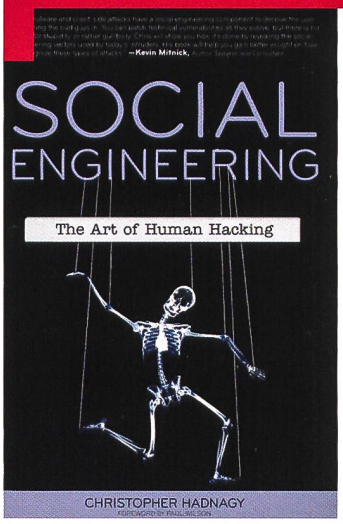
Ingénierie Sociale : Interview avec Christopher Hadnagy



Cyber

Ingénierie Sociale : Interview avec Christopher Hadnagy

Christopher Hadnagy
Consultant en sécurité, auteur et ingénieur social professionnel

Christopher Hadnagy a plus de 16 ans d'expérience en tant que praticien et chercheur dans la sécurité informatique. Ses efforts en matière de formation, d'éducation et de sensibilisation ont contribué à exposer l'ingénierie sociale comme étant la principale menace à laquelle les organisations sont aujourd'hui confrontées.

Auteur et conférencier convoité, Chris a participé à des conférences telles que la « RSA » ou encore la « *Black Hat.* » Il a également effectué diverses présentations pour des multinationales ainsi que des gouvernements.

Il est l'auteur de deux *best-seller* : « *Social Engineering : The Art of Human Hacking* » *and* « *Unmasking the Social Engineer : The Human Element of Security* .»

Qu'est-ce l'ingénierie sociale et en quoi cela consiste-t-il ?

Je définis l'ingénierie sociale comme tout acte qui influence une personne à prendre une action qui est ou n'est pas dans son intérêt.
J'en donne une définition assez large car je ne crois pas qu'il s'agisse toujours de quelque chose de négatif.
Nous utilisons les compétences d'ingénierie sociale lorsque nous communiquons tous les jours. Mais ces mêmes compétences seront utilisées par des personnes malintentionnées pour nous amener à faire des choses que nous ne devrions pas.

L'ingénierie sociale fait un peu penser à un art obscur. Pourtant, comme vous venez de le dire, beaucoup d'aspects liés à l'ingénierie sociale peuvent être trouvés dans la vie quotidienne. Comment se fait-il que nous avons commencé à en entendre parler seulement ces dernières années ?

Vous avez raison. L'ingénierie sociale existe depuis le début de l'humanité. Nous en entendons parler que depuis peu car les medias en parlent de plus en plus comme un vecteur d'attaque particulièrement viable.
Au début des années 1990 Kevin Mitnick a été arrêté pour avoir utilisé l'ingénierie sociale afin de pirater de nombreuses grandes entreprises de téléphone ainsi qu'échapper au FBI.
Depuis, ce vecteur d'attaque a de plus en plus été mentionné au cours des dernières années et mon travail l'a porté au devant de la scène afin que beaucoup puisse s'éduquer en conséquence.

Vous disiez avant que vous ne croyez pas que l'ingénierie sociale soit toujours quelques chose de négatif...

Non, ce n'est pas toujours négatif. Les mêmes techniques d'influence, le renforcement des liens et la confiance sont des choses qui sont utilisées par nos enfants, ou lorsque nous communiquons avec notre patron, notre thérapeute, le clergé, et bien d'autres.
Mais lorsque vous analysez ces communications elles sont similaires à celles appliquées par les arnaqueurs, escrocs ou ingénieurs sociaux afin de nous amener à prendre des décisions que nous ne devrions pas prendre. Ainsi, bien que ce ne soit pas toujours négatif, lorsque nous nous concentrons sur elles dans les médias ou dans les livres, nous parlons généralement des parties négatives de l'ingénierie sociale en raison de la façon dont elles sont utilisées pour pénétrer dans les entreprises.

En regardant votre site www.social-engineer.com il semble que la seule façon de prévenir les aspects négatifs de l'ingénierie sociale soit l'éducation. Appelons un chat un chat : diriez-vous que la majorité des gens est essentiellement ignorante à cet égard ?

Il est vrai que la plupart des gens sont ignorants vis-à-vis de l'apprentissage nécessaire pour se protéger de

l'ingénierie sociale. Ce n'est pas une question de stupidité mais d'éducation. Une fois instruit sur les aspects de ces attaques, il est ensuite plus facile de les repérer et de s'en protéger.

Et quelle a été votre expérience professionnelle en ce qui concerne, non pas le citoyen moyen, mais le professionnel de la sécurité (informatique)? Est-il bien informé?

*L'informaticien moyen dépense beaucoup de temps et d'énergie dans le matériel comme les pare-feu, les programmes anti-virus, les systèmes de détection d'intrusion; mais il ne passe pas beaucoup de temps à se former ou former son équipe aux techniques d'hameçonnage (*phishing*), d'hameçonnage vocal (*vishing*) ou d'usurpation d'identité pouvant mener à une pénétration de ses systèmes. Beaucoup d'informaticiens savent ce que ces choses sont, mais ils ne sont pas conscients comment se mettre soit-même ou leur entreprise en sécurité.*

Quelle est l'importance de l'ingénierie sociale dans les tests de pénétration? Pourriez-vous donner un pourcentage, cela varie-t-il au cas par cas?

Il est difficile de mettre un pourcentage mais en analysant les principales attaques au cours de la dernière année (NdlR: 2014), vous pouvez facilement voir que plus de 60% d'entre elles impliquent de l'ingénierie sociale à un moment ou un autre.
Il est très important que les entreprises permettent l'utilisation des tactiques d'ingénierie sociale lors des tests car elle est une réalité. Limiter l'utilisation de celle-ci ne fait que réduire la capacité des entreprises à se mettre réellement en sécurité.

C. H.

Christopher Hadnagy, «*Social Engineering: The Art of Human Hacking*», Wiley, 2010.

Propos receuillis par Yves Garcia.

New

Promotions au sein de la FOAP av 31

En l'église de Belfaux, le 30 janvier dernier, la FOAP av 31 a conduit la promotion de 47 aspirants: 11 lieutenants, 2 sergent-major chef, 1 fourrier et 33 sergents. La cérémonie fut agrémentée par les prestations des *Bag Pipers* de Wangen an der Aare ainsi que par une salve d'honneur du noble contingent des Grenadiers du canton de Fribourg. Le brigadier Peter Soller, commandant de la FOAP, a rappelé aux aspirants fraîchement promus une citation de Gandhi: «*L'histoire apprend aux hommes que l'homme n'apprend rien de l'histoire.*»

En effet: Guinée, Moyen-Orient, attentats de Paris ou autres catastrophes comme Fukushima sont déjà oubliés alors même que ces événements mettent en exergue la fragilité de nos sociétés modernes. Une situation qui se marie bien avec la devise de la FOAP av 31, «PA CAPONA» soit ne pas capituler et demeurer attentifs et prêts à faire face à chaque situation. L'invité du commandant, Monsieur Pierre Schuwey, commandant de la Police cantonale de Fribourg, a, quant à lui, adresser un mot aux familles pour les remercier du soutien amenés à ces nouveaux cadres dans l'accomplissement de leur mission. Par son discours, il a également défini le terme de cadres par «quelqu'un sur qui l'on peut compter,» des paroles pleines de sens dans notre époque moderne où tout change rapidement, y compris les goûts et les intérêts de tout un chacun.

J. G.