait trop risqué d’ouvrir une API sans avoir eu une réflexion amont sur la sécurité des architectures.

Comme nous l’avons dit, l’ouverture des API est un gain pour l’entreprise mais il faut maintenir des règles de sécurité strictes pour éviter le piratage et cela à tous les niveaux d’interaction. Il ne faut donc pas oublier, ni négliger, la sensibilisation des employés. Ceux-ci doivent suivre des formations spécifiques car, ne l’oublions pas, le maillon le plus faible de la cyber criminalité reste souvent l’être humain.

Au-delà des collaborateurs, l’entreprise doit prévoir un cryptage des données, des accès restreints, des changements réguliers d’informations de connexion, etc. Si aujourd’hui le Hacking touche de moins en moins la structure technique de plus en plus et de mieux en mieux protégée, les pirates peuvent détourner l’utilisation d’une API et avoir un impact négatif sur la chaine de sécurité de manière générale.

Ce qu’il faut retenir !

Pour conclure, toutes les sociétés doivent désormais ouvrir leurs SI pour proposer des services complémentaires de meilleure qualité et plus rapidement. Les établissements bancaires en première ligne avec la DSP2 ! Avec, dans la balance, le lourd enjeu de la sécurité que les entreprises doivent maitriser à tous les niveaux, il faut garder en tête la recherche d’un équilibre. Une réflexion profonde doit s’engager avant tout pour déterminer l’emplacement du curseur oscillant entre le coeur fonctionnel et la maitrise de la donnée mise à disposition.