

## Violation de données chez Barclays, une leçon pour tout le monde

### Sécurité

Posté par : JPilo

Publié le : 13/2/2014 11:00:00

Le journal britannique The Mail, dans son édition de dimanche dernier, a révélé que les informations personnelles et financières de près de 27 000 clients de la banque Barclays aurait été volées, ce qui constitue la pire violation de données subis par une banque britannique à ce jour.

La fuite a été mise au jour par un indicateur anonyme, qui a donné au journal anglais une clé USB contenant un échantillon des données disponibles sur 2 000 des clients de la banque tout en affirmant que ces informations faisaient l'objet de ventes sur le marché noir, à environ 50 \$ par dossier. À l'heure actuelle, les détails sur la façon dont la violation a pu être réalisée n'ont pas encore été révélés; toutefois, une enquête vient d'être ouverte par l'organisme chargé de la protection des données.

**Jean-Pierre Carlin**, Directeur Europe du Sud chez LogRhythm, se confie :



« Ce dernier vol de données est incroyable, et de sérieuses questions doivent être posées à la Barclays, non seulement en ce qui concerne la façon dont ce vol s'est déroulé, mais aussi sur le fait qu'il ait fallu un informateur anonyme pour que la banque soit avertie de la perte de ces données. Aujourd'hui, la sophistication des cyber-attaques n'est plus un secret et il est extrêmement inquiétant qu'une institution financière de haut niveau telle que la Barclays puisse en être victime. Si les entreprises ont encore besoin de preuves pour comprendre qu'il ne s'agit pas de savoir « si » elles seront victimes d'une violation de données, mais bien « quand » - car cela arrivera inéluctablement, cette attaque en est le parfait exemple.

Les détails sur la façon dont les données ont été exfiltrées n'ont pas encore été rendus publics, mais en réalité, que ce soit un acte malveillant interne ou une cyber-attaque très sophistiquée, la leçon à retenir est toujours la même : sans savoir exactement ce qui est passé sur le réseau à tout moment, et sans parvenir à comprendre ce qu'est l'activité "normale", les données peuvent être l'objet d'exfiltration, de manière totalement inaperçue. Cette nouvelle violation prouve que chaque entreprise doit déployer des systèmes de défense puissants et en temps réel sur leur réseau, afin d'être en mesure de repérer et de combattre les menaces dès qu'elles se produisent - pas une fois qu'il est trop tard ou que, par chance, quelqu'un lance l'alerte.

Il n'y a aucun doute que cette violation de données aura des conséquences profondes pour la banque Barclays, mais cela doit également servir de veile à toutes les autres organisations dans le pays. La clé absolue à la sécurité des données est une surveillance proactive. Non

*seulement cette stratégie peut empêcher une violation survenant en premier lieu mais, si une attaque est réussie, elle peut aussi l'identifier et la corriger beaucoup plus rapidement.*

*Il est également grand temps que le gouvernement accélère la mise en œuvre des lois obligatoires de divulgation de violations de données, afin d'inciter les organisations à mieux protéger les données de leurs clients. Aujourd'hui, il n'est pas admissible qu'un événement extérieur soit à l'origine de la découverte d'une violation ; au lieu de cela, les alarmes devraient d'abord sonner en interne - et fort. »*