La formation du personnel, seule vraie solution contre les attaques informatiques

3

	La formation du personnel, seule vraie solution contre les attaques informatiques

Publié quelques jours après la révélation d'une cyberattaque qui a touché plus de 100 banques à travers le monde et causé aux alentours de 900 millions d'euros de dégâts, le nouveau rapport d'Intel Security démontre toute l'importance d'une prise de conscience collective et souligne la nécessité d'éduquer les collaborateurs aux méthodes de persuasion utilisées par les hackers.

Dans ce fameux cyber-casse dont l'existence a été révélée la semaine dernière, ce sont des attaques de phishing ciblées qui ont permis de créer des brèches au sein des réseaux bancaires, démontrant ainsi la faiblesse intrinsèque du "pare-feu humain". Ce que confirme l'étude Threat Report d'Intel Security qui indique que 92 % des employés français ne sont pas en mesure d'identifier un courriel de phishing sur sept."Aujourd'hui, les cybercriminels n'ont pas nécessairement besoin de savoir-faire technique pour atteindre leurs objectifs, explique Paul Gillen, directeur des opérations du Centre Européen de lutte contre la cybercriminalité.
Certains logiciels malveillants peuvent infecter les ordinateurs en y accédant directement par emails. Ces attaques ciblées manipulent les victimes et les incitent à ouvrir des pièces jointes, prétendument légitimes, ou à cliquer sur un lien qui semble provenir d'une source sûre".
Sur l'année 2014, McAfee Labs a constaté une augmentation spectaculaire du nombre d'URL malveillantes soit plus de 30 millions de liens suspects. Une hausse qui peut être attribuée à la fois à une forte croissance du nombre de liens de phishing, ainsi qu'à une utilisation plus commune des URL courts qui cachent, souvent, des sites Web malveillants. Le rapport des 500 chercheurs du McAfee Labs pointe par ailleurs du doigt le fait que deux tiers des emails mondiaux sont des spams qui visent à soutirer des informations et de l'argent à leurs destinataires.
Il est donc important que les consommateurs et les collaborateurs d'entreprises soient informés des techniques d'escroquerie couramment utilisées dans le monde numérique.
"Pour conserver une longueur d'avance sur les cybercriminels et réduire le risque d'être l'une des victimes de la cybercriminalité, les entreprises doivent non seulement optimiser leurs processus et compter sur la technologie mais aussi former leurs personnels pour pallier à la brèche dans ce qu'on nomme 'l'OS humain'" conclut Raj Samani, Directeur Technique EMEA d'Intel Security.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Vous souhaitez participer à une de nos formations ?
Besoin d'informations complémentaires ?
Contactez-nous

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel, Nous sommes en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.infodsi.com/articles/154213/formation-personnel-seul-vrai-rempart-attaques-informatiques.html