AUDIT DE LA SÉCURITÉ INFORMATIQUE ET L'INFRASTRUCTURE RÉSEAU

SOMMAIRE

A. OBJET DE LA CONSULTATION

L'objet de cette consultation est d'auditer La plate forme de sécurité informatique et l'infrastructure réseau des établissements liés à la Mairie de Saint-Genis-Laval. Les objectifs de la consultation sont déclinés comme suit :

- Évaluer le niveau d'infrastructure réseaux, télécoms et de sécurité´;
- Proposer les recommandations d'améliorations nécessaires ;
- Définir les architectures cibles qui seront en mesure de :
  - Mettre à niveau l'existant selon les nouveaux besoins et les règles de l'art,
  - Assurer et sécuriser les échanges à l'intérieur des réseaux LAN et au niveau du réseau VPN MPLS de la Mairie de Saint-Genis-Laval.
- Disposer d'une feuille de route pour la mise en œuvre des architectures cibles et des recommandations pour des projets d'optimisation de l'existant.

Cette consultation vise aussi à conseiller la ville dans la définition de la politique de sécurité.

B. PÉRIMÈTRE DE L'AUDIT

L'ensemble des établissements afférents à la Mairie de Saint-Genis-Laval, seront inclus dans le périmètre de l'étude. Ce périmètre couvre :

- Les établissements connectés via fibres optiques en centre ville, à savoir :
  - L'Hôtel de Ville et les services techniques,
  - La médiathèque B610,
  - Le théâtre de la Mouche.
- Les établissements connectés via le réseau VPN MPLS :
  - FLPA Les Oliviers
  - FLPA Le Colombier
  - Police Municipale
  - Crêche P'tits Mômes
  - Maison Chapuis
  - Annexe Médiathèque des Basses Barolles
  - RAM St Genis 2
  - Gymnase Giono
  - Stade Beauregard
  - Atelier Entretien
  - Atelier Logistique

C. DÉMARCHE DE L'AUDIT

L'étude couvrira l'ensemble des établissements cités ci-dessus. Le prestataire doit élaborer les recommandations d'amélioration par site et entre site.

Le titulaire devra proposer un audit composé de plusieurs étapes qu'il doit détailler dans son offre. Au démarrage de son action, il devra prendre connaissance de l'environnement, de leur organisation, de leurs missions et de la particularité de leurs champs d'actions.

Le prestataire pourra proposer dans son offre des missions complémentaires utiles qu'il n'aurait pas été listées. Il les identifiera clairement et en individualisera le coût.

D. DÉTAIL DE LA PRESTATION ATTENDUE

1. AUDIT INFRASTRUCTURE RÉSEAU

L'entreprise devra indiquer le pourcentage de couverture des différents bâtiments en câblage informatique (préciser la catégorie -5/5e/6,...), en Wifi et en câblage téléphonique. Les bâtiments non-équipés devront être indiqués.

Les pièces hébergeant les serveurs, les PABX, les différents switchs, routeurs, pare-feux, etc devront également être décrites, notamment les alimentations électriques, liens réseaux, fauxplanchers, climatisation, baie de brassage, armoires informatiques, onduleurs, étiquetage, accessibilité, sécurisation…

Les liens entre sites et entre bâtiments du même site (FO, Câblage,...) feront également partie de ce descriptif.

- Établir la cartographie du réseau (Emplacement machines, Hub, connectique, câblage, prises, identifications machines, tables des droits d'accès, etc.)
- Faire l'inventaire complet des serveurs (état machine, configuration détaillée exacte, logiciels installés et versions, trafic du réseau)
- Vérifier la qualité des raccordements pour s'assurer du respect des normes en vigueur;
- Vérifier l'utilisation et la performance des liens, des utilisateurs et des applications ;
- Rédiger un plan de recollement par établissement ;
- Définir le niveau de conformité du câblage informatique par rapport aux différentes normes ;
- Réaliser une Cartographie des flux de données
- Calcul de la bande passante nécessaire à chaque flux : Il s'agit d'estimer les besoins pour une transmission de bonne qualité de chaque type d'informations.
- Mesure du débit de chaque lien : c'est l'estimation de la capacité physique des liens : quelle quantité d'informations peuvent-ils transporter par unité de temps.

L'audit réseau devra s'appuyer sur les points suivants :

- Isoler les problèmes de performance liés aux serveurs et aux réseaux ;
- Analyser, identifier et classifier les flux de trafic internes et externes ;
- Analyser les équipements (routeurs, switchs, baies de brassage...);
- Analyser l'usage de la bande passante par machine et par service ;
- Analyser les besoins en bande passante ;
- Analyser les performances réseaux ;
- Faire un rapport de synthèse du réseau ;
- Établir des recommandations d'évolution, d'optimisation d'infrastructures.
- Étude approfondie et validation de l'architecture Wan et Lan du réseau.
- Étude et évaluation des choix technologiques adoptés.
- Étude et validation du plan d'adressage.
- Étude approfondie et validation du routage IP.
- Évaluation de la performance et capacités des équipements.
- Évaluation du paramétrage des équipements
- Évaluation des optimisations à faire au niveau architecture et configurations des équipements du réseau.
- Évaluation de l'état du câblage informatique
- Étude visuelle de l'état du câblage et vérification de la qualité de tous les raccordements pour s'assurer qu'ils ont été faits dans le respect des normes en vigueur en matière de longueur, du respect des pas de torsades et de l'appairage,

- Procéder à un relevé quantitatif des connections en se basant sur le plan de câblage. Si celui-ci n'en dispose pas ou si le plan de câblage est trop ancien et n'a pas été mis à jour, l'entreprise devra fournir un nouveau plan de câblage au terme de son Audit,
- Procéder à un contrôle qualitatif des connections aux deux extrémités, faire un état du repérage des liens, des platines et des autres équipements installés.
- Procéder à des tests de mesure soit sur l'ensemble du réseau, soit par échantillonnage. Ces mesures seront effectuées par réflectométries et un testeur adapté à la catégorie des câbles concernés qui permettent d'en valider :
  - Le schéma de câblage et la présence de la masse,
  - La longueur,
  - L'impédance,
  - La paradiaphonie,
- Les limites de fréquence et de bande passante du câble, de s'assurer ainsi de la conformité du câble pour que l'ensemble du réseau puisse être qualifié et exploité au mieux de ses capacités.
- Tester grâce à des appareils de mesure adaptés l'ensemble des liens ; FO, Liaison radio, LL, etc
- Identifier dans le plan de câblage les câbles devant être déposé,
- Étude de cohérences clients serveur LAN et WAN,
- Métrologie et analyse de la charge du réseau et des temps de réponse,
- Validation des redondances et du fonctionnement en mode dégradé,
- Étude de l'aptitude du réseau à supporter de nouvelles charges, nouvelles applications, nouveaux utilisateurs,

Les informations qui seront mises en évidence durant l'audit seront :

- Cartographie logique et physique du réseau ;
- Analyse du trafic réseau ;
- Analyse des performances réseau et évolution ;
- Mesure de la charge réseau ;
- Effet des applications sur la bande passante ;
- Définition des protocoles ;
- Tracking des flux et temps de réponse ;
- Analyse des échanges entre stations, serveurs et routeurs ;
- Identification des stations générant des trafics importants ;
- Mesure de la longueur des trames ;
- Identifier et classer les flux grâce à des outils spécifiques (sondes) ;
- Analyse des sept couches du modèle OSI, par segment, anneau ou Vlan,
- Mise en évidence de la répartition Unicast, Multicast et Broadcast,
- Mise en évidence des différents types d'erreurs et repérage des stations, serveurs ou matériels actifs qui les génèrent,

2. AUDIT WIFI

- Cet audit aura pour objectif de :
- Détecter l'ensemble des émissions WiFi dans le périmètre du réseau, déterminer leur position.
- Obtenir un « état des lieux », d'identifier les problèmes de couverture et de qualité de service.
- Réaliser un ensemble de tests intrusifs en "aveugle"
- Mener une étude de site pour fixer précisément la zone de couverture utile & l'implantation des équipements.
- Rédaction d'un rapport d'Audit précis, analyse des données et conseils pour la sécurisation de l'existant et l'intégration de façon simplifiée de la future architecture WiFi.
- Audit de sécurité Wifi

Cette prestation permettra de faire le point sur l'architecture actuelle, d'identifier les éventuelles failles et de déterminer les nouveautés les plus adaptées pour faire évoluer l'infrastructure actuelle dans de bonnes conditions.

3. AUDIT DE SÉCURITÉ

Tous les points liés à la sécurité informatique sont systématiquement étudiés, l'objectif est d'assurer la disponibilité, la confidentialité et l'intégrité du système d'information.

L'objectif de cette partie est de référencer l'ensemble des vulnérabilités du réseau afin de pouvoir proposer une solution répondant à la politique de sécurité de la Ville.
L'Audit de sécurité s'attachera à détecter et à mettre en évidence une/des vulnérabilité(s) dans les domaines suivants.

- La sécurité logique : Cela inclue la sécurité au niveau des données de la Ville, les applications ou encore les systèmes d'exploitation.
- La sécurité des réseaux : L'architecture du réseau, la configuration des équipements réseaux qui le composent, les serveurs de la Ville, les réseaux d'accès, etc
- La tolérance de pannes si nécessaire.
- L'administration, la gestion des logs, les remontées d'alertes…

3.1. Méthodologie

- Cette étude doit se référer à la norme organisationnelle ISO 27000.
- Collecte d'information via la consultation de la documentation existante, des entretiens avec les équipes IT, des visites des sites concernés, etc
- Capture et analyse des échantillons du trafic
- Tests actifs de mesure de temps de réponse et de taux de pertes sur le réseau temps de réponse de quelques services.

Cette étude a pour but d'identifier les menaces qui sont pertinentes pour le système d'information.
Le prestataire effectuera une intervention technique sur l'évaluation de la sécurité du système d'information.
Dans son offre, il proposera les tests nécessaires et en individualisera le coût :

3.2. Tests d'intrusion:

les tests d'intrusions permettent d'évaluer et de qualifier le niveau de vulnérabilité existant du système d'exploitation, réseau, messagerie, progiciel et application spécifique, locaux, etc.
Les tests doivent être effectués à partir de l'extérieur (internet) et en interne à partir du réseau LAN et WAN de la Ville

Les tests intrusifs ne doivent en aucun cas altérer, modifier ou détruire les données appartenant au SI de la Ville, ni perturber le bon fonctionnement du système d'information.

La réalisation des tests d'intrusion sur l'environnement de production doit être strictement accompagné par les responsables du SI de la Ville; les horaires de tirs peuvent être aménagés afin d'éviter toutes perturbations de la production. Il sera de la responsabilité du prestataire de mettre en garde, prévenir et conseiller les responsables de la Ville des risques encourus lors de la mise en œuvre de ces tests.

Ces tests seront de deux natures :

- Tests d'intrusion externes : Le test d'intrusion externe devra se dérouler à partir d'une connexion Internet, et s'effectuera en deux étapes :
  - Étape N°1 en boite noire : Les experts du titulaire procéderont à ce test en disposant uniquement des informations publiques.
  - Étape N°2 en boite blanche : Dans ce cas, le maître d'ouvrage communiquera plus de détails sur sa configuration au titulaire qui va procéder à un deuxième test d'intrusion en prenant en considération ces détails.

- Tests d'intrusion internes : Ce test devra se dérouler à partir d'un poste connecté au réseau local.

Le titulaire présentera à la Ville un rapport détaillé sur le résultat de ces tests. Le rapport devra inclure les différentes vulnérabilités exploitées lors des tests d'intrusion ainsi que les recommandations pour l'implémentation des mesures de sécurité avec explication des solutions de défense proposées ainsi que le détail technique complet pour le rejet des tests d'intrusion.

3.3. Audit de vulnérabilité :

Le prestataire devra réaliser les tests de vulnérabilité permettant de ressortir les principales failles de sécurité visibles sur les systèmes et dispositifs de sécurité audités. Pour chaque faille et vulnérabilité, il est demandé au prestataire de détailler les points suivants:

- Niveau de compétence requis pour l'exploitation de celle-ci.
- Probabilité d'exploitation.
- Conséquence en cas d'attaque réussie.

Ces vulnérabilités devront être catégorisées selon l'échelle des impacts :
Critique, Sensible, Moyenne, Faible.

S'en suit l'établissement d'un plan d'action sur les éléments de sécurité à améliorer ou à corriger.
Ce plan d'action devra prendre en compte notamment la politique de mise à jour et les recommandations pour la résolution des problèmes de sécurités les plus connus.
Les tests de vulnérabilité sur l'environnement de production doivent être réalisés dans des horaires bien aménagés afin d'éviter toutes perturbations de la production.
Il sera de la responsabilité du prestataire de mettre en garde, prévenir et conseiller les responsables de la Ville des risques encourus lors de la mise en œuvre de ces tests.

3.4. Audit de configuration :

Le prestataire devra réaliser un audit des configurations permettant de compléter la recherche des failles existantes par des points faibles liés à la configuration des équipements audités.

Le titulaire devra faire une analyse complète de la configuration des différentes composantes, à savoir : plateforme de connexion à internet, serveurs, architecture réseau, L'infrastructure réseau (Switch, routeurs, câblage), outils de sécurité et de gestion de bande passante, et tout autre périphérique et les comparer à l'état de l'art en la matière.

Le titulaire présentera un rapport détaillé de l'audit de configuration qui intégrera les points faibles/points forts, les vulnérabilités détectés ainsi que les recommandations pour les corriger avec explication des solutions à mettre en œuvre.

3.5. Obligation du prestataire :

- Le prestataire devra réaliser les audits de type : tests d'intrusion, audit des vulnérabilités et audit des configurations tel que décrit dans les paragraphes précédents.
- Prendre en charge les outils qui seront utilisés lors de l'audit.
- Réaliser la prestation objet de l'appel d'offre sans jamais altérer, modifier ou détruire les
- données appartenant au SI de la Ville, ni perturber le bon fonctionnement du système
- d'information.
- Chaque intervention sera planifiée. Aucune intervention sur site ne pourra avoir lieu sans un accord préalable de l'un des correspondants désignés par la ville.

4. AUDIT MATÉRIELS ET LOGICIELS

Tout le matériel informatique appartenant aux établissements (Serveurs, switchs, routeurs, onduleurs, pare-feux) devra être inventorié.

L'audit portera aussi sur:

- La performance des architectures et infrastructures réseaux (locaux et distants)
- La performance des équipements réseaux tel que les switch, routeur, etc.;

L'entreprise devra également répertorier tous les logiciels utilisés dans les établissements notamment en ce qui concerne : Anti-Virus, Anti-Spam, Bases de données, etc.

Pour chaque logiciel, il devra être indiqué les services les utilisant, le nombre de licences, le nombre d'utilisateurs réels, les contraintes particulières s'y rapportant ainsi que la maintenance.

E. OUTILS

L'auditeur devra mentionner dans son offre les différents types d'outils sur lesquels il va s'appuyer pour analyser le réseau :

- des scanners de vulnérabilités pour identifier le nombre de failles présentes dans le réseau,
- des sondes placées sur des points stratégiques du réseau de façon à mesurer les niveaux de performances et identifier les goulots d'étranglements par exemple,
- des normes comme ISO 27000, COBIT ou Mehari.

F. LIVRABLES

Les livrables sont :

- Rapport d'audit de l'infrastructure réseau (serveurs, switchs, routeurs, câblage, etc.) en plus des différents éléments de configuration (plan d'Adressage, plan de routage, etc)
- Recommandations et améliorations sous forme de best practices pour endiguer aux problèmes liés a l'architecture actuelle réseau et actions à entreprendre pour mettre à niveau de l'existant.
- Rapport d'Audit incluant une analyse des données et conseils pour la sécurisation de l'existant et l'amélioration de l'architecture et de la QoS WiFi
- Rapport de l'audit de détection d'intrusion, de vulnérabilité et de configuration afin de vérifier la capacité du réseau en termes de résistance à des intrusions et l'efficacité de ses mesures actuelles de sécurisation de son Système d'Information.
- Rapport d'Audit de la plateforme de sécurité avec les recommandations nécessaires sur l'état du matériel/logiciel existant.
- Rapport d'audit des performances réseaux WAN de la Ville. Avec une proposition de solution fiable et performante.
- Recommandations et améliorations sous forme de best practices pour endiguer aux problèmes et failles détectées et actions à entreprendre pour mettre à niveau l'existant.
- Définition d'une politique déclinant les règles de sécurité à mettre en œuvre pour accroître la sécurité des réseaux en interne et depuis l'Internet.
- Cahier de charge pour la mise à niveau des réseaux locaux en s'appuyant sur les recommandations issues de la phase d'audit d'infrastructure réseau avec l'estimation du budget de mise en place.

Les différents rapports d'audit (présentant bilan et recommandations) doivent être livrés en version papier et électronique.

G. QUALIFICATION DU PERSONNEL AFFECTE AU PROJET

L’équipe du prestataire affectée à ce projet doit comporter des profils ayant une très bonne expérience dans le domaine audit des réseaux informatiques et la sécurité des systèmes d’information.
Le prestataire décrira l'équipe affectée au projet et les compétences précises.

H. PLANNING

A proposer par le prestataire.