INGÉNIEUR Tterritorial

CONCOURS INTERNE

SESSION 2015

ÉPREUVE D'ETUDE DE CAS OU PROJET

ÉPREUVE D'ADMISSIBILITÉ :

Établissement d'un projet ou étude portant sur l'une des options choisie par le candidat lors de son inscription au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : Réseaux et télécommunications

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni signature ou paraphe, ni votre numéro de convocation.
- Aucune référence (nom de collectivité, nom de personne, …) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.
- Pour la rédaction, seul l'usage d'un stylo à encre soit noire, soit bleue est autorisé (bille non effaçable, plume ou feutre). L'utilisation d'une autre couleur, pour écrire ou pour souligner, sera considérée comme un signe distinctif, de même que l'utilisation d'un surligneur.
- Pour les dessins, schémas et cartes, l'utilisation d'une autre couleur, crayon de couleurs, feutres, crayon gris, est autorisée le cas échéant.
- L'utilisation d'une calculatrice en mode autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 36 pages

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué

S'il est incomplet, en avertir le surveillant

- Vous préciserez, le cas échéant, le numéro de la question et de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Ingénieur territorial, vous êtes nommé adjoint au chef de service informatique de la commune d'INGEVILLE, 25 000 habitants.

La première mission qui vous est confiée est de mener une réflexion sur la sécurité du système d'information.

À l'aide des différents éléments contenus dans le dossier d'analyse et en utilisant vos connaissances personnelles, le directeur des systèmes d'information vous demande :

Question 1 (4 points)

Vous rédigerez une note qui réponde aux interrogations suivantes :

1) Comment organiser et mener un audit de sécurité du système d'information ? (1,5 point)

2) Vous donnerez les pré-requis indispensables. (1 point)

3) Quelles sont les 3 phases d'un audit sécurité, en précisant la portée et les objectifs de chacune ? (1,5 point)

Question 2 (5 points)

La sécurité du système d'information présente certains risques.

Dans une note :

1) Vous expliquerez à quels types de risques vous pouvez être confronté. (3 points)

2) Comment les classifier ? (2 points)

Question 3 (6 points)

A partir des éléments des questions 1 et 2, vous rédigerez le cahier des charges en vue de la consultation des entreprises pour réaliser cet audit sécurité. Vous intégrerez à ce cahier des charges un planning de réalisation de l'audit.

Question 4 (5 points)

Vous rédigerez une charte utilisateur des ressources informatiques, téléphoniques et des services internet de la commune.

Liste des documents :

Document 1 : « Métro : la Mairie de Paris victime d'une attaque informatique ! » - *Métro* - 23 août 2012 - 2 pages

Document 2 : « Réseau informatique : en quoi consiste un audit de sécurité » - *réseau-informatique.prestataire.com* - consulté le 12 décembre 2014 - 1 page

Document 3 : « Réaliser un audit de vos systèmes informatiques » - *ACIPIA* - consulté le 12 décembre 2014 - 1 page

Document 4 : « Audit général de sécurité » - *société Lynx Technologies* - édité le 12 décembre 2014 - 18 pages

Document 5 : « Cahier des charges - audit du système d'information » - *Commune de La Verrière* - 2009-2010 - 8 pages

Document 6 : « La sécurité informatique, une mission d'utilité publique ? » - *Tanguy de COATPONT - Les Experts* - 7 avril 2013- 2 pages

Document 7 : « Charte informatique et téléphonique » - *Ville de Cahors, Grand Cahors, CCAS, CIAS, EPIC Tourisme* - 5 juillet 2013 - 1 page

Jeudi 23 août 2012

Métro : La Mairie de Paris victime d'une attaque informatique !

Métro : le 23 août 2012

Les données de près de soixante mille Parisiens potentiellement piratées !

Le Canard Enchaîné a révélé hier que l'un des sites de la mairie de Paris avait été piraté la semaine dernière. Les deux hackers auraient accédé aux données personnelles de 58 599 Parisiens. La Ville rétorque qu'aucune donnée confidentielle n'est partie dans la nature.

Le 16 août, le site 'paris.plan.fr' qui permet de consulter et de s'inscrire aux activités de la ville (Pass Jeunes, jeux concours), a été piraté depuis l'Algérie par deux hackers.

Selon Le Canard Enchainé, ils ont réussi à percer une faille du système informatique et se sont emparés des données personnelles, (identité, adresse électronique, numéro de téléphone, mot de passe) des 58 599 usagers inscrits sur le site.

A la Ville de Paris, l'informatique c'est vraiment façile !

Des informations "non confidentielles" selon la mairie. D'après l'hebdomadaire, la Ville aurait tenté dans un premier temps "camoufler l'incident" et n'a pas alerté tout de suite ses internautes (Ndr: C'est pourtant pas le genre de la maison) !. Elle a tout d'abord mis son site Internet en quarantaine en diffusant ce message : "Le site 'plan.paris.fr' est hélas indisponible. Il se refait une beauté, caché dans les laboratoires techniques pour quelques semaines". Ce n'est qu'après plusieurs coups de fil du journal, le 20 août que l'Hôtel de Ville a prévenu les internautes de cette fuite, comme l'exige une ordonnance d'août 2011 en cas d'intrusion dans des données informatiques.

"Nous n'avons pas attendu l'appel du Canard Enchaîné pour réagir, rétorque t-on à la Ville de Paris. Il était nécessaire de relever les niveaux de sécurité et de cryptage avant d'avertir nos inscrits qu'ils devaient changer leur mot de passe." Une intrusion "bénigne" selon la mairie de Paris car elle n'a "potentiellement concerné que des adresses mail qui ne contenaient aucune information confidentielle". "Ce site était le plus ancien que nous avions développé, conclut la Ville de Paris. Il n'y a aujourd'hui plus de faille." (NdR: Comme dans les bibliothèques alors ? Lire là)

C'est bon, on a pénetré le système de la Ville de Paris

"On compte une centaine d'intrusions par jour". Selon, Jérémie Zimmermann, ingénieur-consultant en technologies collaboratives, "la plupart des entreprises et services publics n'ont pas connaissance de la loi Informatique et Libertés qui stipule qu'il faut alerter "par tout moyen" les usagers victimes d'intrusion". D'après le spécialiste, "on compte une centaine d'intrusions par jour et la politique de sécurité des données personnelles est loin d'être prise au sérieux".

Pas assez vigilants, les utilisateurs sont aussi fautifs. "90 % de la population utilise le même mot de passe sur différents sites, poursuit Jérémie Zimmermann, ce qui facilite l'intrusion permanente des robots sur les réseaux informatiques". La collecte d'adresses mails peut servir à de nombreuses pratiques : Spam, usurpation d'identité, services d'envoi de mails depuis la Chine...

DOCUMENT 2

Réseau informatique :En quoi consiste un audit de sécurité ?

réseau-informatique.prestataire.com - consulté le 12 décembre 2014

Inspecter les procédures de sécurité. C'est le rôle de l'audit de sécurité dans une entreprise, avant de mettre en œuvre toutes les mesures de protection.

Présentation

Un audit de la sécurité du réseau consiste à confier à un prestataire indépendant l'analyse des politiques de sécurité mises en place dans l'entreprise afin d'en valider la conformité et l'efficacité. Le prestataire peut être une société de services informatiques ou un auditeur freelance. L'auditeur dresse un rapport dans lequel il livre une cartographie de la sécurité du réseau et ses recommandations pour combler les failles répertoriées.

Objectifs

L'audit de sécurité du réseau consiste globalement à évaluer la sécurité du réseau informatique ainsi que les risques potentiels auxquels s'expose l'entreprise. Au-delà de préserver la performance et l'efficacité, l'audit de sécurité vise à valider les mesures prises par l'entreprise pour se protéger, elle et son activité. En ce sens, l'audit de sécurité du réseau informatique s'inscrit dans une démarche de gouvernance du SI.

Démarche

Pour atteindre ces objectifs, l'audit de sécurité doit valider les étapes suivantes :

- vérifier la conformité des politiques de sécurité,
- vérifier que les règles des politiques de sécurité sont bien appliquées,
- contrer une attaque,
- établir une liste des vulnérabilités du réseau,
- tester une nouvelle infrastructure, un équipement ou une nouvelle technologie.

Méthode

L'audit de sécurité repose sur le contrôle et l'analyse des comportements, des outils de sécurité en place et des politiques de sécurité. La réalisation d'un audit de sécurité du réseau informatique consiste à s'appuyer sur des outils, des mesures et des relevés effectués par l'auditeur. La démarche comprend notamment :

- des entretiens des DSI et utilisateurs,
- des relevés et des mesures des outils en place,
- l'audit du code et des protocoles qui animent le réseau,
- la détection d'intrusion.

Outils

Outre des moyens techniques (sondes, logiciels de détection d'intrusion), l'audit de sécurité du réseau informatique s'appuie sur des méthodes rigoureuses qui dictent les étapes à suivre pour évaluer les risques. Ces méthodes s'inscrivent dans des plans de gouvernance du SI. Parmi ces méthodes d'audit de sécurité du réseau informatique, citons :

- Ebios,
- COBIT,
- Marion,
- Mehari,
- Feros.

DOCUMENT 3

Réaliser un audit de vos systèmes informatiques

Pour évaluer et améliorer la disponibilité de votre infrastructure système

Avec l'importance croissante des systèmes d'information dans la production des entreprises, la fiabilité et la gestion des performances de vos systèmes informatiques deviennent des paramètres important de votre compétitivité.

Vos systèmes sont-ils performants ? Quels sont les risques de panne que vous encourez ? Votre infrastructure est-elle bien conçue et dimensionné pour répondre à vos besoins actuels ? et futurs ? Comment l'améliorer ? Quelles conséquences une panne aurait-t-elle sur votre production ?

Présentation

L'audit système a pour objectif à la fois **d'évaluer** la disponibilité et les performances de votre infrastructure, et de déterminer quelles **améliorations** peuvent être mises en oeuvre afin de les renforcer. La démarche d'audit appliquée par Acipia porte à la fois sur les **aspects techniques,** et sur les **aspects humains et organisationnels**. Selon vos besoins et selon le périmètre à auditer, nous mettons en oeuvre les outils et les ressources adaptées afin de **collecter les informations** nécessaires (entretien, expertise technique, supervision, test de charge, test de panne, documentation, etc ...). Ces informations sont ensuite confrontées à **l'état de l'art** en matière d'infrastructure système, et analysées par nos ingénieurs afin de connaître les **risques** réellement encourus et les **impacts** d'une défaillance sur la production de votre société.

La prestation d'audit est conrétisée par un rapport. Ce document présente les **observations** et les analyses effectuées durant l'audit, en précisant et en expliquant les **risques détectés**. Dans un deuxième temps, le rapport détaille les **préconisations** et les projets qui permettent d'**améliorer vos systèmes**. Quand cela est pertinent, des architectures cibles sont éventuellement proposées. Le rapport peut ainsi servir de base à la rédaction d'un cahier des charges. Les préconisations sont classées selon le gain en sécurité qu'elles apportent à l'infrastructure. Leurs impacts sur les aspects financiers et humains sont évalués, et sont pris en compte dans l'élaboration du plan d'action général, visant à les mettre en oeuvre. Les conclusions sont généralement présentés à la direction générale et à la direction informatique lors d'une **soutenance.**

Bénéfices

- Connaissance des risques réellement encourus par votre architecture
- Connaissance des impacts potentiels pour votre production en cas d'incident
- Élaboration du plan d'action pour l'amélioration de l'infrastructure (dans l'immédiat, à moyen terme et à long terme)
- Évaluation des impacts financiers et humains de chaque projet
- Adéquation des choix avec vos besoins et votre budget
- Transfert de compétences entre vos équipes et les nôtres

Domaine de compétence Infrastructure système

Besoin

Évaluer et améliorer votre infrastructure

Autres articles susceptibles de vous intéresser Audit réseau, audit sécurité

Pour plus d'informations, contactez nous via notre formulaire de contact ou au 03.20.28.61.62

DOCUMENT 4

Audit général de sécurité

société Lynx Technologies - édité le 12 décembre 2014

L'objectif d'un audit général de sécurité est d'établir un état des lieux complet et objectif du niveau actuel de sécurité de l'ensemble du système d'information tant sur les plans organisationnel et procédural que technologique.

La méthode et l'expérience

Pour mener à bien ce type de mission, Lynx Technologies applique une méthodologie d'audit et d'analyse de risques, mise au point au cours de nombreuses prestations réalisées sur ce thème.

Cette méthodologie synthétise les méthodes connues (Marion, Méhari, Mélissa, Ebios, Ersi, etc.) et intègre les recommandations de la norme ISO 17799.

Elle se base sur l'étude de documents, l'interview des acteurs désignés, la vérification sur place des éléments communiqués, l'analyse des composants de l'architecture informatique, etc...

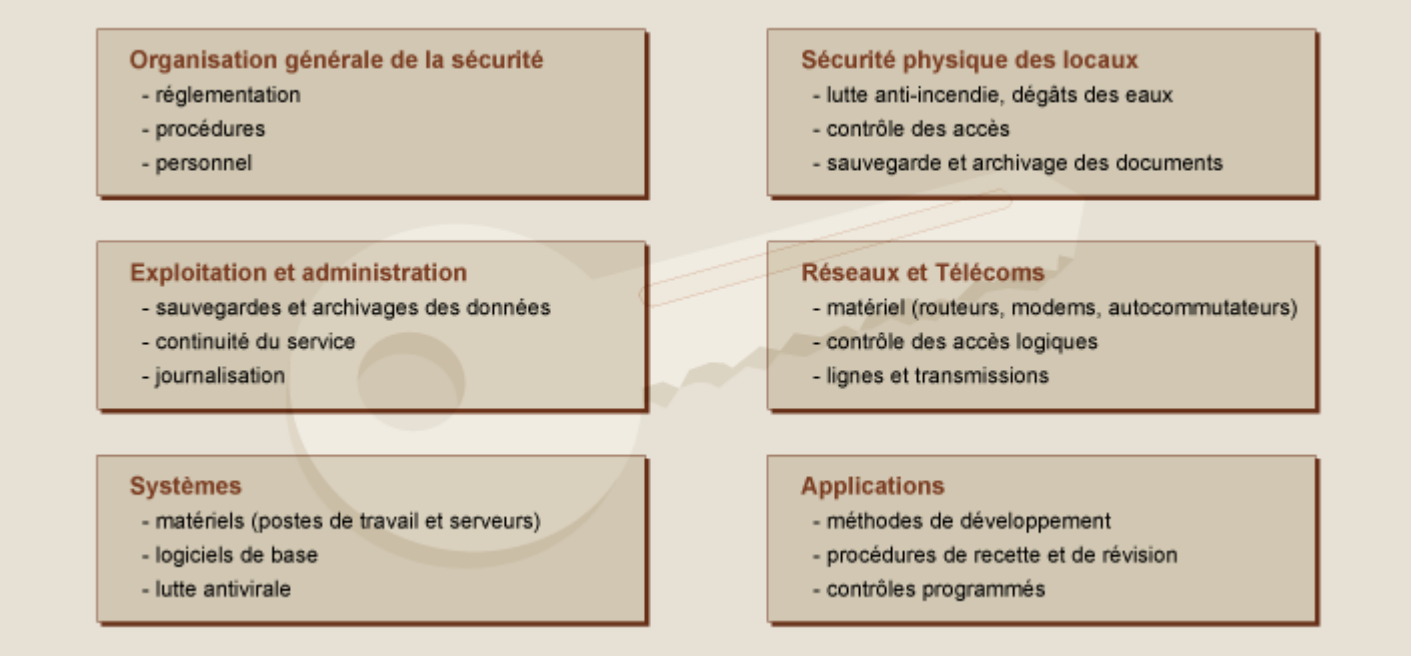
Etape 1 : Formalisation des exigences de sécurité et évaluation des impacts d'un sinistre

Les exigences de sécurité sont la synthèse des avis formulés par chacun des collaborateurs du client impliqués dans cet audit.

Par ailleurs, une estimation des impacts d'un sinistre pouvant survenir sur tout ou partie des ressources est effectuée au cours d'entretiens avec les responsables fonctionnels.

Etape 2 : Etat des lieux de la sécurité du système d'information

Les audits généraux de sécurité réalisés par Lynx Technologies couvrent notamment les domaines suivants :



L'évaluation du niveau de sécurité s'établit à partir :

- d'entretiens avec les principaux responsables de domaines, sur la base d'un questionnaire établi spécifiquement.
- de vérifications de la configuration et du paramétrage des différents équipements composant l'architecture informatique (audit technique).

Etape 3 : Analyse des risques

De manière synthétique, la méthode appliquée permet de mesurer l'impact de sinistres sur les ressources en termes de Disponibilité, Confidentialité et Intégrité.

Les vulnérabilités identifiées lors des précédentes étapes seront rapprochées des menaces pouvant survenir dans le contexte technique et fonctionnel, objet de l'audit.

Etape 4 : Recommandations et plan d'actions

Les recommandations formulées par Lynx Technologies visent à corriger les lacunes et vulnérabilités des dispositifs actuels de protection (organisation, procédures, architecture technique, systèmes, etc.).

Cette étape permet de disposer de tous les éléments techniques, financiers et opérationnels nécessaires au renforcement du niveau de sécurité du système d'information.

A l'issue de la mission, Lynx Technologies présente ses résultats et conclusions à deux niveaux :

- **Au niveau technique :** présentation des principales opérations réalisées et des mesures à mettre en œuvre :

- **Au niveau Direction :** présentation de la synthèse de la mission avec pour objectif de sensibiliser sur les **risques** potentiels et les mesures à mettre en œuvre face aux enjeux de l'entreprise.

Audit de configuration

Les audits de configuration permettent d'expertiser l'architecture technique déployée et de mesurer la conformité des configurations des éléments qui la composent (serveurs, bases de données, équipements réseau, pare-feu, autocommutateurs privés, etc.) avec la politique de sécurité définie et les règles de l'art en la matière. Ils en exposent les points faibles de l'architecture et se concentrent sur les actions à entreprendre pour mettre en œuvre un processus de sécurisation par couche.

La démarche

Les audits de configuration sont intrinsèquement fonction de la nature du composant ou de l'architecture à analyser. Lorsqu'ils ciblent des applicatifs ou des systèmes (serveurs, équipements réseaux, etc.), ils requièrent un accès total qui permettra soit d'analyser la configuration manuellement soit d'exécuter un script automatisant la collecte des informations pertinentes. Lorsqu'ils ciblent des composants dont la fonction même est partie prenante dans une architecture (pare-feu, architectures Web 3 tiers, architectures de courrier électronique, …), les audits nécessitent d'analyser l'ensemble des parties concernées (architecture réseau et politique de filtrage pour les pare-feu par exemple).

La réalisation d'un audit est par nature non destructrice (contrairement à certaines étapes d'un test d'intrusion). Ainsi, elle ne vise pas à confirmer l'existence de vulnérabilités ou les possibilités d'exploitation subséquentes mais s'intéresse à présenter les points faibles d'un système ou d'une architecture et les actions permettant d'y remédier.

Les résultats : rapports d'audit de configuration

Pour chaque composant audité, un rapport détaillé d'audit de configuration est réalisé. Ce rapport présente tout d'abord les résultats de l'audit puis les mesures à mettre en œuvre pour corriger ou atténuer les failles identifiées.
Sont ensuite détaillées, sous forme de fiches et pour chaque vulnérabilité décelée pendant l'audit, les recommandations à mettre en œuvre. Ces fiches exposent d'une part la description de la vulnérabilité et l'action corrective à réaliser et d'autre part des indicateurs spécifiques quant à la réalisation attendue : priorité de mise en œuvre, charge de réalisation, etc.

Audit de Code

Souvent plus par méconnaissance des risques que par malveillance, les développeurs introduisent des vulnérabilités dans les applications qu'ils développent. Tant que ces applications restent utilisables à l'intérieur de l'entreprise, les risques engendrés peuvent être considérés comme mineurs.

Mais aujourd'hui, beaucoup de développements sont réalisés pour permettre d'étendre, via des connexions externes, le système d'information de l'entreprise vers ses clients et ses fournisseurs, introduisant au sein même des applications des risques nouveaux liés au codage des programmes.

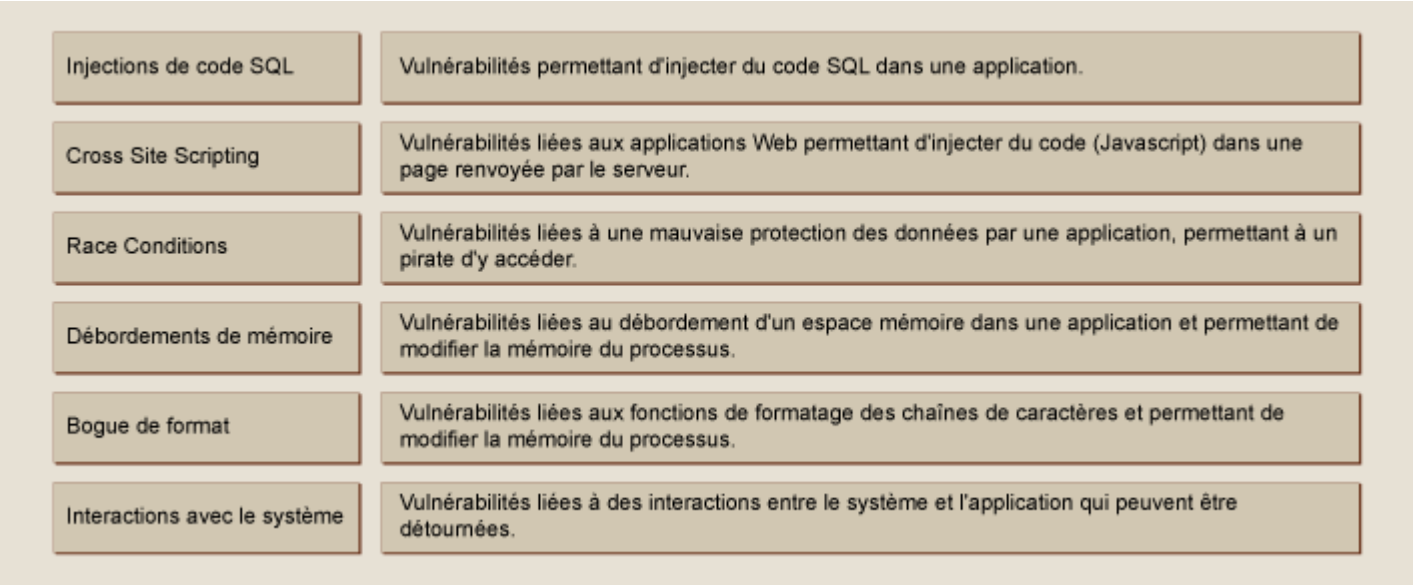
Pour couvrir ces risques, il est important de suivre une démarche qui prenne en compte la sécurité depuis la phase de spécification jusqu'à la phase de validation (recette).

Cette démarche d'intégration de la sécurité dans les méthodes de développement doit prévoir l'audit du code source de l'application pour identifier les vulnérabilités indécelables au cours d'une recette fonctionnelle.

L'audit consiste donc à :

- analyser le code source de l'application à la recherche de vulnérabilités,
- caractériser les vulnérabilités identifiées,
- formuler des recommandations afin de corriger le code et rendre ainsi l'application plus sécurisée.

Exemples de vulnérabilités recherchées :



Bien que cette prestation soit le plus souvent demandée pour des applications Web compte tenu des risques inhérents à ce type d'application, Lynx Technologies propose également des audits de code pour des applications non Web (application sensible client/serveur par exemple).

Audit de la gestion des habilitations

La notion d'entreprise étendue implique aujourd'hui que les ressources du système d'information soient connectées, disponibles et accessibles aux seules personnes habilitées, qu'elles soient à l'intérieur ou à l'extérieur du périmètre de confiance.

Ces évolutions ont ainsi poussé les entreprises à renforcer leur modèle de sécurité tant au niveau de l'infrastructure technique (et équipements sous-jacents) qu'au niveau des mécanismes de gestion de l'identité (**Identity Management**).

Une gestion des identités et des accès maîtrisés permet d'une part, de renforcer la politique de sécurité de l'entreprise et d'autre part, d'être en conformité avec les textes de loi récents tels que SOX (Sarbanes-OXley) et la LSF (loi de Sécurité Financières).

Démarche préconisée par Lynx Technologies

Dans un contexte aussi évolutif (passage de la gestion des droits d'accès à la gestion des identités numériques), Lynx Technologies préconise une approche pragmatique afin d'analyser toute la problématique de gestion des habilitations, concernant les accès aux ressources systèmes ou applicatives et impliquant des utilisateurs internes ou externes à l'entreprise.

Ainsi, les comptes et les droits fantômes seront détectés, les actions de fraude seront rendues plus difficile et la détection des actes malicieux sera facilitée.
Pour atteindre ces objectifs, Lynx Technologies audite l'ensemble des accès (ou habilitations) des différentes populations d'utilisateurs sur les ressources du système d'information de l'entreprise.

Les investigations menées par Lynx Technologies permettent de vérifier :

- **Sur le plan organisationnel :**
  - la définition et cohérence des profils définis au niveau des ressources ciblées (applications, systèmes, composants réseaux, ...) ;
  - les modalités d'attribution de ces profils (qui établit la demande ? qui la valide ? qui la traite ? qui la contrôle ?) ;

- la cohérence entre la base d'habilitations et les utilisateurs autorisés (les identités stockés au niveau du ou des référentiels) à intervenir, et les moyens de la contrôler périodiquement ;
- la traçabilité des actes d'habilitation et des actions entreprises par les utilisateurs (piste d'**Audit**) ;

Sur le plan sécurité :

- les **Autorisations** à travers les permissions sur les fichiers et les répertoires en fonction des profils attribués (accès aux données sensibles, mécanismes de conservation, journalisation, etc.) ;
- la vulnérabilité et la complexité des référentiels existants (annuaires, bases de compte, …..) ;
- les mécanismes utilisés (**Authentification** des utilisateurs, confidentialité des échanges, …) ;
- l'interopérabilité des plates-formes (systèmes, annuaires, BdD, ..) ;
- les risques liés à la localisation des bases de données et leurs interactions avec les autres composants de l'architecture applicative,
- les risques liés à la propagation de l'identité (cookies, requêtes, formulaires, etc.),
- etc.

Audit de la politique antivirale

Les virus informatiques constituent aujourd'hui une menace quotidienne pouvant entraîner des dégâts rapides et considérables sur tout système d'information. Pour pallier à cette menace, la définition et l'implémentation d'une politique de lutte antivirale doivent s'inscrire au sein de la politique globale de sécurité. Les audits de politique antivirale permettent d'expertiser l'architecture technique déployée et de mesurer la conformité des procédures en vigueur.

Démarche

La méthodologie d'audit et d'analyse de risque d'une politique de lutte antivirale a pour objectif de déterminer le niveau de protection du Système d'Information à la fois sur les plans organisationnel, procédural et technique :

- L'audit organisationnel permet de vérifier que des processus indispensables comme l'existence d'une charte d'utilisation et d'un plan de sensibilisation des utilisateurs sont mis en œuvre.
- L'audit procédural consiste à vérifier, par une analyse documentaire et des entretiens, si l'intégration de l'infrastructure de lutte antivirale au sein du système d'information répond théoriquement aux règles de sécurité (cloisonnement, contrôle des flux, détection antivirale, complémentarité des logiciels utilisés, etc.).
- L'audit technique de la stratégie antivirale porte sur certains points essentiels tels que le paramétrage des suites logicielles employées (reconnaissance de virus, mise en quarantaine, détection de virus, alertes, etc.) et la vérification des mises à jour (notamment pour les postes clients distants et les postes *nomades*).

Livrables

L'analyse de la politique de lutte antivirale existante (charte, architectures, plans de sensibilisation, etc.) et de son implémentation au sein du SI (infrastructures déployées, mises à jour des composants, mises à jour des signatures, etc.) conduit à la production d'un rapport d'audit qui comprend notamment :

- Une évaluation " points forts / points faibles " de la politique et de son implémentation.
- Un plan d'actions à différents niveaux de priorité fournissant les recommandations à mettre en œuvre.

Audit des infrastructures sans-fil (wifi) et mobilité

Les réseaux sans fils basés sur les **normes 802.11** connaissent actuellement un fort engouement autant pour les entreprises que pour les particuliers. D'une part, le besoin en mobilité est de plus en plus fort et d'autre part les investissements nécessaires sont sans commune mesure avec les projets de 3ème génération des opérateurs de téléphonie mobile. Les équipements sont bon marché, l'installation et l'administration aisées, les débits intéressants. Le seul frein à l'expansion de cette technologie reste la **sécurité**. Pourquoi ?

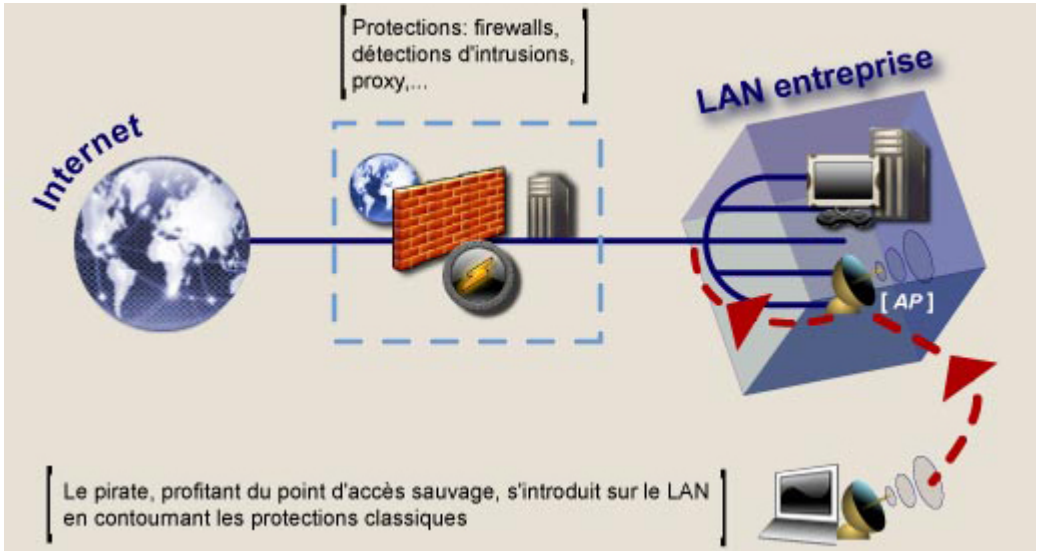
- **L'écoute passive** est facile.
- **Le WEP** (le protocole de sécurité de la norme) comporte des failles.
- **La publicité** autour de ces réseaux entraîne l'intérêt de tous : universitaires, chercheurs, hackers.

Wi-Fi : quelques scénarios de menaces

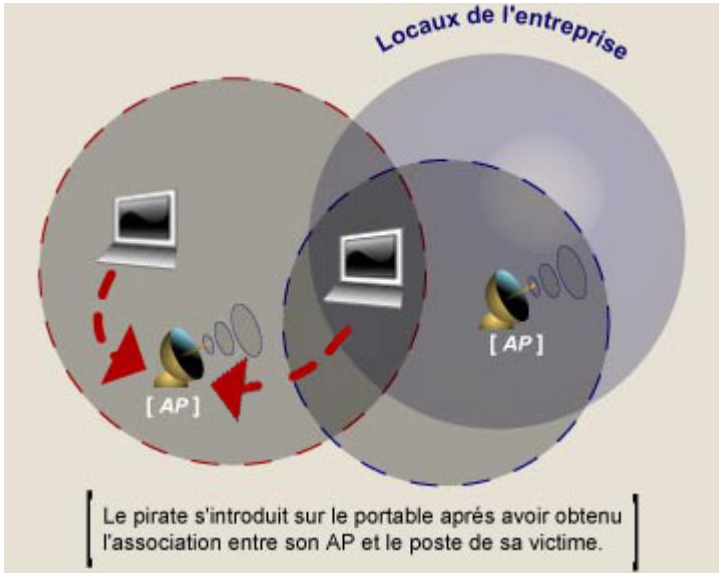
Les réseaux Wi-Fi basés sur les normes 802.11 constituent des architectures de type LAN radio partagé, soit en mode infrastructure (tout le trafic passe par un nœud central appelé AP pour access point), soit en mode ad hoc(communication directe de poste à poste).

Les menaces pesant sur ces architectures sont multiples, en voici quelques exemples :

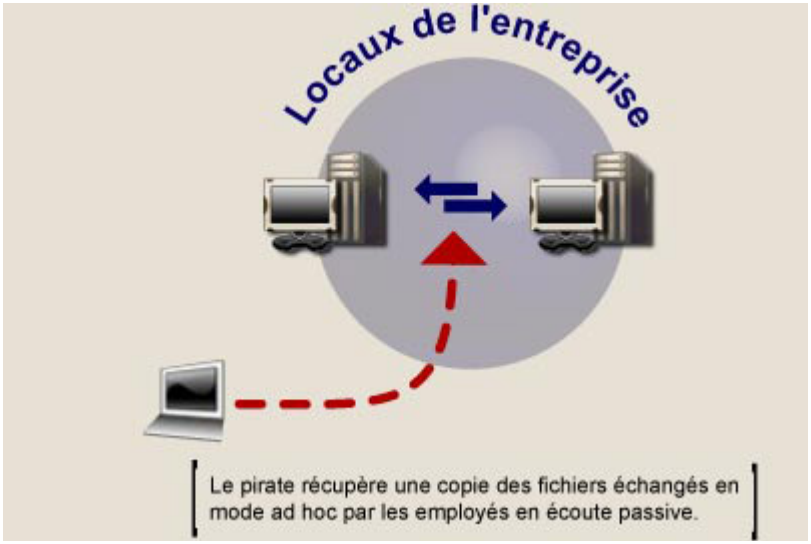
- **L'AP sauvage** : un employé prend l'initiative d'installer un point d'accès et de le relier au réseau filaire du réseau de son entreprise.



L'attaque " man in the middle " : un pirate place un point d'accès à proximité des salles de réunion de l'entreprise en espérant qu'un client viennent " s'associer " involontairement avec l'AP pirate (en bleu) à la place de l'AP de l'entreprise.



- **L'écoute passive** : deux employés échangent des fichiers en mode ad hoc.



- **Le double attachement** : un employé utilise son portable professionnel pour se connecter à son point d'accès domestique. Le pirate s'associe avec ce point d'accès et parvient à récupérer des informations sensibles stockées sur le disque dur de la victime pendant que celui-ci est connecté.

Wi-Fi : les failles de sécurité de la norme

La norme 802.11 prévoit un protocole de sécurité : le WEP (Wired Equivalent Privacy). Malheureusement, ce protocole comporte des failles importantes :

- **confidentialité des données** : l'algorithme RC4 est employé avec une initialisation constituée d'un vecteur d'initialisation de 24 bits (changeant à chaque trame et envoyé en clair) et d'une clé secrète partagée par les AP et les postes (40 ou 108 bits). Plusieurs attaques ont été publiées. La plus spectaculaire et médiatisée est l'attaque dite des IV faibles qui remonte à la clé secrète après une écoute passive variant de la demi-heure à quelques heures à l'aide de logiciels téléchargeables sur Internet.
- **authentification des utilisateurs** : le mécanisme d'envoi de challenges-réponses chiffrés par le WEP ne doit pas être utilisé à cause des attaques " clair-chiffré " qu'il rend possible.
- **intégrité des données** : le code CRC32 linéaire et donc réversible n'est guère adapté pour assurer cette fonctionnalité de sécurité.

Wi-Fi : l'approche de LYNX TECHNOLOGIES

Sécuriser une infrastructure Wi-Fi n'est pas chose facile :

- Les technologies radio sont souvent mal maîtrisées dans les entreprises,
- La succession des barrières de sécurité est lourde à gérer autant pour les administrateurs que les utilisateurs.

LYNX TECHNOLOGIES possède une forte expertise en matière de sécurité des systèmes d'information et une solide expérience du Wi-Fi. Nous sommes en effet en mesure de proposer nos services aussi bien dans le choix que dans la qualification et l'audit d'une architecture sans fil.
Notre expertise sur les architectures sans fils couvre les aspects suivants :

- **Définition et mise en œuvre d'architectures Wi-Fi sécurisées :**
  - radio (où placer les points d'accès, paramétrages, …),
  - configuration des points d'accès (trames de synchronisation, filtrage des adresses MAC, mise à jour des firmwares, …),
  - réseau (cloisonnement des sous-réseaux filaire et radio, utilisation du DHCP, utilisation des IDS sur le LAN, règles de firewall, …),
  - solutions (IPsec, SSL, authentification par serveur Radius, déploiement de PKI, Kerberos, EAP-SIM, …), etc.

- **Audits (détermination du niveau de confidentialité et de sécurité)**
  - tests d'intrusion externes (attaques clients et AP pirates) et internes (en radio et à partir du réseau filaire des points d'accès),
  - audit de configuration des composants de l'infrastructure.

- **Organisation :**
  - rédaction des normes et usages des équipements sans fil au sein de la politique de sécurité de l'entreprise.
  - sensibilisation des utilisateurs...

Les tests d'intrusion

Les tests d'intrusion permettent de " mettre à l'épreuve la sécurité d'un environnement et de qualifier sa résistance à un certain niveau d'attaque " [source : Clusif]. Cette prestation à forte composante technique, ponctuelle ou récurrente, est réalisée après autorisation explicite du client et se fonde sur un ensemble de moyens mis en œuvre pour compromettre un système d'information (soit en se rendant maître du cœur du système, soit en s'emparant du plus grand nombre de ressources) en contournant les dispositifs de sécurité.

L'objectif d'un test d'intrusion n'est pas d'identifier de manière exhaustive l'ensemble des vulnérabilités d'un système ni d'apporter la preuve qu'un système est sécurisé (dès lors qu'aucune vulnérabilité significative n'aurait été mise en évidence lors du test). Le test d'intrusion fige à un instant déterminé le niveau de sécurité d'un système d'information en démontrant ce qu'un profil d'attaquant particulier est capable de faire sur un point d'accès déterminé. Réalisés de manière récurrente, les tests d'intrusion permettent de valider périodiquement le niveau de sécurité du système d'information et d'en mesurer les variations.

La démarche

La démarche suivie pour réaliser un test d'intrusion s'articule autour de trois principes :

- La convention : tout test d'intrusion se limite à un périmètre défini (équipements, serveurs, applications), est borné dans le temps (la durée des tests étant dépendante du type de scénario, du point d'accès et des ressources ciblées) et doit être réalisé dans le respect des règles de déontologie et d'éthique [1].

- Le type de scénario :
  - les scénarii dits en aveugle (ou boîte noire) sont réalisés sans connaissance préalable et dans des conditions analogues à celles dont disposerait un éventuel attaquant ;
  - les scénarii avec connaissance partielle (ou boîte grise) sont réalisés avec des informations communiquées par le client dans des conditions analogues à celle dont disposent des partenaires, des prestataires, etc.

- Le point d'accès : qu'il soit externe ou interne, le ou les points d'accès peuvent être la connexion Internet du système d'information, l'infrastructure Wi-Fi, l'infrastructure téléphonique, etc.

Le déroulement du test d'intrusion se décompose en trois phases :

- la phase de collecte d'informations " publiques " (ou *phase passive*) : cette phase consiste, sans interagir avec l'environnement cible, à rassembler des informations disponibles

publiquement ;

- la phase de cartographie de l'environnement cible (ou *approche active*) : cette phase consiste à localiser et caractériser les composants cibles (systèmes d'exploitation et services applicatifs, positionnement des équipements les uns par rapport aux autres, types de dispositifs de sécurité mis en œuvre, etc.)
- les tentatives d'intrusion : cette phase, à forte composante technique, consiste à exploiter les vulnérabilités mises en évidence dans les phases précédentes de façon à obtenir un accès " non autorisé " aux ressources et/ou au cœur du système d'information.

Afin d'assurer le maintien en conditions opérationnelles du périmètre testé, un contact permanent avec le client est assuré et des points de suivi à intervalle régulier sont accomplis tout au long du test d'intrusion.

Les résultats

Les tests d'intrusion donnent lieu à la rédaction d'un rapport technique et d'une note de synthèse.

La note de synthèse, principalement destinée à la direction informatique, présente un constat du niveau de sécurité mesuré, les conséquences qui découlent des insuffisances constatées et les préconisations dont la forte priorité indique qu'elles sont à prendre en compte dans les plus brefs délais.

Le rapport technique expose un descriptif des actions ayant permis d'identifier les failles, l'exploitation de ces failles, les conséquences de ces exploitations et l'ensemble des recommandations à prendre en compte pour améliorer le niveau de sécurité du système d'information.

[1] Lynx Technologies, membre du CLUSIF, adhère au code éthique des métiers de la sécurité des Systèmes d'Information et applique, pour les audits de vulnérabilités, un cadre réglementaire très strict décrit dans son code de déontologie.

Audit de plan de continuité des activités

Problématique sous-tendue / Objectif sécuritaire visé

Quelle que soit la qualité du processus de maintien en conditions opérationnelles du Plan de Continuité des Activités mis en place par l'entreprise, il importe qu'un diagnostic soit régulièrement réalisé quant :

- à l'adéquation des solutions de secours mises en oeuvre à l'égard des objectifs fixés par la Direction Générale et des exigences exprimées par les Métiers ;
- au caractère effectif du processus de maintien à niveau du plan dans la durée.

L'audit doit ainsi permettre d'apporter une réponse à deux questions essentielles :

- les activités critiques de l'entreprise sont elles actuellement correctement prises en considération ?
- l'ensemble du dispositif de secours actuel est-il validé par des tests satisfaisants ?

Démarche préconisée par Lynx Technologies

L'étude est conduite en se référant aux règles et bonnes pratiques généralement admises en matière d'élaboration et de mise en oeuvre de Plans de Continuité des Activités. Une attention particulière est portée aux thématiques majeures suivantes :

- organisation de l'entreprise à l'égard de la gestion de crise ;
- niveau de formalisation du plan et de complétude des procédures, tant techniques que fonctionnelles ;
- qualité et efficacité du dispositif de maintien en conditions opérationnelles.

L'approche déroule les étapes classiques d'une mission d'audit, à savoir :

- Analyse du corpus documentaire relatif au plan (exhaustivité, cohérence, conditions de mise à jour, ...) ;
- Conduite d'entretiens avec les différents acteurs concernés (Direction Générale, responsables techniques et métiers, responsable du Plan) sur la base de questionnaires spécifiques :
  - Sensibilisation / maturité à l'égard de la problématique ;
  - Connaissance et niveau de formation aux rôles attribués ;
  - Implication dans le processus de maintien à niveau du plan.
- Contrôle de certains aspects clés du dispositif de maintien en conditions opérationnelles :
  - Qualité du plan de sauvegarde de recours ;

- Intégration d'un volet " Plan de continuité " dans le processus de développement de systèmes d'information ou de déploiement d'architectures de production ;
- Vérifications organisationnelles ponctuelles (listes, check-list, …) ;
- Etc.

Résultats fournis

Un rapport d'audit est produit à l'issue de l'étude. Chaque aspect abordé lors des investigations donne lieu à une évaluation " points forts / points faibles ". Les résultats sont consolidés fournissant une réponse objective, quantifiée et justifiable aux attentes formulées dans la lettre de mission.

Le rapport comprend notamment :

- Un avis sur l'adéquation du plan aux exigences de continuité des Métiers ;
- Un jugement sur l'exhaustivité du contenu du plan ;
- Un bilan sur le caractère opérationnel effectif des dispositifs prévus ;
- Un plan d'actions à différents niveaux de priorité.

DOCUMENT 5

CAHIER DES CHARGES

AUDIT

DU SYSTEME D'INFORMATION

Ville de la Verrière - 2009-2010

Présentation Générale

Introduction

Le présent document constitue le Cahier des Charges de la Commune de La Verrière pour l'audit du Système d'Information.

Ce document présente tout d'abord une vue générale de l'architecture informatique, ensuite les attentes de la Commune de La Verrière dans le cadre de cet audit et enfin les clauses administratives et juridiques.

Le pouvoir adjudicateur de la présente consultation est M. Pierre SELLINCOURT, Maire de la Commune de La Verrière

Le choix du candidat est prévu pendant la 2ème quinzaine du mois de février 2010, dans la perspective d'un démarrage de l'audit le 1er mars 2010.

ARCHITECTURE INFORMATIQUE

- Serveur BULL Express 5800- 120 RH2.(EXPRESS) - *800185680093*
- Serveur Windows serveur 2003 avec base Oracle

- Serveur BULL NAS PRO 600 APPLIANCE RNR.(BULLNAS2) - *800185690092*
- Serveur Windows Storage serveur 2003

- Libraire de Sauvegarde NEO2000, 1 IBM-LTO-2 DRIVE (LVD), 30 SLOTS, RM - *2B70400058*

- Serveur BULL ESCALA NODE PL250R+ (ESCALA) - *XDU-6D6-065CA0G*

- Onduleur BULL RACK 36U (BLACK) WITH ONE PDU - *XDU-T00-6509C8C*

- Proxy (EQUIBOX) – serveur de messagerie – antivirus – antispam - serveur fichier

- Serveur VMWARE HP Proliant ML350 G5

- Serveur BULLNAS (ordinateur configuré avec windows XP)
- Serveur Windows XP hébergeant les applications avec base Oracle

- Réseau 100 Base T (câble et switch) (*annexe 1*)

- Connexion Fibre Optique (*annexe 2*)

- Postes clients (une cinquantaine)

Nature de la mission et Rapport d'Audit

Objet :

La Commune de La Verrière confie au soumissionnaire qui l'accepte, le soin d'assurer un audit complet des systèmes d'information de la Commune de La Verrière suivi de préconisations pour son évolution.
Il tiendra la Commune de La Verrière informée de l'avancement et du bon déroulement de sa mission et lui remettra un rapport d'audit.

Nature de la mission :

Le soumissionnaire se chargera, en partenariat avec le service informatique, de délimiter les besoins et d'analyser le système d'information de la Commune de La Verrière.
Un diagnostic exhaustif au vu des documentations fournies sera établi et remis à la Commune de La Verrière.
L'opération d'audit du système d'information de la Commune de La Verrière prendra notamment en compte les éléments suivants :

1- Etude et diagnostic de l'architecture globale du système d'information avec l'examen des possibilités offertes pour l'utilisation des serveurs informatiques et par l'utilisation de serveurs propres ou extérieurs.

2- Evolution de la sécurité informatique, des serveurs et des postes de travail (Accès, sauvegardes, procédures, messagerie, plan de reprise d'activité, etc…), étude de la sécurité des accès distants (validation de l'existant, mise en évidence des faiblesses, renforcements possibles)

3- Appréciation de la qualité, de l'accès, de la disponibilité du réseau et des connexions internet.

4- Etude de la complémentarité des compétences au sein du service informatique

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

Le Rapport d'Audit :

Le soumissionnaire informera la Commune de La Verrière au fur et à mesure de l'avancement de sa mission, aux fins de faire valider par la Commune de La Verrière les constatations déjà effectuées.
Le rapport d'audit comprendra notamment un exposé de l'organisation actuelle des systèmes d'information de la Commune de La Verrière, ainsi qu'une analyse détaillée et chiffrée des choix techniques et matériels, en distinguant les solutions optimales, acceptables, et prioritaires avec une évaluation de leur efficacité.
Le rapport présentera les préconisations en matière d'évolution du système d'information avec comme objectif principal la rationalisation des équipements et la mise en place de technologies durables dans le cadre d'un budget contraint.
Ce rapport fera apparaître des comparaisons avec des collectivités similaires.

Pour l'accomplissement de cette mission, le soumissionnaire s'interdit de désigner une autre personne, de telle sorte que le présent marché ne pourra en aucun cas être transmis à un tiers, sauf accord exprès et préalable de la Commune de La Verrière.

Le rapport d'audit doit être communiqué au plus tard le 26 mars 2010.

Clauses Administratives et Juridiques

Responsabilité du soumissionnaire

En toute circonstance, le soumissionnaire reste seul responsable de l'organisation, de la réalisation et de la synthèse de la mission qui lui a été confiée par la Commune de La Verrière.

Interprétation et modification

Le présent marché exprime l'intégralité de l'accord entre les parties. Il remplace et annule tous les pourparlers, accords verbaux ou écrits pré-contractuels entre les parties.

Règlement des litiges

En cas de litige persistant, à défaut de transaction, les juridictions françaises sont seules compétentes pour régler les litiges.

Ceux-ci sont régis par les lois et règlements en vigueur en France.

Tout litige relatif à l'exécution du présent marché relève de la compétence du Tribunal Administratif de Versailles.

Rémunération du soumissionnaire :

En contrepartie de l'exécution de sa mission, le soumissionnaire percevra une rémunération forfaitaire qu'il chiffrera, correspondant à un nombre de jours/hommes, d'un montant en euro HT qui représente l'intégralité du coût de cette mission.

La facturation s'effectuera :

- A la remise du rapport d'audit en fonction des jours réellement passés,

Les conditions de paiement sont de 45 jours après la date de réception des factures par virement administratif.

Pièces constitutives du marché

Les pièces constitutives du marché sont les suivantes par ordre de priorité :
Pièces particulières
L'acte d'engagement et ses annexes éventuelles, dont l'exemplaire original conservé dans les archives de la personne publique fait seul foi ;
Le présent Cahier des Clauses Administratives Particulières et son annexe, dont l'exemplaire original conservé dans les archives du maître de l'ouvrage fait seul foi sans modification ;

Les factures sont adressées à l'adresse suivante :

MAIRIE DE LA VERRIERE
Avenue des NOES
78320 LA VERRIERE

Outre les mentions légales, les factures sont établies en un original et deux copies et doivent impérativement comporter les mentions suivantes, sous peine de rejet immédiat :

- le détail des prestations exécutées et livrées,
- le montant H.T. et T.T.C. des prestations exécutées,
- le taux et le montant de la T.V.A.

Résiliation

Cette résiliation s'opère conformément au chapitre V du Cahier des Clauses Administratives Générales Fournitures Courantes et Services.

Dans l'hypothèse où le titulaire disparaîtrait par fusion avec une autre société, il est précisé que la mise au point de l'avenant de transfert est subordonnée à la réception immédiate par l'exécutif du pouvoir adjudicateur des modifications énumérées à l'article 2.22 du Cahier des Clauses Administratives Générales Fournitures Courantes et Services complétés par l'acte portant la décision de fusion et la justification de son enregistrement légal.

A défaut, le pouvoir adjudicateur se réserve le droit de résilier le marché en application de l'article 28 du Cahier des Clauses Administratives Générales Fournitures Courantes et Services.

En cas d'inexactitude ou refus de produire les documents et renseignements mentionnés aux articles 44 et 46 du Code des Marchés Publics, le marché est résilié aux torts et aux frais et risques du titulaire, sans indemnités.

Redressement ou liquidation judiciaire

Par dérogation au CCAG FCS, les dispositions qui suivent sont applicables en cas de redressement judiciaire ou de liquidation judiciaire.

« Le jugement instituant le redressement ou la liquidation judiciaire est notifié immédiatement au pouvoir adjudicateur par le titulaire du marché. Il en va de même de tout jugement ou décision susceptible d'avoir un effet sur l'exécution du marché.

En cas de redressement judiciaire, le pouvoir adjudicateur adresse à l'administrateur une mise en demeure lui demandant s'il entend exiger l'exécution du marché.

Cette mise en demeure est adressée au titulaire dans le cas d'une procédure simplifiée sans administrateur si, en application de l'article 141 de la loi du 25 janvier 1985, le Juge-Commissaire a expressément autorisé celui-ci à exercer la faculté ouverte à l'article 37 de la loi. En cas de réponse négative ou en l'absence de réponse dans le délai d'un mois à compter de l'envoi de la mise en demeure, la résiliation du marché est prononcée.

Ce délai d'un mois peut être prolongé ou raccourci si, avant l'expiration dudit délai le Juge-Commissaire a accordé à l'administrateur une prolongation ou lui a imparti un délai plus court.

La résiliation prend effet à la date de la décision de l'administrateur ou du titulaire de renoncer à poursuivre l'exécution du marché ou à l'expiration du délai d'un mois ci-dessus. Elle n'ouvre droit, pour le titulaire, à aucune indemnité.
En cas de liquidation judiciaire, la résiliation du marché est prononcée sauf si le jugement autorise expressément le maintien de l'activité de l'Entreprise.

Confidentialité

Le soumissionnaire 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 la Commune de La Verrière, que l'exécution de leur mission les amènerait à connaître, sans que lesdites informations n'aient à être estampillées "confidentielles ".

Le soumissionnaire 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 la Commune de La Verrière lui-même.

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

Propriété du Rapport d'Audit

Il est expressément stipulé que le rapport d'audit établis par le soumissionnaire dans le cadre de sa mission est la propriété exclusive de la Commune de La Verrière

En aucun cas le présent marché n'emporte transfert du droit d'utiliser, de publier ou de reproduire, au profit du soumissionnaire les informations qui lui auront été communiquées par la Commune de La Verrière

Le soumissionnaire sera libre de faire état de son intervention auprès de la Commune de La Verrière dans ses références commerciales.

DOCUMENT 6

La sécurité informatique, une mission d'utilité publique ?

Tanguy de COATPONT – Les Experts – 7 avril 2013

62% des entreprises françaises déclarent avoir connu au moins un incident de sécurité en 2012.

La sécurité, et rien que la sécurité !

La sécurité sous toutes ses formes, est au coeur de la plupart des préoccupations des infrastructures publiques.
La sécurité physique des habitants est assurée par la police municipale, par le bon fonctionnement du réseau d'eau de la commune, la sécurité environnementale, par la préservation des espaces publics. Et ce ne sont là que quelques exemples des nombreuses responsabilités incombant aux différents services publics.

Pourtant, au sein de ces missions, il en est une, moins évidente, mais dont l'importance peut être cruciale, c'est la sécurité informatique ! Son caractère immatériel rend difficile pour les personnes non sensibilisées la prise de conscience des menaces réelles. Ce qui entraîne donc une sous-évaluation des risques de ce fait des moyens humains et techniques mis en œuvre pour y faire face.

Pourtant l'actualité relaie largement les incidents relatifs à la sécurité informatique : des sites publics sont victimes de malveillance, tant au sommet de l'État, avec les récentes attaques de l'Élysée ou du ministère de l'intérieur, que dans les communes. Récemment, la messagerie du premier adjoint de la mairie de Menton a été détournée pour tenter d'extorquer des fonds à ses contacts. Cet été, la mairie de Dieulefit a vu son site piraté par un groupe de hackers, comme la ville de Nanteuil-le-Haudouin, dans l'Oise.

Par ailleurs, fait désarmant, aucune obligation n'est faite, tant dans le public que le privé, de publier les attaques et les dommages subis. Au grand dam de l'ANSSI (Agence nationale de la sécurité des systèmes informatiques) qui milite activement dans ce sens, afin de permettre une prise de conscience généralisée du problème.

L'informatisation des services publics : un phénomène inéluctable

Cet état des lieux qui peut paraître alarmiste ne doit en aucun cas freiner les collectivités locales et les infrastructures publiques en général dans leur élan vers les technologies de l'information.

Les services publics doivent évoluer pour répondre aux modes d'accès à l'information actuel des citoyens : qu'il s'agisse de l'ouverture de services en ligne ou de la mise à disposition des données, ce sont aussi de nouvelles opportunités pour simplifier et accélérer les démarches administratives.

Cette ouverture vers l'internet a également changé l'approche nécessaire de la sécurité et la protection des données, puisqu'elle créé de nombreux ponts entre l'intérieur et l'extérieur.

Respecter une bonne hygiène informatique

Comme dans tous les secteurs d'activité, tous les métiers, en matière de sécurité informatique, il convient souvent de respecter des règles simples pour éviter une très grande majorité de risques.

La première règle à respecter est de mettre à jour systématiquement le ou les systèmes d'exploitation utilisés par l'infrastructure publique, ainsi que les logiciels. Les éditeurs publient régulièrement des « patches » de sécurité qui viennent combler des failles identifiées. Ces failles sont autant de portes laissées entrouvertes vers le réseau interne à destination des pirates.

De même, il convient d'installer une suite antivirus qu'il est impératif de mettre à jour régulièrement pour être certain de bénéficier d'une protection contre les derniers virus détectés … et les quelques millions déjà identifiés.

Ensuite, il faut se protéger des agents pathogènes venus de l'extérieur qui s'introduisent dans le système pour en éprouver l'immunité. Pour cela, ils utilisent plusieurs points d'entrée. Les périphériques de stockage en sont un. Ils semblent anodins, mais sont terriblement dangereux ! La clé USB, par exemple, est un vecteur important d'infection.

Il suffit qu'elle ait été utilisée, par exemple, dans une borne de développement de photos numériques, pour se trouver infectée par des dizaines de virus qui pourront ensuite être injectés dans le réseau informatique de l'établissement public.

Autre point d'entrée, le navigateur web. Les collaborateurs ne doivent jamais saisir de données personnelles sur des sites qui n'offrent pas toutes les garanties requises. Elles pourraient être utilisées à mauvais escient. À titre informatif, Google recense chaque jour 9500 nouveaux sites malveillants … La messagerie électronique peut, elle aussi, servir de porte cachée si le serveur de mail n'est pas correctement sécurisé.

Parmi les bonnes pratiques, on notera de ne jamais cliquer sur un lien d'un email demandant de s'authentifier, de même il est recommandé de ne pas ouvrir les pièces jointes se terminant par les extensions pif, bat, com, exe, ink.

Enfin, la gestion des mots de passe est cruciale : il faut impérativement les rendre complexes en combinant majuscules et chiffres. Et, il faut en utiliser un différent pour chaque usage et en changer régulièrement. L'idéal restant d'utiliser un logiciel de gestion de mots de passe qui simplifiera la démarche.

La sécurité informatique est certes un domaine complexe et anxiogène, mais elle peut être abordée à travers des solutions de plus en plus simples et en respectant quelques bonnes pratiques. Le plus compliqué finalement, c'est d'en prendre conscience …

Ville de Cahors CCAS

CHARTE INFORMATIQUE ET TELEPHONIQUE
Mairie de Cahors, Grand Cahors, CCAS, CIAS, EPIC Tourisme

Préambule :

La Ville de Cahors, son CCAS, le Grand Cahors, son CIAS et son EPIC Tourisme mettent en œuvre des systèmes d'information et de communication nécessaires à leurs activités, comprenant notamment des réseaux informatiques et téléphoniques.

Leurs utilisateurs, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens d'information et de communication mis à leur disposition et à les utiliser dans un cadre professionnel territorial.

L'utilisation des systèmes d'information et de communication doit en effet être exclusivement effectuée à des fins professionnelles territoriales, sauf exception particulière prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée des systèmes d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Les utilisateurs des systèmes d'information doivent en effet être sensibilisés aux risques liés à l'utilisation des outils informatiques. Cette sensibilisation est formalisée dans le présent document : une charte fixant les règles à respecter en matière de **sécurité** informatique et celles relatives au **bon usage** des outils d'information et de communication (ordinateurs, téléphones, Internet, messageries, etc.) mis à disposition des utilisateurs par leur administration. La charte informatique fixe les **droits et obligations** des utilisateurs des outils dédiés qui, sensibilisés sur les **comportements à observer** et les **dérives à éviter**, ne doivent pas porter atteinte à l'intérêt collectif.

Cette charte, approuvée par délibérations du Conseil municipal de la Ville de Cahors en date du ..., du Conseil communautaire du Grand Cahors en date du 18 Décembre 2012, des Conseils d'administration du CCAS de Cahors en date du ..., du CIAS du Grand Cahors en date du ... et du Comité de direction de l'EPIC Tourisme en date du ..., après avis des Comités Techniques Paritaires sera opposable, en tant qu'acte administratif règlementaire, à tous intéressés.

La charte informatique, définissant un cadre clair et transparent à valeur pédagogique, informative et normative, doit en effet être connue des utilisateurs, qui sont informés des modalités d'utilisation des outils mis à leur disposition par leur employeur et des **bonnes mœurs** qu'ils doivent respecter.