Contrat de TESTS d'INTRUSION ET AUDIT SECURITE

Entre les soussignés :

ci-après dénommée " L'audité ", d'une part,

et

ANDRE ALLAGUY-SALACHY (INFORMATICIEN INDEPENDANT N° TAHITI 556001),

ci-après dénommé " L'auditeur ", d'autre part,

Il a été préalablement exposé ce qui suit :

souhaite réaliser des Tests d'Intrusion et un Audit de Sécurité afin de vérifier la capacité de son réseau en termes de résistance à des intrusions et l'efficacité de ses mesures actuelles de sécurisation de son système d'information;

ANDRE ALLAGUY-SALACHY (INFORMATICIEN INDEPENDANT N° TAHITI 556001) a accepté d'effectuer ces Tests d'Intrusion et cet Audit de Sécurité, et le présent contrat a pour objet de préciser les termes et conditions de cette mission.

Ceci exposé, il a été convenu ce qui suit :

Objet du contrat

Article premier. L'audité confie à l'auditeur qui accepte le soin d'assurer des Tests d'intrusion et un Audit de Sécurité pour éprouver la sécurité des systèmes d'information de l'audité. La mission se conclura par la remise à l'audité d'un rapport des Tests d'Intrusion et d'un rapport d' Audit de Sécurité complet.

Nature de la mission

La mission se déroulera en deux étapes

Article 2. Les Tests d'Intrusion se dérouleront suivant la méthodologie ci--dessous :

- **Cible de sécurité :**
  - Système d'Information de l'organisme,
  - Résistance aux intrusions et menaces externes
  -
- **Modalité d'Intervention :** Tests d'Intrusion de type "black box"
  (Tests de vulnérabilités et tests d'intrusion à l'aveugle i.e. sans connaissance antérieure ou dans les conditions d'un pirate qui n'aurait pas plus de connaissance du système de l'audité)
- **Périmètre d'analyse :** réseaux, systèmes, applications, personnel, accès physiques, etc...
- **Moyens :** Tout accès de type réseau : ADSL, PABX, ISDN, RTC, Transfix, ATM, Wireless, GSM, Satellite, GPRS, 3G, Edge, Fibre Optique, liaisons à vos clients et fournisseurs, ou point de connexions, accès physiques, ingénierie sociale (social engineering)
- **Périodicité Ponctuelle :** Tests d'Intrusion unique suivi d'un audit

- **Contraintes Juridiques :**

En conformité avec l'article 323 du nouveau Code Pénal, ce contrat vaut accord préalable du propriétaire ou de l'exploitant du système d'informations à auditer.

Toute partie du système cible hébergée ou confiée à des tiers prestataires (hébergeurs, providers, sous-traitant en régie…) devra être couverte par une autorisation accordée par ceux-ci, le test se déroulant à l'aveugle, l'audité aura la charge de prévenir et d'obtenir les autorisations de ceux-ci.

- **Contraintes Fonctionnelles :**

La nécessité d'une continuité de service du SI tout au long des tests impose de ne pas entraver le fonctionnement des systèmes d'information durant le test.

Une sauvegarde système, applicative et des données est donc nécessaire

Etant difficile de tester comme un pirate n'hésiterait pas à le faire tout en étant certain de ne pas provoquer de dysfonctionnements ou d'entraîner un déni de service,

l'audité a la possibilité d'indiquer une préférence horaire pour les tests sur les différents systèmes :

1. Heures de Déjeuner
2. Toute la nuit
3. Suivant les créneaux horaires précisés ci-après : soit au total:

- **Contraintes Opérationnelles:**

La nécessité d'une coopération du service du SI tout au long des tests impose de ne pas entraver les tests des systèmes d'information par la modification des comportements, habitudes, us et coutumes des utilisateurs ou administrateurs réseau durant le test en dehors des procédures réactives en vigueur dans l'organisme au moment de la signature de ce contrat.

- **Contraintes Déontologiques :**

L'auditeur s'interdira par principe et respect déontologique les nuisances résultant, en cas de succès, d'une prise de contrôle total, à distance, des systèmes vulnérables:

1. de falsifier ou corrompre des données, a fortiori des données confidentielles (courrier électronique, rapports, mots de passe, contrats, numéros de cartes de crédit, etc.) ;
2. d'installer des programmes destructeurs
3. de laisser des applications de types backdoors, installées et utilisées pendant les tests, persister à la fin des tests sur les machines auditées.
4. d'attaquer depuis ces machines des machines externes au système d'informations de l'organisation auditée et lui faire endosser ainsi la responsabilité de ces attaques ;

Article 2bis. L'audit de la sécurité du système informatique se déroulera suivant la méthode ci-dessous conformément aux normes et pratiques en vigueur:

- Étude du contexte
- Expression des besoins
- Étude des menaces :
- Identification des objectifs de sécurité : hiérarchisée selon l'importance des risques (en termes d'impact et d'opportunité des menaces) afin de d'ordonnancer un plan d'action ;
- Détermination des exigences de sécurité : réalisée avec le concours de l'audité et de ses utilisateurs afin de déterminer des exigences encore plus adaptées et directement applicables.

L'opération d'audit de la sécurité du système d'information de l'audité comprendra notamment :

- l'analyse des risques, menaces, vulnérabilités et niveau d'exposition par rapport aux parades disponibles ou mises en œuvre des éléments matériels, progiciels, logiciels, documentations, sociétés de services, utilisés par l'audité;
- appréciation globale de l'adéquation entre les besoins en sécurité spécifiques à certains services et le système d'information existant, intéressant notamment les activités administratives comptables et financières de l'audité;
- examen des méthodes d'organisation, de contrôle et de planification des services informatiques, de la formation, de la qualification et de l'aptitude des personnels, initiés ou non à la sécurité informatique
- évaluation de la sécurité informatique, de son efficacité, de la bonne utilisation des terminaux, des procédures de saisies de données, des méthodes de gestion des programmes, des sauvegardes, des accès et de la confidentialité
- appréciation de la qualité, de l'accès, de la disponibilité et de la facilité de compréhension de la documentation actuelle (note de service , charte, etc.)liée aux risques et à la sécurité;
- mise en évidence des utilisations imparfaites du système d'information, abus, usages, …
- analyse comparative du coût et des charges afférentes au fonctionnement du système d'information et notamment par rapport à sa sécurité:
- évaluation des capacités, des performances, de la compatibilité, de l'évolutivité du système d'information, etc., plus appréciation de la performance, de la compatibilité des logiciels;
- analyse et diagnostic des moyens d'optimiser la sécurité de traitement au moment de la saisie, de la gestion, du stockage et de la diffusion d'une information,
- examen de la sécurité liée au site web
- audit de la sécurité découlant des contrats informatiques tels que : contrats d'assistance, contrats de maintenance des matériels, des logiciels, contrats d'accès et d'hébergement, contrats d'animation de site;
- vérification du libre usage des droits d'auteur sur toutes les créations en matière de communication internes ou externes
- analyse des prestations fournies par des entreprises extérieures, et principalement des risques inhérents à ces prestations, menaces engendrées, etc.;
- examen des menaces, risques, vulnérabilités, parades disponibles ou mises en œuvre et des besoins en sécurité issus de l'utilisation de serveurs propres ou extérieurs.
-
-
-
-

Plus généralement, l'auditeur établira toutes les constatations dont il aura connaissance, en plus de celles ci-dessus énoncées à titre indicatif.

Durée de la mission

Article 3. La taille du réseau lui étant inconnu, l'auditeur afin de réaliser sa mission de Tests d'Intrusion de type "black box" i.e. en aveugle et d'Audit de Sécurité se verra attribuer par l'audité une durée minimale de mission correspondant au total calculé ci-dessous :

- *NB. DE SERVEURS* 3
- *NB. DE CLIENTS* 2
- *NB. DE RESSOURCES RESEAU (IMPRIMANTE ROUTEUR SWITCH HUB)* 5
- *NB. D'APPLICATIONS CRITIQUES SUR SERVEURS* 0

La Durée contractuelle totale sera donc de 0 jours (MAX DE 60 JOURS).

Le rapport des Test d'Intrusions

Article 4. L'auditeur n'est pas tenu d'informer l'audité au fur et à mesure de l'avancement de sa mission de Tests d'Intrusion.

Néanmoins toute faille critique détectée et présentant un risque grave sera portée à la connaissance de l'audité si sa divulgation ne peut être repoussée à la remise du rapport devant le danger imminent qu'elle représente (danger et menaces classées très graves d'atteinte au SI pour un niveau d'expertise du pirate classé à faible).

Le rapport des Tests d'Intrusion comprendra notamment un exposé de l'organisation actuelle des systèmes d'information de l'audité, exposé issu des prises d'empreinte, recensement, balayage, obtention d'accès, méthodes d'ingénierie sociale les Tests d'Intrusion.

Le rapport des Tests d'Intrusion comprendra de manière détaillée,

1. les vulnérabilités, failles, risques et menaces découvertes,
2. l'impact qu'elles ont sur le système d'informations
3. les actions à mener pour combler ces failles, qu'il s'agisse de mises à jour de logiciels, d'ajustements de configuration, ou encore de modifications de fond dans l'architecture réseau ou encore dans la politique de sécurité de l'organisation.

Le rapport des Tests d'Intrusion pourra être débattu lors de la présentation de ses conclusions et suivi de discussions constructives et d'actions concrètes décidées de concert pour la mise en œuvre de l'audit de sécurité.

Le rapport d'audit

Article 4bis. L'auditeur informera l'audité à mesure de l'avancement de sa mission, aux fins de faire valider par l'audité les constatations déjà effectuées.

Le rapport d'audit comprendra notamment un exposé de l'organisation actuelle des systèmes d'information de l'audité, ainsi qu'une analyse détaillée et chiffrée des choix techniques, matériels et humains, en distinguant les solutions optimales, acceptables, et prioritaires avec une évaluation de leur efficacité.

Le rapport d'audit intégrera l'analyse des 4 paramètres clés :

- Disponibilité : accessibilité du système d'information pour le traitement des données.
- Intégrité : garantie de la consistance des données.
- Confidentialité : garantie d'accessibilité à l'information dans le réseau que par la bonne personne/application.
- Preuve : propriété du système d'exploitation qui garantit que l'on est capable de savoir qui a accédé à quel moment à une donnée ou une application

Le rapport formulera également et en particulier des recommandations sur les performances des installations, sur l'organisation informatique actuelle, sur le perfectionnement de celle-ci et sur l'opportunité de l'élaboration d'un nouveau cahier des charges.

Le rapport d'audit pourra déboucher sur la proposition d'établissement

- *d'un schéma directeur*
- *d'une charte utilisateur informatique*
- *d'une politique de sécurité,*

où seront notamment précisés les délais, le prix et le contenu de cette/ces nouvelle(s) mission(s).

Lieu, modalités et délai d'exécution de la mission

Article 5. La mission de Tests d'Intrusion et d'Audit de Sécurité s'effectuera respectivement envers et dans les différents sites composant le système d'information.

L'auditeur accomplira sa mission en toute indépendance.

Pour l'accomplissement de cette mission, l'auditeur s'interdit de désigner une autre personne, de telle sorte que le présent contrat ne pourra en aucun cas être transmis à un tiers, sauf accord exprès et préalable de l'audité.

Le rapport des Tests d'Intrusion doit être communiqué au plus tard le

Le rapport d'Audit de Sécurité doit être communiqué au plus tard le

Rémunération de l'auditeur

Article 6. En contrepartie de l'exécution de sa mission, l'auditeur percevra une rémunération forfaitaire, d'un montant de CFP HT qui représente l'intégralité du coût de cette mission.

La rémunération de l'auditeur est payable à l'expiration de la mission.

Confidentialité

Article 7. L'auditeur et les personnes qui l'assisteront dans sa mission, sous sa responsabilité exclusive, s'engagent à considérer comme " confidentielles " et entrant dans le champ d'application du secret professionnel auquel ils seront tenus, les informations de toute nature, écrites ou orales, relatives aux activités et attributions de l'audité, que l'exécution de leur mission les amènerait à connaître, sans que lesdites informations n'aient à être estampillées " confidentielles ".

L'auditeur et les personnes qui l'assisteront dans sa mission, sous sa responsabilité exclusive, s'engagent à ne pas divulguer lesdites informations confidentielles à quiconque, et en tout état de cause à respecter la présente clause de confidentialité, aussi longtemps que lesdites informations n'auront pas été portées à la connaissance de tiers par l'audité lui-même.

L'auditeur fera signer un contrat de confidentialité par toutes les personnes intervenant à l'exécution de cette mission.

Propriété du rapport des Tests d'Intrusion et du rapport d'Audit de Sécurité

Article 8. Il est expressément stipulé que les rapports de Tests d'Intrusion et d'Audit de Sécurité établis par l'auditeur dans le cadre de sa mission seront la propriété exclusive de l'audité. En

aucun cas le présent contrat n'emporte transfert du droit d'utiliser, de publier ou de reproduire, au profit de l'auditeur les informations qui lui auront été communiquées par l'audité.

L'auditeur sera libre de faire état de son intervention auprès de l'audité dans ses références commerciales.

Responsabilité de l'auditeur

Article 9. En toute circonstance, l'auditeur reste seul responsable de l'organisation, de la réalisation et de la synthèse de la mission qui lui a été confiée par l'audité.

Interprétation et modification

Article 10. Le présent contrat exprime l'intégralité de l'accord entre les parties. Il remplace et annule tous les pourparlers, accords verbaux ou écrits précontractuels entre les parties.

Règlement des litiges

Article 11. Tous litiges qui s'élèveraient à propos de l'exécution ou l'interprétation du présent contrat et qui ne pourraient être résolus à l'amiable, seraient dénoués par voie d'arbitrage, suivant le règlement d'arbitrage du Centre de conciliation et d'arbitrage des techniques avancées (ATA) auquel les parties déclarent expressément se référer. Le tribunal statuera en amiable compositeur.

Fait à le

L'audité L'auditeur

Réinitialiser

B.P. 52383 98716 PIRAE - GSM: 0689-705353 – andre.allaguy@mail.pf
N° TAHITI: 556001