

CONTRIBUER A LA
SECURITE DE
L'ENTREPRISE EN SE
FORMANT

Une formation régulière est l'un des meilleurs moyens de se tenir informé des dernières techniques pour gérer efficacement une infrastructure IT et les risques qui s'y rapportent.

ET EN FORMANT LES
UTILISATEURS

Mais il est tout aussi important de prendre en compte le facteur humain si l'on veut éviter de gros soucis de sécurité.

Sans une sensibilisation régulière des utilisateurs, il est illusoire d'attendre de leur part un abandon des pratiques à risque

AVEC NAVIXIA

S'appuyant sur la grande expérience du terrain de ses ingénieurs, Navixia propose une gamme de cours de formation destinés à divers niveaux de compétences dans le domaine de la sécurité.

Cours de formation spécialisés en sécurité de l'information



I Cours de sensibilisation

Navixia recommande de mettre l'utilisateur au centre de la stratégie sécurité de l'entreprise, non seulement en informant régulièrement de ce qui est permis ou interdit à l'utilisateur du système d'information de la société, mais aussi en le sensibilisant aux risques liés à une utilisation inadéquate des systèmes informatiques et de communications.

Public visé

Tout utilisateur du système d'information de la société.

Aucune connaissance préalable n'est requise.

Durée et programme d'une séance

Le workshop de 2 à 3 heures se déroule dans votre entreprise. Il comporte une présentation théorique ponctuée par des démonstrations d'attaques servant à illustrer les dangers encourus. Une séance type est structurée comme suit:

- Introduction présentant les objectifs, les tendances et les différents facteurs de la sécurité du système d'information
- Traitement de thèmes tels que: gestion des mots de passe, risques liés au virus, risques liés à l'utilisation de la messagerie (e-mail, webmail, instant messaging, etc), utilisation d'internet, sécurité du poste de travail, responsabilité de l'utilisateur, ingénierie sociale.
- Questions, réponses

Pré-requis pour l'organisateur ou "sponsor interne" des séances

L'introduction des séances de sensibilisation à la sécurité du système d'information devrait être faite par un membre de la direction afin de convaincre les participants de l'implication des dirigeants dans cette démarche importante.

Une phase préparatoire est nécessaire afin de procéder à l'état des lieux, adapter le contenu au public ciblé et discuter avec vous quel est le message que vous souhaitez faire passer aux utilisateurs lors de cette séance de sensibilisation.

Remarque importante

Le cours est entièrement adapté aux besoins propres de votre société. De même, les démonstrations de vulnérabilités sont ajustées en fonction du niveau technique et des intérêts de l'audience.

CE QUE DISENT
D'ANCIENS
PARTICIPANTS

« This is seriously the most interesting course I have been to for a long time. »

« Focus on practice, good instructor, cool topics.”
"Amazing and excellent!! Great teaching. »

« I liked the way the course is delivered, in an interactive and challenging way. »

« Combat Edition est à conseiller à tous ceux qui pensent être bons dans le domaine de la sécurité informatique. Ce cours rend modeste ;-) »

« The performance of the instructor is excellent. He's willing to share his craft and is very successful in communicating his ideas. »

II Cours HBN – Sécurisation du réseau



© Sina Parov - Fotolia.com

La palette des cours HBN permet d'améliorer la sécurité de votre système d'information en vous montrant ses faiblesses potentielles ainsi que les motivations des agresseurs et les outils dont ils disposent pour essayer de pénétrer au cœur de vos systèmes. Chacun des cours - organisés avec le soutien de notre partenaire à la réputation mondiale, SensePost - vous donne les outils vous permettant de mieux vous défendre et assurer la sécurité de vos affaires.

Tous les cours HBN se donnent en anglais. Nos tarifs comprennent l'équipement, la documentation de cours, les repas de midi avec boissons et les pauses-café. Vous recevez un certificat de participation.

Bootcamp Edition

Lu-me 24-26 septembre 2012 (3 jours)

Introduction à la protection du système d'information
Cours d'introduction destiné à ceux qui n'ont pas encore une expérience approfondie des risques du piratage informatique sur le terrain.

Des faits réels, de la théorie et beaucoup d'exercices pratiques. Ce cours explique le détail des méthodes d'attaques des agresseurs aujourd'hui pour vous apprendre à mieux vous en protéger. Des experts vous feront assister à la déstabilisation complète de l'informatique d'une société, en vous expliquant les outils et technologies utilisés, mais plus particulièrement la manière de penser, la stratégie et la démarche des agresseurs durant chaque étape du processus.

Combat Edition

Je-ve 27-28 septembre 2012 (2 jours)

Destiné aux experts possédant une maîtrise approfondie des processus d'attaque et de défense des réseaux.

Portant sur le détail des méthodes d'attaque, ce cours, seul de son espèce au monde à un tel niveau d'expertise, est d'une grande technicité. Il combine la théorie à une pratique intense. Dès la première minute, vous êtes confronté à différents scénarios d'attaque bien réels dans un environnement complexe et vous êtes pressé par le temps pour relever le défi.

Lors de chaque exercice, l'instructeur discute des attaques, des alternatives et des défenses possibles pour le scénario en question. Les exercices présentent de nombreuses sortes d'attaques, de la plus simple à la plus complexe, pour vous apprendre à y résister.

CE QUE DISENT
D'ANCIENS
PARTICIPANTS

« Impressionnant, en tant que développeur on ne se rend pas compte de l'étendue des risques. Ce cours permet de prendre conscience des dangers. »

« If 10 is the best rate, I'd say 9.5 (just so as not to be too nice ;-) »

« I liked the demos most. They were very impressive. »

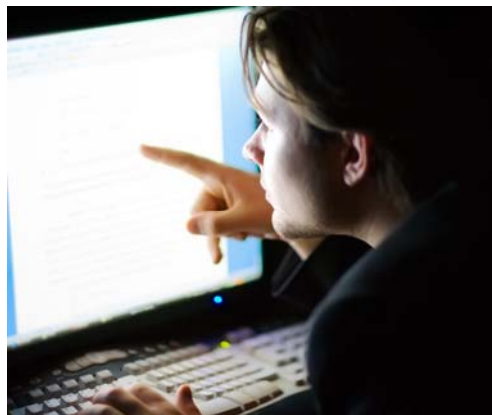
« Very interesting course. A lot of domains have been talked about, and exercises. »

« Excellent content and trainer. »

« This course opened my mind to application security issues. »

« Very interesting, instructor makes it interesting with real examples, simple examples, not only theory. Great training! »

Cours HBN – Sécurisation du réseau (suite)



© Steve Pienov - Fotolia.com

La prise de conscience des risques touchant à la sécurité du système d'information concerne tous les échelons de l'entreprise. C'est pourquoi la palette des cours HBN comporte un cours destiné aux développeurs et un autre destiné aux décideurs sans formation technique.

Chacun des cours - organisés avec le soutien de notre partenaire à la réputation mondiale, SensePost - vous donne les outils vous permettant de mieux vous défendre et assurer la sécurité de vos affaires.

Tous les cours HBN se donnent en anglais. Nos tarifs comprennent l'équipement, la documentation de cours, les repas de midi avec boissons et les pauses-café. Vous recevez un certificat de participation.

Developer Edition

Sur demande (2 jours)

Destiné aux développeurs souhaitant améliorer le niveau de sécurité de leurs applications

Les applications web écrites en Java, Perl, ASP, etc. représentent une cible tentante et facile pour les attaques. Beaucoup d'applications web étant connectées à des systèmes-clé de l'entreprise, une attaque peut avoir de très sérieuses conséquences.

Ce cours vous fait connaître les techniques d'attaques en usage et se focalise sur les questions: "Qui est mon adversaire?" et "Comment puis-je protéger mes applications contre les attaques?".

Des applications sont passées en revue pour découvrir les bugs cachés dans le code. Des exercices pratiques vous permettent de tester l'impact des faiblesses potentielles du code. Ce cours n'est pas basé sur un langage de programmation particulier. Il vise à donner aux développeurs une approche orientée vers la sécurité plutôt que du code tout fait, et il sera donc utile à tout développeur qui programme pour le web.

Cadet

Sur demande (2 jours)

Destiné aux débutants. Le B.A.-BA du hacking pour les collaborateurs techniques sans aucune notion préalable du domaine. Il s'agit d'une plate-forme de base pour toutes les autres formations HBN.

Le cours enseigne à voir le monde dans la perspective du hacker – une approche indispensable pour bien appréhender les risques et les prévenir efficacement – et donne les outils techniques de base nécessaires pour explorer cet univers.

Au travers de théorie et de beaucoup d'exercices pratiques, le cours fournit une méthodologie de travail de base ainsi qu'un panorama de l'environnement technologique du hacker, de ses outils et méthodes actuelles, y compris un peu de codage et de scripting,

Même destiné aux débutants, ce cours est néanmoins très technique. Il est indispensable pour les participants d'avoir une solide connaissance pratique des systèmes d'exploitation, des réseaux et des bases de données.