FPTI

Fédération des Professionnels des Tests Intrusifs

La Charte de l'Intrusion

FPTI : Association loi 1901

Parc de la Défense
41 rue des trois Fontanot
92024 - NANTERRE cedex
Tél : +33 (0)1 41 91 39 00
Fax : +33 (0)1 41 91 39 99

CONTEXTE

Les Professionnels des tests intrusifs ont décidé de se regrouper au sein de la Fédération des Professionnels des Tests Intrusifs (FPTI) et de se doter de règles déontologiques au travers de la présente Charte.

La Fédération des Professionnels des Tests Intrusifs (FPTI) a d'ores et déjà décidé, dans les douze mois de sa constitution, de promouvoir la création d'un organisme indépendant chargé du contrôle de l'application des règles énoncées aux présentes par ses membres.

La FPTI pourra notamment définir des partenariats adaptés avec des organismes représentatifs de la profession ou d'autres professionnels de l'informatique et exercer toute action de promotion auprès des instances compétentes afin que la réglementation des activités de cette nouvelle profession soit en cohérence avec les règles et principes énoncés dans la présente Charte.

PREAMBULE

L'ouverture des systèmes d'information par leur interconnexion aux réseaux de communication, dont l'Internet, les a fragilisés.

Dans un contexte où les technologies étaient stables et peu communicantes, la préoccupation de sécurité des systèmes d'information était relativement faible et une démarche d'audit pouvait suffire à la mesure de cette sécurité.

Dans un monde de technologies évolutives, basées sur l'interconnexion, le souci de la sécurité des systèmes d'information se doit d'être constant. Face à la fréquence et la variété des " attaques " que peuvent subir ces systèmes d'information, une démarche nouvelle et complémentaire à l'audit doit être menée : les tests intrusifs.

Les tests intrusifs[1] doivent être distingués des effractions menées par les "hackers" qui, s'ils agissent dans un environnement technique similaire ayant pour base l'introduction dans les réseaux et systèmes informatiques[2], le font dans un contexte pénalement répréhensible[3].

Ces trois actions sont couramment regroupées sous le vocable unique d'intrusion.

Face à cet amalgame, les Professionnels ont décidé de se regrouper afin de lutter contre les stéréotypes véhiculés par l'action des " hackers " considérée souvent comme ludique mais néanmoins délinquante.

La réunion de ces Professionnels au sein d'une Fédération a pour finalité de démontrer qu'il existe une véritable profession de l'Intrusion exerçant selon des règles garantissant aux clients le respect d'une déontologie en opposition avec ces pratiques délinquantes : soudoiement, chantage, déni de service, altération des données, vol, introduction physique dans les locaux, altération et/ou destruction des ressources informatiques, introduction et/ou maintien dans les systèmes informatiques de tiers ...

---

[1] toutes actions effectuées grâce à des systèmes externes permettant d'atteindre ou de traverser une ressource informatique et de juger du degré de résistance du système d'information dans lequel elle réside, afin de le qualifier

[2] toutes actions effectuées grâce à des systèmes externes permettant d'atteindre ou de traverser une ressource informatique

[3] toutes actions effectuées de manière déloyale grâce à des systèmes externes permettant d'atteindre ou de traverser une ressource informatique pour la détruire ou en détourner l'utilisation à son profit

Ce document appartient à la FPTI et est librement diffusable et copiable dès lors que la référence à la FPTI est maintenue

La définition de règles d'exercice de leurs activités par les professionnels de l'Intrusion permettra de parvenir à une auto régulation de la profession. Elle assurera en outre les clients de la rigueur et du sérieux des entreprises avec lesquelles ils contractent, afin d'établir avec les professionnels une relation de confiance.

La présente Charte de l'Intrusion énonce les quatre principes fondateurs des règles déontologiques de ses adhérents :

- la Moralité,
- la Transparence,
- la Confidentialité,
- la Probité.

En conséquence, tout adhérent à la Présente Charte :

PRINCIPE DE MORALITE

ARTICLE 1

S'engage à ne pas employer de "hackers" pour l'exécution de ses activités d'intrusion

En conséquence,

- il ne saurait employer pour l'exécution de ses activités d'intrusion qu'un personnel avec lequel il a une relation de travail stable et officialisée
- il prohibe toute pratique d'intéressement ponctuel de ses employés ou préposés aux opérations d'intrusion

ARTICLE 2

Certifie que les employés ou préposés à son service ont accepté les règles et principes contenus dans la présente Charte

En conséquence,

- il devra leur faire approuver les articles de la Charte les concernant

PRINCIPE DE TRANSPARENCE

ARTICLE 3

S'oblige à une information claire et précise sur son identité et celle de ses éventuels sous traitants

En conséquence,

- en tant que membre de la Fédération des Professionnels de l'Intrusion, il se soumet aux devoirs et obligations découlant de cette appartenance
- il fournira à première demande du client toutes informations relatives à son identité, son personnel, ses partenaires ou sous traitants, ses méthodologies et pratiques utilisées pour ses opérations d'intrusion, sous réserves de la protection de son savoir faire
- il s'obligera, à première demande, à procéder à toute déclaration ou enregistrement de son opération d'intrusion auprès de toutes autorités ou organismes de contrôle compétents

ARTICLE 4

S'oblige à une information claire et précise sur les actions menées lors des tests intrusifs

En conséquence,

- il communiquera toutes informations sur le lieu de situation de ses techniciens chargés des tests intrusifs
- il assurera une traçabilité des actions menées dans le cadre d'une opération d'intrusion

Ce document appartient à la FPTI et est librement diffusable et copiable dès lors que la référence à la FPTI est maintenue

ARTICLE 5

S'oblige à une information claire et précise sur tous les résultats des opérations d'intrusion

En conséquence,

- il informera le client de toute pratique illicite ou anormale qu'il aurait pu constater lors de l'exercice de ses tests intrusifs
- il s'engage à fournir à son client tous les résultats obtenus, qu'ils aient été demandés explicitement ou non

PRINCIPE DE CONFIDENTIALITE

ARTICLE 6

Garantit le respect de la plus stricte confidentialité sur toutes les informations dont il pourra avoir connaissance

En conséquence,

- cette obligation de confidentialité s'exerce tant à l'égard des personnels du client, autres que le mandant ou son délégataire, qu'à l'égard de tout tiers

ARTICLE 7

S'astreint à limiter la transmission des informations relatives aux tests intrusifs d'un client aux seuls membres de son personnel devant en connaître et à se porter fort du respect par ces personnes des clauses générales ou particulières de confidentialité s'appliquant à ces tests.

PRINCIPE DE PROBITE

ARTICLE 8

S'oblige à agir en toute indépendance dans l'exécution de ses prestations d'intrusion

En conséquence,

- il ne transmettra aux organes de l'état aucune information dont il pourrait avoir eu connaissance lors de l'exécution de ses tests intrusifs, sauf obligation légale
- il certifie qu'il n'utilisera pas, aux fins d'effectuer une prestation d'intrusion, des informations dont il aurait pu avoir connaissance à l'occasion de l'exercice d'une autre activité

ARTICLE 9

S'oblige à agir en toute loyauté et à n'effectuer de tests intrusifs que dans le strict cadre d'un mandat préalable et express

En conséquence,

- il s'interdit toute prestation intrusion avant vente
- il s'astreint à n'effectuer de prestations d'intrusion qu'après vérification des pouvoirs du mandant
- toutes prestations d'ingénierie sociale ne sauraient être effectuées sans signature préalable d'un mandat explicite spécifique

ARTICLE 10

S'astreint dans l'exercice de son métier à prendre toutes mesures permettant d'assurer la protection des droits de la personne humaine

Ce document appartient à la FPTI et est librement diffusable et copiable dès lors que la référence à la FPTI est maintenue