Des comptes mails d'ambassades pas si confidentiels sur Internet

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 3 septembre 2007

Un consultant freelance en sécurité a découvert la faille qui concerne plusieurs représentations diplomatiques dans le monde.

Des données permettant de se connecter à plus d'une centaine de boites mails de personnels des ambassades et agences gouvernementales à l'international ont été publiées en ligne. Ces données - dont les noms d'utilisateurs, mots de passe et adresses des serveurs - ont été transmises par Dan Egerstad, un consultant freelance en sécurité.

Parmi les administrations concernées figurent les ambassades du Kazakhstan aux Etats-Unis et en Russie, ainsi que l'ambassade d'Inde aux Etats-Unis et l'ambassade de Russie en Suède. Ont également été publiées les données d'accès aux comptes mails des employés du bureau britannique délivrant les visas au Népal, ainsi que celles du ministère des affaires étrangères d'Iran et des quarante ambassades ouzbèques réparties dans le monde.

"J'ai fais un test et je suis tombé sur les données par accident", a indiqué Dan Egerstad à Computer Sweden. Il affirme ne pas avoir essayé de consulter les comptes mails en question pour ne pas enfreindre la loi. Il a toutefois justifié sa décision de publier les informations en ligne sans en avertir au préalable les institutions concernées.

"Habituellement, lorsque vous découvrez quelque chose comme cela, vous contactez les personnes concernées pour leur demander de résoudre le problème. Mais dans le cas présent, il était trop compliqué de contacter tous les pays étrangers affectés", a-t-il indiqué. Avant d'ajouter qu'il espère que "cela les fera réagir. Avec un peu de chance un peu plus vite qu'auparavant ".

De son coté, Graham Cluley, consultant senior chez Sophos, considère que cette découverte est très gênante pour les gouvernements et les ambassades impliquées. "Il est difficile de savoir pour l'instant comment ces fuites se sont produites mais il est assez probable qu'il y a eu une erreur humaine ", d'après lui. Les erreurs les plus fréquentes étant le choix de mots de passe "faciles" à découvrir, l'usage des mêmes mots de passe pour toute sorte de sites Web ou le fait de ne pas changer régulièrement de mot de passe.

Traduction d'un article de Vnunet.com en date du 31 août 2007

Post-scriptum :

http://www.vnunet.fr/fr/vnunet/news...