80 millions de comptes de l'assureur Anthem compromis, la Chine visée

Le bilan est provisoire, mais il laisse entrevoir l'ampleur de la **cyber-attaque** dont **Anthem** a été victime : les données personnelles de plusieurs dizaines millions de personnes seraient tombées dans les mains de pirates informatiques.

Le deuxième assureur sur le marché américain évoque un assaut « ultra-sophistiqué » découvert par ses soins la semaine passée. Tout a commencé lorsqu'un administrateur s'est aperçu que ses identifiants avaient été usurpés pour lancer des requêtes dans une base de données, selon nos confrères d'ITespresso.

80 millions d'assurés potentiellement affectés

Sur le site web AnthemFacts, créé pour l'occasion, le CEO Joseph R. Swedish reconnaît que les victimes pourraient effectivement « se compter par dizaines de millions ». D'autant plus que le serveur piraté hébergeait non seulement des éléments renseignés par les **37,5 millions de clients revendiqués à fin 2014,** mais aussi des informations sur d'anciens souscripteurs. Si bien que **80 millions de personnes** pourraient finalement être concernées, d'après le *Wall Street Journal*.

Parmi les données exfiltrées figurent des noms, des dates de naissance, des numéros de téléphone et de Sécurité sociale, des adresses postales et électroniques, ainsi que des éléments relatifs à l'activité salariée des clients, comme le niveau de revenus.

Anthem (ex-WellPoint ; basé à Indianapolis) déclare n'avoir « aucune preuve » que des informations bancaires et médicales – en tête de liste, les résultats de diagnostics – aient été volées. L'assureur précise toutefois que son personnel est également concerné par ce hack.

La piste chinoise évoquée

La faille exploitée dans le cadre de cette attaque a été comblée. Une investigation coordonnée avec le FBI est en cours. La firme Mandiant (filiale de FireEye) a été sollicitée pour mener un audit du système d'information et recommander les solutions de protection *ad hoc*. Elle a d'ores et déjà confirmé que l'offensive était d'un « haut niveau de sophistication ». Selon une source interrogée par Reuters, **la piste chinoise est évoquée** avec des similitudes sur une attaque liée au domaine de la santé.

Pour compliquer la détection de leur méfait, les pirates ont stocké les données dérobées sur un service de stockage en ligne « communément utilisé par les entreprises aux Etats-Unis », d'après le FBI.

L'agence fédérale surveille tout particulièrement le secteur de la santé depuis la cyber-attaque qui avait entraîné, l'été dernier, la fuite de rapports médicaux sur 4,5 millions de patients pris en charge dans l'un des 135 hôpitaux que le Community Health Systems (CHS) gère à l'échelle de 29 Etats

américains.

Alors qu'il disposait – conformément à la loi – d'un délai de 60 jours pour avertir le public et les autorités, Anthem a choisi de communiquer rapidement. Un numéro gratuit est en place pour recevoir les demandes des clients. Tous ceux qui sont concernés seront avertis par voie postale « dans les prochaines semaines » et si possible par e-mail. Les mots de passe des employés disposant d'un accès à des bases de données critiques ont été réinitialisés et l'authentification forte, généralisée. A noter que **l'assureur a déjà été condamné à une amende de 1,7 millions de dollars pour le vol de données en 2010** de 612 000 personnes. Une paille par rapport aux 80 millions potentiellement compromis.

Le bilan de ce hack est du niveau de ceux de J.P Morgan (76 millions de foyers touchés), Home Depot (56 millions de cartes de paiement ; 53 millions d'adresses e-mail) et de Target (40 millions de cartes de paiement).

A lire aussi :

Vol de données : 2014, année de tous les records (infographie)

Adobe : le plus grand vol de données de tous les temps ?