Le pouls de l'économie suisse – retrouvez les derniers chiffres économiques clés décryptés en graphiques

Voir l'inflation

Voir le commerce

Voir le PIB

Voir le chômage

Voir le tourisme

L'INVITÉ ABONNÉ

Les banques privées suisses, la confidentialité numérique et la nécessité d'un accès légal par l'Etat

Le scandale Crypto AG a montré que la confidentialité de la place bancaire suisse a pu être en danger. Les solutions de sécurité informatique purement logicielles ne peuvent pas offrir le même niveau de protection que les solutions matérielles, car une application ne peut jamais être plus sûre que l'appareil sur lequel elle fonctionne

Une grande majorité des piratages de confidentialité restent non découverts (car plus l'espionnage non découvert est long, plus il a de valeur pour l'agresseur) ou non signalés (car la victime et l'agresseur n'ont aucun intérêt à se faire connaître). — © shutterstock

Rufo Guerreschi, fondateur & CEO, TRUSTLESS.AI
Publié vendredi 11 décembre 2020 à 15:24
Modifié vendredi 11 décembre 2020 à 15:24

Rufo Guerreschi, fondateur & CEO, TRUSTLESS.AI. © DR

Le 25 novembre dernier, un reportage de l'émission *Rundschau* de la SRF a rendu public le fait qu'Omnisec AG, un grand fabricant suisse de systèmes de cryptage, était également contrôlé ou compromis par les services secrets américains et allemands. Nous avons aussi appris comment la confidentialité des systèmes informatiques utilisés par UBS, le plus grand gestionnaire de fortune du monde, a pu être affectée. *Rundschau* est le même média qui a codirigé le reportage sur Crypto AG et InfoGuard AG en février dernier.

Ce n'est pas une nouvelle ou une surprise pour les experts. Pourtant, jusqu'à aujourd'hui, peu d'articles de presse ont fait le lien entre le fait avéré que certaines grandes banques suisses ont été pendant des décennies clientes d'InfoGuard AG, jusqu'en 2018 une société sœur de Crypto AG. La plupart des médias n'ont pas exploré ce que ces informations signifiaient pour la confidentialité de la place bancaire suisse. En fait, peu d'informations étaient publiquement disponibles sur la nature et la portée de ces relations commerciales.

Bien que les banques aient pu ignorer l'existence de ce type d'espionnage étranger, elles ont indirectement bénéficié d'un service inestimable et sans équivalent de KYC (Know Your Customer ou connaissance du client), leur permettant d'éviter de s'engager avec les criminels les plus dangereux ou les Etats voyous. Cela était finalement bénéfique pour les banques, pour la Suisse et pour la paix et la sécurité dans le monde.

Solutions logicielles moins efficaces

Il y a deux ans, Omnisec AG a été fermée tandis que la propriété d'InfoGuard AG a été officiellement transférée à quelques cadres supérieurs de longue date de l'entreprise. En réponse à ces changements, certaines de ces banques semblent continuer à utiliser InfoGuard AG pour leurs communications les plus sensibles – et il reste à savoir si l'influence des nations étrangères a été maintenue – alors que d'autres ont partiellement ou totalement changé pour d'autres solutions basées sur des applications de messagerie ultra-sécurisées faites maison ou suisses, comme Threema – fonctionnant sur des appareils mobiles grand public sécurisés par des systèmes anti-malware avancés.

Ces solutions purement logicielles ne peuvent pas offrir le même niveau de protection que les solutions matérielles, car une application ne peut jamais être plus sûre que l'appareil sur lequel elle fonctionne. Ces solutions restent donc vulnérables non seulement aux nations puissantes – alliées ou non – mais aussi et surtout aux organisations criminelles avancées et aux nations moins puissantes.

On estime qu'une grande majorité des piratages de confidentialité restent non découverts (car plus l'espionnage non découvert est long, plus il a de valeur pour l'agresseur) ou non signalés (car la victime et l'agresseur n'ont aucun intérêt à se faire connaître). Néanmoins, ces nouvelles approches logicielles sont apparues publiquement dans le récent scandale d'espionnage interne à Credit Suisse. Ce scandale a généré des dommages considérables et irréversibles en termes d'image.

Contrôle démocratique approfondi

Paradoxalement, ces solutions logicielles empêchent parfois les services policiers d'accéder aux preuves en raison d'un cryptage fort, qui peut avoir été acquis auparavant par des criminels grâce à des logiciels malveillants fonctionnant sur l'appareil pendant leur utilisation, avec de graves risques de chantage ou pire.

Cette situation moins qu'idéale offre à ces banques la possibilité d'explorer de nouvelles voies pour parvenir à la plus grande confidentialité des communications internes et des communications avec les clients, tout en permettant l'application légitime de la loi au niveau international. Cette alternative pourrait être basée sur un contrôle démocratique approfondi et une transparence appliquée à la fois aux systèmes informatiques et aux mécanismes utilisés pour permettre un accès légal légitime.

Grâce à cette alternative, les banques privées suisses peuvent non seulement mieux protéger leur confidentialité et celle de leurs clients, tout en garantissant un accès légal international légitime, mais elles peuvent aussi devenir les fournisseurs de confiance numérique de leurs clients, en approfondissant leur relation de confiance, en augmentant le confort des clients, en offrant des services supplémentaires et en améliorant leurs relations publiques en temps de crise mondiale.

Lire aussi: Le scandale Crypto AG, une tache sur l'image de la Suisse