OPM : un autre piratage de 21,5 millions de données

La note s'alourdit pour l'Office of Personnel Management (OPM). Au début du mois de juin, l'agence en charge de la gestion des agents du gouvernement fédéral annonçait avoir été victime d'une attaque informatique. Le butin des cybervoleurs était évalué par la perte de plus de 4 millions de données sur des fonctionnaires américains. Une lettre de David Cox, président de la Fédération des employés fédéraux américains (syndicat qui regroupe 670 000 employés fédéraux) à Katherine Archuleta, responsable de l'OPM apporte un éclairage sur cette opération. Parmi les informations récupérées par les cyberattaquants, il y a « *le numéro de sécurité sociale de chaque salarié, le dossier militaire, l'adresse, la date de naissance, l'historique de travail et de paie, l'assurance-santé, l'assurance-vie, les pensions, l'âge, le genre, statut marital et plus* ». Le syndicaliste constate avec effroi que les numéros de sécurité sociale ne sont pas chiffrés.

Puis le chiffre de 4 millions a été revu une première fois à la hausse pour atteindre 14 millions. Cette révision devra maintenant prendre en compte une seconde attaque menée cette fois-ci sur les données du personnel militaire et sur la communauté du renseignement. La grogne s'est amplifiée y compris jusqu'à la Chambre des représentants où certains membres ont directement été concernés par ce vol de données.

Des données très personnelles en fuite

Aujourd'hui, l'OPM indique qu'au total, 21,5 millions de données ont été dérobées dont 19,7 millions d'informations relatives à des personnes sollicitant un emploi dans la fonction publique y compris certains postes sensibles dans les agences militaires et de renseignement. Les 1,8 million de données restantes sont liées à la famille proche. Parmi l'ensemble de ces informations, l'OPM recense 1,1 million d'empreintes digitales.

Les cyberattaquants ont donc eu accès à des données sensibles et très personnelles. Les candidats à des postes dans l'armée ou dans les services de renseignements sont obligés de remplir des formulaires (dont le SF86) avec des questions très indiscrètes : consommation de drogue, infidélités, alcoolisme, addictions aux jeux, dettes, surendettement, troubles maritaux, activités criminelles ou délictueuses.

On se doute de l'intérêt de tels renseignements pour une puissance étrangère. Dès la première attaque, la Chine a été visée comme étant à l'origine des intrusions. Pour la seconde attaque, le même pays est dans le collimateur du gouvernement américain. Cette affaire a montré les faiblesses de la sécurité IT des différentes agences et ministères américains.

A lire aussi :

La Chine accusée du vol de 4 millions de données de fonctionnaires US

Un accord à double tranchant pour Cisco en Chine ?

GlebStock-Shutterstock