Le service en ligne PayMaxx vulnérable

La société PayMaxx offre au travers de son portail ASP (Application Service Provider), un ensemble de services de ressources humaines dédié aux entreprises qui souhaitent externaliser ce type de prestations. Ainsi les employés des sociétés clientes de PayMaxx peuvent très simplement consulter leurs bulletins de salaires, demander le virement de leurs soldes, gérer leurs cotisations de sécurité sociale ou leurs déclarations de revenus.

Il y a une quinzaine de jour, une faille de sécurité permettant de récupérer les formulaires de déclaration de revenus de l'ensemble des utilisateurs du service PayMaxx a été révélée. La vulnérabilité aurait exposé les numéros de sécurité sociale et bulletins salaires de plus de 25.000 individus. *« Il n'y a pas de système qui soit 100% sûr contre un pirate déterminé »*, affirme l'un des porte-parole de PayMaxx. *« PayMaxx a par le passé, et continue jour après jour de s'efforcer à sécuriser ses systèmes contre tout type de faille »*. Selon l'acte SB1386, la société PayMaxx est dans l'obligation d'avertir par lettre recommandée l'ensemble de ses clients basés en Californie. A ce jour aucun des clients n'aurait reçu l'information… **Une faille si simple à exploiter…** Aux États-Unis, l'impôt sur le revenu est prélevé à la source à partir d'une estimation globale du revenu annuel. Une déclaration de revenus est néanmoins nécessaire une fois l'année écoulée de façon à ajuster le différentiel au besoin. La déclaration est basée sur un formulaire, appelé W2 qui affiche le montant du salaire perçu ainsi que les impôts déjà versés l'année passée. Ce formulaire est généralement délivré par l'employeur en février, sachant que la déclaration doit être effectuée pour le 15 avril. Pour identifier l'employé, le formulaire W2 se base sur un identifiant unique à chaque individu : son numéro de sécurité sociale. L'un des clients du service PayMaxx, Aaron Greenspan, est le fondateur de Think Computer, une société de services en sécurité informatique. Après avoir été averti par son service de ressources humaines que son formulaire W2 était disponible, Aaron s'authentifie sur le portail PayMaxx et récupère son formulaire au travers d'un document PDF imprimable. Aaron fut surpris de constater que l'adresse du document pointait vers un fichier stocké dans un répertoire nommé « 2004 » et que le nom du document était un simple identifiant numérique. En bon « bidouilleur », Aaron tente tout d'abord d'incrémenter ce numéro, ce qui lui a permis de récupérer le formulaire d'un inconnu ! En reproduisant l'opération, Aaron a pu démontrer que plus de 25.000 formulaires W2 étaient accessibles à tout individu préalablement authentifié. Une recherche plus poussée a également démontré la présence du login « 000-00-000 » combiné au mot de passe « 000000 ». De plus, les mêmes documents seraient disponibles pour les années passées en modifiant simplement le nom du répertoire. A l'issu de sa découverte, Greenspan a bien évidemment contacté par e-mail les équipes techniques de PayMaxx et a par ailleurs offert ses services pour les aider à résoudre le problème. Après 15 jours de silence, la faille est toujours là et Greenspan a publié un papier qui expose les détails du problème. En France, les risques liés à la divulgation du numéro de sécurité sociale restent limités mais aux États-Unis, toute la vie d'un individu est basée sur ce précieux sésame. C'est sans doute l'information la plus sensible pour un américain… Si vous souhaitez effectuer une opération bancaire, modifier les services de votre abonnement d'électricité, de votre téléphone mobile, ou tout autre service dont vous êtes abonné, on vous demandera toujours les 4 derniers chiffres de votre numéro de sécurité sociale. (*) **pour Vulnerabilite.com**