Syndicat Intercommunal des Technologies de l'Information pour les Villes

50 Boulevard Ambroise Croizat 69200 Vénissieux

69200 Vénissieux

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

MARCHE DE PRESTATIONS DE SERVICE A BONS DE COMMANDE

Objet du marché	Le présent marché a pour objet : - Sécurisation des flux de messagerie entrant et sortant du SITIV
Type de procédure	Marché public à procédure adaptée Marché passé en vertu des articles L2123-1, R2162-13 et R2162-14 du Code de la commande publique
Date de réponse	Le vendredi 15 mars 2024 à 12h00

Le présent marché est soumis aux dispositions du Code de la commande publique entré en vigueur le 1er avril 2019

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

Table des matières

1 CADRE DE LA CONSULTATION

Le présent marché porte sur la sécurisation des flux entrant et sortant de messagerie de la solution collaborative ZIMBRA exploitée par le SITIV pour le compte de ses communes adhérentes.

1.1 CONTEXTE

Le SITIV héberge pour le compte de ses collectivités membres des services numériques variés :

- Outils collaboratifs : messagerie, plateforme documentaire, réseau social
- Sites Internet, Gestion de la relation citoyen, E-democratie
- Logiciels métiers : gestion financière, ressources humaines, action sociale, élection, état civil, services techniques, délibération …
- Outils transverses : tiers de télétransmission, parapheur électronique, archivage numérique

Le service de messagerie collaborative est basé sur la solution Zimbra.

Il héberge les différents domaines des villes adhérentes du SITIV pour un total actuel de 6000 boites aux lettres et avec une progression annuelle d'environ 10%.

Le SITIV souhaite externaliser l'analyse des flux entrant et sortant de la messagerie pour garantir à la fois un haut niveau de sécurité et un haut niveau de délivrabilité des messages des collectivités.

1.2 DESCRIPTIF DES PRESTATIONS ATTENDUES

Le SITIV souhaite externaliser, en mode hébergé, une solution de sécurisation globale des flux entrants et sortants de messagerie électronique à destination de ses villes adhérentes.
La solution mise en place sera donc totalement exploitée par le titulaire et sous son entière responsabilité.
Le titulaire devra assurer un haut niveau d'engagement sur sa solution : disponibilité du flux, qualité de la détection des SPAM (faux positifs et négatifs) et des VIRUS, réactivité et adaptation aux nouvelles techniques d'agression.
Le titulaire s'attachera à démontrer comment la multiplicité des techniques et algorithmes mis en œuvre dans sa solution sont en mesure de prémunir le SITIV de la réception de mails dangereux tout en limitant les « faux » et à augmenter la délivrabilité des messages émis par les collectivités

- Variété et complémentarité des solutions antivirales employées
- Etendue de l'analyse heuristique
- Qualité des listes noires
- Capacité de réactivité devant les nouvelles attaques
- Mécanismes variés de détection d'émetteurs peu surs
- Analyse des pièces jointes et des images
- Saisie de captcha
- Antivirus, Antispam, Anti-phishing, Anti-ransomware, Anti-ddos, Anti publicité
- Protection contre l'émission de mails corrompu ou frauduleux
- Protection contre le blacklistage, renforcement de la délivrabilité

Le délai total d'acheminement des mails légitimes ne sera pas augmenté, en moyenne quotidienne, de plus de 4 secondes du délai d'acheminement initial des mails au prestataire.
Le service de transmission de flux de messagerie et d'analyse du courrier doit être garanti par un taux de disponibilité de 99,997 %. Toute heure de dépassement de ce délai garanti annuel (au-delà de 24 heures d'arrêt par an) sera soumise au régime des pénalités de GTI.
Un portail web sera mis à disposition des utilisateurs pour leur permettre au minimum de visualiser les statistiques d'analyse de leurs boites aux lettres et de contrôler leurs éventuels courriers mis en quarantaine.

Ce portail devra être intégré au portail agent du SITIV par un système d'authentification unique. Ce portail est basé sur la solution LemonLDAPNG qui permet la mise en œuvre du protocole SSO Openid Connect. Le prestataire décrira précisément comment il envisage cette interconnexion.

L'enrôlement des utilisateurs sur ce portail devra s'effectuer sans intervention récurrente des administrateurs SITIV et Villes.

Un portail web sera également mis à disposition des administrateurs du SITIV et des Villes qui leur permettra de contrôler l'activité des boites aux lettres des utilisateurs, et ce pour les noms de domaine qui les concernent. Les données de logs et les courriers en quarantaine seront conservés au minimum pendant une durée de 30 jours.
Le titulaire assure l'accompagnement des utilisateurs et des administrateurs du SITIV et des communes pendant la phase de mise en œuvre de sa solution et tout au long de son exploitation.
Le titulaire fournit les documents de communication et de formation destinés aux utilisateurs finaux de la solution.
Le titulaire forme les administrateurs du SITIV et des Villes et fournit les procédures d'administration.

La solution recherchée doit être mis en œuvre en moins de 24 heures par simple redirection des flux de messagerie et sans aucune installation de matériel, ni de logiciel dans l'environnement du SITIV et des villes.

Le titulaire assiste le SITIV dans le paramétrage des composants réseaux et de messagerie existants pour rendre opérationnel et sécuriser la liaison entre son service SAAS et la plateforme ZIMBRA du SITIV. Cet engagement est entendu comme un engagement de résultat.

En cas de panne ou d'arrêt de la plateforme ZIMBRA du SITIV, le titulaire s'engage à conserver automatiquement l'intégralité des mails non acheminés pendant une durée minimum de 7 jours, qui pourra sans frais, être prolongée jusqu'à 30 jours en cas de sinistre majeur sur les installations du SITIV.

Dans ce cas, le titulaire proposera au SITIV une solution de messagerie web temporaire permettant d'assurer la continuité d'activité.

La totalité des données et serveurs seront hébergés en France dans un ou plusieurs Datacenter Sécurisés. Le titulaire s'engage à ne pas conserver les données délivrées au SITIV au-delà d'une durée permettant d'en valider l'acheminement et à ne conserver sur ses infrastructures que les courriers non remis. Il ne pourra faire un autre usage de ces données qu'à des fins statistiques et internes

Dès la première année, et pour l'ensemble de la durée du marché, le titulaire accompagne le SITIV dans l'exploitation de la plateforme en production.

En cas de non mise en production du service pour l'intégralité des boites aux lettres existantes dans le délai précédent, outre les pénalités, le prestataire prendra à sa charge l'intégralité des frais liés à la continuité du service existant.

1.3 TARIFICATION

Le prestataire doit compléter le bordereau des prix du SITIV.

Ces prix incluront obligatoirement :

I- Une mise à disposition forfaitaire annuelle du service incluant l'ensemble des prestations d'hébergement, de support, de mise à niveau et de maintien en condition opérationnelle pour 6000 boites aux lettres.

II- Les prestations forfaitaires nécessaires à la mise en œuvre initiale du service global pour l'ensemble des boites aux lettres existantes.

III- Les prestations forfaitaires nécessaire pour l'intégration d'une collectivité supplémentaire au service

Ces prix seront fixés pour la durée du marché sans réactualisation ni révision.

2 RESPECT DES REFERENTIELS

En tant que personne publique, les dispositifs livrés devront être conformes en tous points avec :

- Référentiel Général de Sécurité (RGS) dans sa version actuelle
- Règlement Général sur la Protection des Données
- Recommandation de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI)

o Ex : les 42 règles de sécurité simple éditées dans le guide d'hygiène informatique – éditions 2017 et à venir de l'ANSSI
- Référentiel Général d'Accessibilité des Administrations (R.G.A.A) dans leur version actuelle, le cas échéant.
- La Politique de sécurité du système d'information du SITIV (PSSI)

Le candidat précisera toute information qui lui paraitra pertinente sur ces sujets.

2.1 R.G.S. – RÈGLEMENT GÉNÉRAL DE SÉCURITÉ

Suite au décret numéro 2010-112 du 02 février 2010 et de l'arrêté RGS publié au Journal Officiel le 18 mai 2010, l'application doit respecter les contraintes imposées par le référentiel général de sécurité (RGS) étendu aux utilisateurs des collectivités.

Ce respect doit s'appliquer tant à l'accès à l'application qu'au stockage des données. Le candidat décrira de façon détaillée les dispositifs qu'il a mis en œuvre pour respecter ces contraintes et notamment, sa capacité à anonymiser/détruire/archiver/crypter des données personnelles et à tenir compte dans ses versions du cycle de mise à jour des composants de base de l'application (versions de java, de php, etc)

Une procédure d'homologation RGS sera réalisée par le SITIV. À la suite des conclusions rendues par la commission d'homologation du SITIV, le candidat devra se mettre en conformité. A minima, les critères précédents seront vérifiés.

Pour obtenir des informations plus poussées sur la sécurité des systèmes d'information, le candidat peut consulter le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

2.2 R.G.P.D. – RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

De plus le prestataire devra fournir toutes les informations utiles et prendre en compte dans son produit le Règlement général sur la protection des données (RGPD).

En effet le nouveau règlement européen sur la protection des données a été définitivement adopté par le Parlement européen le 14 avril 2016. Ses dispositions seront directement applicables dans l'ensemble des 28 États membres de l'Union Européenne à compter du 25 mai 2018. Le logiciel devra prévoir :

· Un consentement « explicite » et « positif » de la part des citoyens.

· Le droit à l'effacement (version allégée du droit à l'oubli) : la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données à caractère

personnel la concernant. Le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais (article 17).

· Le droit à la portabilité des données personnelles : les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine. De plus, elles ont le droit de transmettre ces données à un autre responsable du traitement.

· Profilage : toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire (article 22 du Règlement).

· Des principes de « protection des données dès la conception » et de « sécurité par défaut » : le règlement européen définit le principe de « protection des données dès la conception » qui impose aux organisations de prendre en compte des exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel. De plus, le règlement consacre la nouvelle règle de la « sécurité par défaut » qui impose à toute organisation de disposer d'un système d'information sécurisé (article 25 du Règlement).

· Des notifications en cas de fuite de données. L'importance des sanctions oblige les collectivités à de la prudence : le règlement donne aux régulateurs le pouvoir d'infliger des sanctions financières allant jusqu'à 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros (le montant le plus élevé étant retenu), en cas de non-respect (article 83.6 du Règlement).

2.3 R.G.A.A – RÉFÉRENTIEL GÉNÉRAL D'ACCESSIBILITÉ POUR LES ADMINISTRATIONS

Le prestataire devra prendre en compte et s'assurer du respect de l'ensemble du référentiel tel que décrit dans les documents officiels comme le Référentiel Général d'Accessibilité pour les Administrations (RGAA) dans sa version courante.

La prise en compte des normes d'accessibilité en vigueur : W3C et niveau AA minimum des exigences d'accessibilité RGAA est obligatoire.

Le titulaire en tant que maitre d'œuvre a le droit d'alerter la maitrise d'ouvrage si elle détecte des contraintes techniques insurmontables pour l'accessibilité ou nécessitant des compromis dans la conception ou les choix opérés.

Le référentiel général d'accessibilité pour les administrations repose sur les 4 grands principes d'un site internet ou intranet accessible :

- Un site perceptible
- Un site utilisable
- Un site compréhensible
- Un site robuste

Toutes les informations de référence sont disponibles sur le site http://references.modernisation.gouv.fr/accessibilite-numerique

2.4 P.S.S.I. – Politique de sécurité du système d'information (SITIV)

Conformément à la PSSI mutualisée avec les villes adhérentes du SITIV, la confidentialité et l'intégrité des flux en interaction avec les systèmes d'information du SITIV doivent respectés les conditions de sécurités suivantes :
Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données. De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière. Le titulaire indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration. (cf Annexe 1 : PSSI) ;

Le cahier des clauses simplifiées de cybersécurité (annexe 2) relatif à l'article 2 du CCAP encadre la PSSI.