J. Krause, Telindus: ‘Le maillon faible de la banque, c’est le client’

Quelles sont les failles dans la sécurité des banques, face à la cyber-criminalité ? Le maillon faible de la banque, c’est le client. Pourquoi aller cyber-braquer le système informatique d’un établissement financier, forcement très défendu, alors qu’il existe tant de clients, et si vulnérables. Le souci majeur se situe au niveau de l’identification et l’authentification. Le client a de multiples activités sur son poste informatique : il ‘tchate’, télécharge tous types de fichiers, se balade sur n’importe quel site. Le tout, pour beaucoup, depuis un système d’exploitation Windows, qui présente en permanence une vingtaine de trous de sécurité. Le meilleur antivirus n’y change rien ! C’est pourquoi les chevaux de Troie représentent le risque essentiel, aujourd’hui, qui enregistrent les actions de l’internaute. Et les éditeurs d’antivirus ont du mal à les repérer. Le phising, plus médiatisé, reste maladroit dans ses réalisations. Quoi que, celui qui a attaqué le Crédit Lyonnais était plus sophistiqué. Quels sont les outils pour répondre à ces attaques ? Quelques banques ont déjà mis en place des systèmes d’authentification forte pour certains clients : des token, qui génèrent des mots de passe à le demande. Même si le cyber-criminel les enregistre, cela ne sert à rien, puisqu’il ne peut pas s’en resservir. Mais ce système reste trop coûteux pour être étendu à tous les clients. Autre outil, le clavier virtuel. Généré par la banque, il apparaît sur l’écran du client. L’internaute y tape son code secret, ainsi que la confirmation de certaines opérations sensibles, comme un virement. Mais attention ! Au Brésil, où cette solution existe depuis plus longtemps, les faux claviers ont déjà fait leur apparition. C’est une course sans fin. Les banques mènent-elles une véritable politique de sécurité ? De manière générale, les banques se montrent très préoccupées par le problème de sécurité. La banque en ligne représente un enjeu financier très important. Le secteur est donc mature, même si certains établissements sont plus avancés que d’autres. Par exemple, depuis 5 ans, je suis intégré dans l’équipe de sécurité d’un établissement. Lorsqu’il y a une plainte d’un client, nous investiguons pour comprendre ce qui s’est passé. Et les banques ont développé des outils pour tracer ce type de fraude et analyser les comportements des internautes. Celui qui se connecte dix ans depuis le Loir et Cher, puis, brusquement, depuis la Lituanie, mérite toute notre attention ! Mais, au-delà de l’investigation, nous mettons en place des systèmes de détection, ou nous émettons des messages de sensibilisation au risque auprès des clients. Il y a une démarche préventive.