FPTI

Fédération des Professionnels des Tests Intrusifs

Réponse à l'Appel à commentaires émis par l'ANSSI concernant le Référentiel d'exigences applicables aux prestataires d'audit de la SSI version 0.9

Référence : AC-ANSSI-REFAUD-20110615

Date : 15 juin 2011

Version : 1.0

Contacts :

Olivier CALEFF – Président FPTI – olivier.caleff@fpti.info

Florence NOLLET – Trésorière – florence.nollet@fpti.info

Olivier REVENU – Secrétaire Général – olivier.revenu@fpti.info

---

Sommaire

1 Présentation de la FPTI

La **FPTI** – **Fédération des Professionnels des Tests Intrusifs** – est une association à but non lucratif (loi de 1901) créée en **1999** qui regroupe des professionnels pratiquant des Tests d'Intrusion.
Elle a été déclarée le **29 novembre 1999** à la préfecture des Hauts-de-Seine et publiée au Journal Officiel n°20000002 du 8 janvier 2000.

Elle a été créée par **3 sociétés françaises CF6, Apogée Communications et EdelWeb**, représentées respectivement par Patrick Coilland, Olivier Caleff, et Paul-André Pays. Déjà à l'époque, face à la dérive de certaines sociétés et au manque de sensibilisation des entreprises quant à la pratique des tests d'intrusion, elles ont souhaité encadrer et promouvoir la profession en se dotant d'une instance représentative.

La FPTI est ainsi à l'origine de la « **Charte déontologique de l'Intrusion » rédigée en 2000** qui est depuis un document de référence pour la profession.

La Charte de l'Intrusion est un code de bonne conduite reposant sur quatre piliers fondamentaux :

- Moralité.
- Transparence.
- Confidentialité.
- Probité.

Après quelques années d'inactivité et fort de cet acquis, la FPTI est aujourd'hui en plein renouveau et a accueilli de nouveaux membres en 2010 (Cf. chapitre 2).

Les **objectifs** de la Fédération sont de :

- fédérer les professionnels des tests d'intrusion au travers d'une organisation protégeant leurs intérêts ;
- développer, promouvoir et protéger la valeur et l'image des tests d'intrusion ;
- favoriser et définir les règles professionnelles des tests d'intrusion, ainsi que les méthodologies, procédures et processus de mise en œuvre, et les faire respecter ;
- représenter les intérêts de ses membres à l'égard des gouvernements, autorités et organisations ;
- offrir aux audités un référentiel de bonnes pratiques leur garantissant d'obtenir une prestation conforme à l'Etat de l'Art et comparable quelque soit le prestataire dès lors que celui-ci est membre de la FPTI.

Les **actions** de la Fédération sont de :

- fournir un cadre méthodologique et déontologique pour la pratique des tests d'intrusion ;
- réaliser des ouvrages, des synthèses sur l'état de l'art et les techniques de la profession ;
- favoriser et organiser pour ses membres des espaces d'échange et de réflexion autour de la profession et de son évolution ;
- communiquer au travers de publications, d'évènementiels (conférences, colloques ou toutes autres manifestations) et de partenariats dans le but de défendre et de promouvoir les intérêts de la profession ;

- mettre en œuvre des actions de promotion auprès des instances législatives et réglementaires pour favoriser l'émergence de règles d'encadrement et d'un encadrement juridique de la profession en adéquation avec les principes de la Charte de l'Intrusion.

Le cadre méthodologique et déontologique, que nous appelons « **Référentiel de l'Intrusion** », est en cours d'élaboration par les membres de la FPTI, il est constitué des éléments suivants :

- La « charte de l'intrusion ».
- La démarche type.
- La méthodologie type.

Nous attirons l'attention de l'ANSSI sur le fait qu'il existe une autre association créée en **2010**, qui utilise le même nom et qui revendique des éléments qui font référence à notre association, telle la « charte de l'intrusion » de 2000. Nous sommes au courant de ce problème et travaillons à le résoudre.

2 Membres de la FPTI

La FPTI est actuellement constituée des membres suivants :

- Devoteam (historiquement Apogée Communications)
- EdelWeb - Groupe ON-X
- HSC
- iTrust
- NBS System
- Telindus (historiquement CF6)

Dès la mise en ligne sur notre nouveau site Web de la première version du « **Référentiel de l'Intrusion** », l'association accueillera tout membre professionnel des tests d'intrusion dès lors qu'il satisfait au règlement intérieur et qu'il est prêt à appliquer le Référentiel de l'Intrusion dans ses prestations.

3 La réponse de la FPTI à l'appel à commentaires

La présente réponse est donc une réponse collective, issue du fruit des réflexions des membres de la FPTI.

Les membres de la FPTI se tiennent à la disposition de l'ANSSI pour discuter plus précisément de toute ou partie de cette contribution, ou de problématiques évoquées dans le *Référentiel d'Exigences*.

Elle comprend quelques remarques générales ainsi que des remarques spécifiques sur plusieurs points du document intitulé **« PRESTATAIRES D'AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION - Référentiel d'exigences » dans sa version 0.9 datée du 11 mai 2011** [1] et ayant servi de base à la réflexion.

La numérotation des commentaires est continue afin de faciliter le travail si le présent document devait servir de base à une analyse plus poussée.

3.1 Remarques générales

Les remarques générales sont les suivantes :

1. Compte-tenu du caractère novateur de ce *Référentiel d'Exigences* et de sa probable reprise par différents acteurs – y compris des commanditaires – sans qu'une relecture attentive en soit faite, il apparaît souhaitable aux membres de la FPTI que le contexte réglementaire soit mis encore plus en évidence (§1.1, second paragraphe, lignes 12 à 14). Il pourrait ainsi y être rappelé que les exigences sont destinées avant tout à l'Administration Française, et que certaines d'entre elles ne s'appliquent pas nécessairement dans tous les contextes du monde civil.

2. La classification et les métriques proposés dans le § 5.7.c (et tout particulièrement le tableau en ligne 534) apparait comme étant tout à fait légitime aux yeux des membres de la FPTI, mais amène à se poser une question : cette classification est-elle une « recommandation », une « préconisation », celle qui devra s'appliquer pour tous les « audits techniques de la sécurité des systèmes d'information des autorités administratives » ? S'agit-il d'un modèle pour les autorités administratives ne disposant pas déjà d'une classification et de métriques propres ?

3. Le *Référentiel d'Exigences* met en avant les devoirs des « autorités administratives » devant faire réaliser des audits techniques. Il semble particulièrement s'adresser à celles qui n'en font pas. Il devrait mentionner la façon dont celles qui en réalisent parfois depuis de très nombreuses années, devraient aborder le *Référentiel d'Exigences*.

4. Le *Référentiel d'Exigences* ne mentionne pas de façon explicite les devoirs des commanditaires, même si une « Convention d'audit » est mentionnée au paragraphe §5.3.

[1] Le document cité en référence est disponible à la date de rédaction du présent document sur la page http://www.ssi.gouv.fr/site_article328.html et téléchargeable à l'adresse http://www.ssi.gouv.fr/IMG/pdf/referentiel-exigences_labellisation_prestataires-audit-teleservices_v0-9.pdf

Or le non-respect de certaines clauses de cette « Convention d'audit » pose de nombreux problèmes. Cela semble particulièrement important aux membres de la FPTI, qu'il est fréquemment constaté que ce non-respect pose de nombreux problèmes de logistiques, de rallongement des délais de réalisation, voire d'incompréhension et est source d'insatisfaction de part et d'autre. Il serait par exemple souhaitable d'expliciter certains de ces devoirs tels que :

- La garantie que les domaines et les périmètres exhaustifs couverts par l'audit sont de responsabilité du commanditaire ou que les responsables (hébergeurs, sous-traitants, partenaires …) sont dûment avertis de l'audit et qu'ils ont donné leur accord. A titre d'exemple, on peut citer des intermédiaires ou des tiers qui seraient impactés par certains tests et qui, par crainte des impacts, pourraient demander leur réalisation dans certains créneaux de temps, afin de ne pas risquer de perturber leur production.

- La garantie que le commanditaire donne en temps et en heures une liste exhaustive des bons contacts, tant en interne de son entité, que pour ses tiers et partenaires.

- La garantie qu'une fois la prestation d'audit terminée, et tous les éléments de preuves détruits par l'auditeur, aucune contestation de la qualité – voire de la réalité – de la prestation ne pourra être opposée.

5. Le *Référentiel d'Exigences* donne une liste de compétences que des auditeurs devraient posséder.

   - D'une part les membres de la FPTI se sont étonnés du niveau des détails donnés quant aux aspects techniques devant être maîtrisés par les auditeurs, et ils considèrent que ce niveau de détail (comme par exemple dans le §5.2.1.c, lignes 339 à 342) devrait plutôt être mis dans une annexe. L'une des raisons étant qu'un état de l'art technique ne devrait pas être explicité dans un référentiel d'exigences, et que la liste donnée dans le *Référentiel d'Exigences* n'est pas apparue comme étant exhaustive déjà aujourd'hui, et d'autre part comme étant susceptible d'évoluer très rapidement dans le temps, sans parler de la publicité indirecte faite aux produits commerciaux cités.

   - D'autre part, seule une lecture attentive du *Référentiel d'Exigences*, permet de comprendre que les compétences requises s'appliquent au « Prestataire d'audit » dont font partie les auditeurs (entreprise unique, regroupement ou consortium de plusieurs entreprises, …). Ils s'appliquent donc à une équipe considérée comme étant un « tout », et non pas individuellement. Les membres de la FPTI pensent que les compétences attendues devraient être reformulées afin de mieux pouvoir s'appliquer à la notion de « Prestataire d'audit » ?

6. Le *Référentiel d'Exigences* fait état aux paragraphes §3.1.m (lignes 200 à 202), §3.2 (lignes 212 à 213) et §5.3.a (lignes 418 à 419) de la problématique de non-divulgation. Un cas devrait toutefois être pris en compte dans le référentiel : celui du traitement et de la transmission de vulnérabilités à des tiers particuliers tels que des éditeurs ou des

constructeurs directement concernés par des vulnérabilités découvertes dans le cadre de l'audit, voir des CERT accrédités. De même, les différentes positions que peut prendre un commanditaire devant la découverte d'une vulnérabilité devraient être mentionnées (divulgation ou non et à quels tiers : éditeur, CERT, autre ?), afin que l'auditeur puisse agir avec l'accord du commanditaire et dans le respect du référentiel.

7. Des membres de la FPTI ont aussi été surpris que le *Référentiel d'Exigences* intègre à la fois des « exigences » et des « recommandations ». *A minima*, il apparait souhaitable qu'à l'instar d'autre documents et normes, une définition du niveau d'importance d'une exigence soit proposée ainsi que sa métrique de lecture. A titre d'exemple, les membres de la FPTI pensaient aux fameux « SHOULD » et « MUST » des documents de type RFC (*Request for Comment*) de l'IETF.

3.2 Remarques spécifiques

Les remarques spécifiques sur des points précis du *Référentiel d'Exigences* sont les suivantes :

8. Les membres de la FPTI proposent qu'un sixième type d'audit et de test soit ajoutée dans le paragraphe §2 du *Référentiel d'Exigences* : les « tests ou audits applicatifs ». La lecture du paragraphe §2.1 sur l'audit de code (notamment les lignes 121 à 123) pourrait laisser penser que de tels tests pourraient être intégrés dans la catégorie des « audits de code source », mais il s'agit de quelque chose de bien distinct, qui requiert sa place à part entière dans une nomenclature des types d'audits et de tests.

9. Les membres de la FPTI déplorent que plusieurs domaines soient non couverts dans le paragraphe §2.6 du *Référentiel d'Exigences* :

    - les audits de la sécurité physique des locaux (ligne 154), ou tout au moins ceux des salles qui hébergent des composants testés directement ou indirectement dans le cadre d'une analyse ou d'un audit ;

    - l'ingénierie sociale (ligne 158), qui est une activité en forte augmentation dans la réalité des attaques et de la cyber criminalité actuelle ;

    - enfin, les membres de la FPTI s'interrogent sur la raison pour laquelle « les audits isolés de détection (scan) de vulnérabilités » ne sont pas couverts par le *Référentiel d'Exigences. Est-ce parce que l'ANSSI ne souhaite pas que ces prestations soient réalisées de manière isolée dans le cadre d'audits de sécurité pour le compte des* « autorités administratives » *?*

10. Dans le paragraphe §3.1.c, un prestataire d'une mission d'audit ne peut « *assume*(r) *l'entière responsabilité de l'audit qu'il réalise pour le compte du commanditaire de l'audit, en particulier des dommages éventuellement causés au cours de l'audit* » (lignes 168 à 170) que pour les actions qui lui incombent. Cela nécessite aussi que le commanditaire lui ait donné tous les éléments permettant à l'auditeur d'analyser les risques. Le contenu de la « Convention d'audit » mentionnée au paragraphe §5.3 prend alors tout son sens afin de définir les rôles et responsabilités des 2 parties. Les membres de la FPTI proposent de

modifier l'exigence comme suit : « *assume(r) la responsabilité de l'audit telle que définie dans la Convention d'audit (voir 5.3)* ».

11. De même, dans le paragraphe §3.1.d, un prestataire d'audit « *doit pouvoir apporter la preuve qu'il a évalué les risques résultant de ses activités d'audit et qu'il a pris les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit* » (lignes 171 à 173) que dans la mesure où le commanditaire lui a communiqué des éléments pertinents, fiables et réels. Les membres de la FPTI peuvent ainsi relater des cas d'erreurs sur l'appréciation des risques, car basée sur des informations communiquées par des commanditaires qui étaient erronées : les causes principales étaient le plus souvent involontaires (omissions, mauvaise connaissance du contexte de la part du commanditaire). Les membres de la FPTI ont pleinement conscience de la difficulté de l'exercice, mais considèrent qu'ils ne peuvent endosser seuls, et dans tous les cas, la responsabilité en cas de mauvaise évaluation des risques, voire de dommages.

12. En revanche, toujours pour le paragraphe §3.1.d, les membres de la FPTI considèrent qu'un soumissionnaire devrait exiger « *que le prestataire d'audit souscrive une assurance couvrant les dommages éventuellement causés aux systèmes d'information de ses clients, y compris après la livraison de la prestation*.» (lignes 174 à 176). Compte-tenu des enjeux, la seule recommandation n'apparait pas comme suffisante.

13. Un cas devrait être explicitement mentionné à côté du paragraphe §3.1.m : celui de l'utilisation du nom d'une société auditée à des fins de référence commerciale si l'audité l'accepte.

14. En se basant sur leur expérience, les membres de la FPTI considèrent que la notion de « *contenu illicite* » mentionnée dans le paragraphe §3.2.a (lignes 214 à 215) devrait être plus détaillée. En effet, il peut s'agir de « *contenu illicite* » au sens de la Loi, de la morale, de chartes de sécurité ou de règlements intérieurs, …

15. Les membres de la FPTI craignent que la formulation de la condition mentionnée au paragraphe §3.3.a (lignes 220 à 222) aie pour effet d'exclure des consultations des sociétés d'audit n'ayant pas une taille minimale. Une formulation qui remplacerait le mot « *employer* » par « *doit disposer de ressources suffisantes, notamment en faisant appel à des partenaires (sous-traitance, …)* »

16. Les membres de la FPTI souhaitent une modification de la phrase « *Il est recommandé que le système que le prestataire d'audit utilise pour le traitement des informations évoquées au a) soit certifié selon la norme ISO 27001* » au paragraphe §3.4.b (lignes 282 à 283). Une reformulation excluant la notion formelle de ISO 27001 mais transformant la recommandation en exigence en indiquant que « *le prestaire doit pouvoir garantir et démontrer qu'il prend toutes les précautions nécessaires pour le traitement des informations relatives aux prestations d'audits* ».

17. Les membres de la FPTI souhaitent que la question de la formation des auditeurs et de leurs expériences du paragraphe §4.2 soient revues :

- D'une part, la formation en « *école d'ingénieur délivrant un diplôme reconnu par la commission des titres d'ingénieur, ou ait suivi un cursus universitaire de niveau Master minimum, avec une spécialisation en informatique* » (lignes 293 à 295) ne devrait pas être une condition nécessaire (même sous forme de recommandation) sous peine d'interdire l'exercice de l'activité d'auditeur à des personnes très compétentes et avec une expertise reconnue et éprouvée, mais n'ayant pas le niveau d'étude mentionné.

- D'autre part, une tolérance est demandée pour les auditeurs ne remplissant pas les conditions d'expérience mentionnées (lignes 296 à 301), afin qu'ils puissent toutefois participer à des audits. Il pourrait ainsi y avoir une « tolérance » pour un auditeur dit « junior » ou « débutant » dans la mesure où il est accompagné par une personne remplissant les conditions d'expérience.

18. Dans le paragraphe §5.2, les mots « *a minima* » (lignes 330, 339, et 351) devraient être supprimés. En effet, le commanditaire peut décider que le périmètre qu'il confie à une équipe d'auditeur est plus réduit, voire qu'un même périmètre est volontairement réparti entre deux équipes provenant de sociétés différentes. Ainsi, chaque auditeur ou équipe d'auditeur n'a qu'une vision parcellaire d'un tout. De manière générale, la liste des contrôles à effectuer ne devrait pas figurer dans ce référentiel mais être proposée dans un autre document plus exhaustif.

19. Il serait souhaitable de remplacer la notion de « *condamnation pour fraude informatique* » au Paragraphe §5.3.a (lignes 420 à 422) par celle factuelle de « bulletin n° 3 du casier judiciaire ». L'employeur ne peut être tenu responsable que s'il dispose des moyens pour vérifier cette information.

20. L'application de l'exigence mentionnée dans le paragraphe §5.8.d « *Le prestataire d'audit doit fournir, à la fin de l'audit, les développements spécifiques réalisés lors de l'audit pour valider les scénarios d'exploitation des vulnérabilités. Ces développements peuvent être fournis sous la forme de scripts ou de programmes compilés, accompagnés de leur code source, ainsi que d'une brève documentation de mise en œuvre et d'utilisation* » (lignes 549 à 553) est complexe (notamment la problématique de responsabilité quant à la fourniture de moyens d'exploitation de vulnérabilités) et risque de provoquer une augmentation très significative de la charge de travail et des coûts de réalisation. Il est donc souhaitable de transformer cette exigence en recommandation et de préciser : « *lorsque les conditions d'ordres techniques, contractuelles ou budgétaires le permettent* ».

21. Dans le paragraphe §5.5.e « *Les actions susceptibles d'entraîner une compromission d'informations sensibles ou un déni de service doivent être effectuées en présence de l'audité* », les membres de la FPTI souhaitent que le terme « *en présence* de l'audité » qui sous-entend une présence physique sur site, soit remplacé par « *avec l'accord du commanditaire* » et que soit ajouté la phase « *dans des conditions définies avec l'audité* ».

22. Dans le paragraphe §8.2.d de l'Annexe B l'exigence que « *Les tests d'intrusion ne devraient pas être réalisés sur des plates-formes d'hébergement mutualisées* » (lignes 688 à 689) semble trop restrictive. Ne serait il pas possible de l'assouplir dans la mesure où toutes des

précautions sont prises et que les risques sont évalués et maîtrisés, et que les responsabilités sont clairement établies (Cf. remarque précédente n°4 relative à la Convention d'Audit) ? Dans le cas contraire, et dans l'approche didactique de ce *Référentiel d'Exigences*, ne faudrait-il pas proposer des alternatives pour réaliser des tests d'intrusions sur les environnements et plateformes cibles ?

Dans le paragraphe §5.6, le terme utilisé est « restituer », et il n'y a pas de précisions sur la forme de cette restitution. Les membres de la FPTI souhaitent que ce premier compte-rendu à la fin de l'audit soit « informel » et de remplacer le terme « restituer » par « informer » car celui-ci peut être réalisé par téléphone, oralement ou par écrit.