



DOSSIER ETHICAL HACKING EN COLLABORATION AVEC NAVIXIA

Une démarche logique

> **Page 28**
Se former au véritable
«ethical hacking»

> **Page 30**
Claude Krähenbühl, Navixia:
«Quelqu'un qui s'assure tous les jours
que les portes sont bien fermées»

Malgré la recrudescence des attaques informatiques et l'augmentation des risques de vol de données ou d'instabilité des systèmes, peu d'entreprises forment leurs collaborateurs aux techniques des hackers. Une étude récente montre cependant que les sociétés qui font appel au ethical hacking améliorent leur posture de sécurité et détectent un plus grand nombre de vulnérabilités – de quoi briser le tabou.

Qu'il s'agisse d'engager des entreprises spécialisées pour tester la vulnérabilité des systèmes ou d'initier des employés aux techniques des hackers, l'idée du ethical hacking consiste à se glisser dans la peau de l'adversaire pour mieux se défendre, de pratiquer l'empathie et non la sympathie.

Une enquête sur le sujet effectuée début 2009 par BT révèle nombre de détails intéressants sur les motivations des entreprises à cet égard. D'abord, entre 14 et 21 % des en-

treprises ne pratiquent pas du tout de ethical hacking. Ensuite, si plus de la moitié des sociétés ne font pas elles-mêmes de tests de hacking, c'est parce qu'elles ne disposent pas de collaborateurs formés à cet effet. Mais elles ne souhaitent pas non plus confier ces tests à des sociétés tierces, car cela coûte cher et elles craignent de miner la confiance de l'équipe informatique de l'entreprise.

Quant aux bénéfices du ethical hacking, les entreprises citent l'amélioration générale de leur posture de sécurité, la protection de leur propriété intellectuelle, la conformité avec les réglementations et la protection contre des plaintes pénales.

Dès lors, la démarche consistant à former des collaborateurs au ethical hacking semble un aboutissement logique: elle apporte une sécurité accrue à moindre coût tout en augmentant l'attrait du travail de l'équipe IT.

Se former au véritable «ethical hacking»

Tout réseau d'entreprise peut subir des attaques s'il est ouvert sur l'extérieur. Comprendre ce qui attire les cybercriminels permet à l'entreprise de renforcer son réseau de l'intérieur et de prévenir les visites indésirables. Cette démarche s'apprend. Encore s'agit-il de choisir la bonne approche! *Evelyne Pintado*

Se mettre dans la peau du hacker, comprendre sa motivation, ses méthodes d'action et les outils dont il dispose pour être ensuite à même de mieux le contrer: c'est ce qui se cache derrière le concept d'ethical hacking ou piratage éthique. Le mouton enfle une peau de loup! Des cours existent pour former les responsables de la sécurité ou de l'informatique à ces techniques. Mais tordons tout de suite le cou aux idées reçues, car on entend tout et n'importe quoi à propos du ethical hacking: il ne s'agit pas ici de guetter les sites louches à l'affût des derniers outils peu recommandables ou de fraterniser avec la pègre du web. Se former au ethical hacking c'est se confronter à une méthodologie extrêmement rigoureuse permettant de comprendre à la fois le fonctionnement de son propre réseau et la démarche du hacker qui cherche à s'y introduire.

De la fausse alerte à la vraie attaque

Comment en vient-on à suivre de telles formations? Souvent après avoir vécu une tentative d'attaque sur le réseau d'entreprise.

Exemple relativement fréquent, une société constate des problèmes de connectivité récurrents dans la partie publique de son réseau. Ces incidents sont signalés par



les systèmes de sécurité, mais le service IT ne parvient pas à en identifier l'origine. Il finit par penser qu'il s'agit d'un problème d'ordre technique et fait alors appel à un spécialiste externe en sécurité informatique pour tenter de comprendre la nature du problème.

Le spécialiste est alerté par la découverte d'un trafic régulier issu de plusieurs systèmes d'un même réseau. Il constate aussi que le firewall et les sondes de détection d'intrusions de l'entreprise renvoient depuis quelques temps de multiples alertes. Comme c'est souvent le cas, le département IT n'a pas pris ces informations en compte car il a reçu tant de fausses alertes par le passé qu'il n'y consacre plus l'attention nécessaire.

Le spécialiste montre qu'il s'agit d'une attaque générique qui, lors des pics de trafic, rend les systèmes instables avec pour conséquence de nombreuses pertes de connexion. Il résout le problème en modifiant la configuration de l'architecture de sécurité: les applications se stabilisent.

Après une telle attaque, il est fréquent que l'équipe IT de l'entreprise souhaite en savoir plus afin de mieux anticiper et gérer de tels incidents dans le futur. L'expérience montre toutefois que l'ethical hacking est un sujet complexe où il est très difficile de se former seul. Celui qui lit en solitaire des ouvrages spécialisés, sans l'aide d'explications complémentaires ou d'exemples concrets, trouvera rapidement la matière parfaitement indigeste. C'est là que les cours de ethical hacking prennent tout leur sens. Encore faut-il choisir le bon, car là aussi on trouve de tout sur le marché.

Savoir choisir son cours

Il faut d'abord choisir un cours d'ethical hacking basé sur une mise en situation concrète des participants avec de la pratique à haute dose. Certaines approches sont ludiques et très stimulantes: les participants sont appelés à relever des défis de plus en plus difficiles pour contrer un hacker fictif dans un temps limité. Mais la condition de base pour que le cours soit bon, c'est que l'instructeur soit un

spécialiste du terrain confronté quotidiennement aux situations qu'il démontre. Dans sa vie professionnelle, l'instructeur idéal sera par exemple un spécialiste de l'audit de sécurité, confronté tous les jours aux attaques les plus diverses. Les formations dispensées par des «donneurs de cours» professionnels, dont les connaissances sont surtout théoriques, n'auront jamais le même niveau de pertinence: il est illusoire d'attendre de leur part une connaissance aussi pointue des derniers développements du domaine. Rien ne vaut les gens du terrain.

Autre critère important, choisir le bon niveau. Les formations en ethical hacking vont du cours d'introduction au perfectionnement le plus pointu destiné aux experts.

En général, un cours de base associe un peu de théorie et beaucoup d'exercices pratiques. On passe en revue les méthodes d'attaque des agresseurs pour apprendre à mieux s'en protéger. Un exemple très parlant est, par exemple, la démonstration de la déstabilisation complète de l'informatique d'une société, avec explication détaillée des outils et des technologies utilisés. On aborde aussi plus particulièrement la manière de penser, la stratégie et la démarche des agresseurs durant chaque étape du processus.

Les formations avancées sont, souvent axées sur de multiples exercices, à la complexité toujours plus grande. Là, il n'existe plus de «réponse toute faite» aux situations proposées. Les participants collaborent sous la conduite de l'instructeur pour parvenir à une solution et modéliser la théorie correspondante. C'est à la fois un challenge individuel et un travail d'équipe où les participants



Evelyne Pintado est Communication Architect chez Navixia.



«Connais ton ennemi et connais-toi toi-même; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites.», Sun Tzu, L'Art de la guerre

Photo: ©iStockphoto.com/BassittART

s'entraident. L'exercice est hautement stimulant et intellectuellement très satisfaisant.

Il faut relever que les responsables du réseau ou de la sécurité ne sont pas seuls concernés par ce type de cours. Les développeurs peuvent aussi y trouver profit, car les applications web de type Java, Perl, ou ASP, qui sont souvent connectées aux principaux systèmes de l'entreprise, s'avèrent des cibles tentantes pour les cybercriminels avec de sérieuses conséquences à la clé. En apprenant à reconnaître son «adversaire» et à repérer, quel que soit le langage de programmation, les faiblesses potentielles du code de ses applications, les développeurs peuvent adopter une approche mieux adaptée aux impératifs de sécurité.

Le hacking démystifié

Certains pensent pratiquer le ethical hacking en dressant des catalogues d'outils, en guettant et collectionnant tous les derniers tools. Ils se trompent. Pour agir efficacement, il est indispensable d'avoir une compréhension approfondie des systèmes, du réseau, de l'équipement, et de suivre une méthode

rigoureuse et claire. Sans cette connaissance, aucun outil ne permet de défendre son architecture intelligemment. Et c'est précisément à cela que servent les meilleurs cours de ethical hacking.

Alors, ces cours transforment-ils un collaborateur brillant en hacker? Non. Ces formations ne mettent pas les outils du hacker à la disposition des participants pour que ceux-ci reproduisent après coup ce qu'ils ont appris. Cela leur serait du reste quasiment impossible. Les formations visent à permettre aux participants de mieux contrôler la mise en œuvre sécuritaire de leurs projets futurs grâce à une nouvelle compréhension de la méthodologie des hackers.

«Mais alors, mon employé reviendra-t-il du cours en me déclarant que toute mon architecture réseau doit être remplacée pour satisfaire aux règles de sécurité?» s'inquiète le chef d'entreprise. Pas du tout. Ce genre de formation amène précisément à pondérer les risques et à les mettre en relation avec la réalité du quotidien de l'entreprise. Le but n'est pas de peindre le diable sur la muraille. Une

analyse équilibrée de la sécurité de l'entreprise montre quel est son niveau de risque par rapport aux autres entreprises; elle montre quelles failles sont éventuellement détectées, lesquelles sont vraiment importantes à corriger (toutes ne le sont pas), et de quelle façon.

Une protection efficace

Au terme d'un cours d'ethical hacking suivant une méthodologie bien précise, les participants comprennent comment fonctionne l'attaquant. Ils perçoivent donc le réseau de leur entreprise de manière très différente. L'expérience montre qu'ils sont alors considérablement mieux armés pour gérer la sécurité au quotidien. Le but n'est pas de savoir diagnostiquer instantanément les attaques lorsqu'elles se produisent, mais de savoir implanter de nouveaux systèmes de manière à ce qu'ils soient efficacement protégés. L'entreprise se retrouve largement gagnante et les participants profitent d'une expérience à la fois ludique et enrichissante tout en gagnant des compétences nouvelles de grande valeur.

«Quelqu'un qui s'assure tous les jours que les portes sont bien fermées»

Connaître son ennemi pour mieux s'en protéger. C'est le principe des cours d'ethical hacking qui enseignent les techniques des hackers aux équipes IT. Entretien avec Claude Krähenbühl, Managing Director de la société Navixia qui dispense de telles formations. *Interview: Rodolphe Koller*

En quoi consistent les cours d'ethical hacking?

Comme le nom l'indique, il s'agit de hacking éthique, c'est-à-dire d'enseigner aux informaticiens des entreprises les techniques utilisées par les hackers et leurs motivations. Il existe différents types de cours selon qu'ils s'adressent aux équipes IT, au management ou encore à des développeurs. Les partici-



Claude Krähenbühl est Managing Director du spécialiste sécurité Navixia.

«Avant, on pratiquait le hacking par goût du défi et pour la gloire. Aujourd'hui, c'est un business; l'argent est la principale motivation des hackers.»

pants apprennent à utiliser concrètement les armes, les outils et les méthodes des hackers avec de nombreux exercices pratiques. L'objectif étant qu'ils puissent tester la sécurité des systèmes de leur entreprise pour mieux les protéger.

Les motivations des hackers ont-elles changé?

Oui, il y a quelques années, on pratiquait le hacking par goût du défi et pour la gloire qui

découlait d'avoir pénétré un site emblématique. Aujourd'hui, c'est un business; l'argent est la principale motivation des hackers. Ils cherchent à accéder à des informations précises pour le compte de quelqu'un qui les mandate ou ils demandent de l'argent à une entreprise pour ne pas exploiter ou divulguer une faille qu'ils ont identifiée.

Quelles sont les mesures que les entreprises peuvent prendre pour se protéger de ces attaques?

Cela dépend de leur environnement informatique. C'est précisément pour cette raison que les cours d'ethical hacking font sens. Les fournisseurs de produits de sécurité proposent des solutions basées sur leur offre et négligent les failles qu'ils ne couvrent pas. Il importe que les responsables IT soient à même de repérer les failles qui subsistent et de décider où déployer des outils de protection et les cours d'ethical hacking les y aident. Il n'y a pas de solution standard. Par ailleurs, une banque et une entreprise industrielle n'ont pas les mêmes priorités et leurs données ne sont pas aussi sensibles; leurs systèmes de protections seront donc différents. Pour les éditeurs de logiciels, l'ethical hacking permet de sensibiliser les développeurs pour qu'ils prennent garde de ne pas introduire de vulnérabilités dans leurs applications.

En outre, les techniques des hackers évoluant, les personnes qui suivent ces cours reviennent souvent chaque année pour se tenir au courant des nouveaux types d'attaques.

Comment faites-vous pour vous tenir à jour sur les nouvelles attaques?

Nous collaborons depuis de nombreuses années avec Sensepost, une société sud-africaine spécialisée dans l'ethical hacking et active dans le monde entier. C'est leur activité première et ils passent donc leur temps à analyser les attaques et à tester les nouveaux outils de hacking disponibles sur internet. Cela demande du temps et des compétences particulières. Ils interviennent d'ailleurs régulièrement dans des événements comme les conférences internationales de sécurité IT, Black Hat. Ce sont leurs spécialistes qui dis-

pensent les formations à nos clients. Nous les mandats chaque année pour venir donner une session de cours de différents niveaux à nos clients et nous collaborons activement avec eux au déroulement des cours. Nous nous chargeons également de l'organisation. C'est aussi avec Sensepost que nous travaillons pour les audits complexes où il s'agit de vérifier des applications particulières. Vu la nature du travail, la confiance doit être absolument totale entre nous, notre partenaire et la société cliente.

Pour quels motifs les entreprises envoient-elles leurs collaborateurs à des cours d'ethical hacking?

Principalement pour mieux protéger leurs actifs en comprenant mieux qui pourrait les attaquer, pourquoi et comment. Nous avons deux types de demandes: soit des responsables IT et sécurité qui estiment qu'il est pertinent que leurs collaborateurs aient cette compétence, soit directement des ingénieurs qui souhaitent se former. Il faut souligner que souvent les seules formations qui leur sont offertes sont celles de fournisseurs, c'est-à-dire essentiellement des cours produits qui ne leur apportent pas une grande satisfaction.

Arrive-t-il que des sociétés vous demandent d'essayer de les hacker pour vérifier la robustesse de leurs protections?

Oui, et bien que l'on appelle cela également ethical hacking ou tests de pénétration, il s'agit d'une approche très différente des cours. C'est un service ponctuel qui permet effectivement de tester la qualité des protections mises en place et, le cas échéant, d'éliminer les failles identifiées. Mais, les systèmes de l'entreprise évoluent; on change l'infrastructure, on modifie la configuration d'un firewall et il est possible que de nouvelles failles apparaissent quelque temps après. En revanche, l'idée des cours d'ethical hacking est de s'assurer que les collaborateurs sont à même de tester la sécurité des systèmes sur la durée et d'empêcher les vulnérabilités en amont. En somme c'est avoir quelqu'un qui s'assure tous les jours que les portes sont bien fermées.