Après les attaques, SWIFT révise un peu sa sécurité

Le réseau financier international, SWIFT, a indiqué qu'il allait « élargir » l'utilisation de l'authentification à double facteur lors des transferts de fonds entre les banques. Cette décision intervient après plusieurs affaires de « cyber braquages », liés à une faiblesse dans SWIFT.

La première victime a été la banque centrale du Banglasdesh qui a perdu 81 millions d'euros. Il y a eu également une banque équatorienne qui a vu s'évaporer 12 millions de dollars. Enfin des attaques similaires ont été interceptées contre une banque des Philippines et du Vietnam. Au total une douzaine de banques sont sous surveillance.

La réponse initiale de SWIFT a été de se dédouaner en expliquant que son réseau n'a pas été compromis et que les braquages sont la conséquence du piratage de systèmes d'autres banques. Cependant les experts en sécurité ont pointé du doigt les faiblesses importantes et une détection des menaces datant d'une décennie.

Une mise à niveau des politiques de sécurité de SWIFT

Mis en accusation, la direction de SWIFT est montée au créneau pour proposer un plan afin d'améliorer la sécurité. Ce plan comprend 5 points notamment, la société va « exiger » une plus grande remontée d'informations des clients, ainsi que le partage de ces informations avec d'autres clients. De même, son système de gestion des incidents sera plus réactif et émettre des « bonnes pratiques » en matière de cyberdéfense. La double authentification va donc être élargie et des outils complémentaires comme des logiciels de monitoring vont être mis à disposition des clients.

Sur la sécurité liée aux transferts et pour laquelle SWIFT est mis en porte à faux, la société va fournir « des règles d'audit » et proposer des éléments de comparaisons des niveaux de conformité des banques avec ses exigences basiques. Des efforts vont être également menés pour, par exemple, « *créer des outils pour permettre aux clients de rappeler rapidement des ordres de paiements frauduleux* ».

Les méchantes langues diront qu'il a fallu plusieurs cas de piratage pour que SWIFT adapte sa sécurité au monde moderne. D'autres expliquent que la société ne pouvait pas lutter face à une opération particulièrement bien ciblée. Plusieurs éditeurs de solutions de sécurité comme Symantec ou BAE Systems ont clairement relié les attaques SWIFT avec l'opération menée contre Sony Pictures.

A lire aussi :

Piratage de Swift : la faute à une mise à jour mal maîtrisée ?

Fraude sur Swift : plusieurs banques sont touchées