Envoyé en préfecture le 16/08/2023
Reçu en préfecture le 16/08/2023
Publié le
ID : 069-216900290-20230813-20230810DEC098-AU

DIRECTION DES SYSTEMES D'INFORMATION ET DES TELECOMMUNICATIONS
Réf. :

DECISION DU MAIRE DE BRON

Numéro : 20230810DEC098

Objet: Prestation de services

Le Maire de Bron, Jérémie BREAUD,

VU les articles L. 2122-22 et L. 2122-23 du Code Général des Collectivités Territoriales,

VU la délibération n° 20200716DEL2 du 16 juillet 2020 donnant, au titre de l'article L. 2122-22 du Code Général des Collectivités Territoriales, délégation au Maire pour prendre toute décision concernant la préparation, la passation, l'exécution et le règlement des marchés et accords cadres ainsi que toutes décisions concernant leurs avenants, lorsque les crédits sont inscrits au budget,

CONSIDERANT qu'il convient de sécuriser l'annuaire Active Directory dans le cadre du plan de sécurisation 2023, validé et subventionné par l'Agence Nationale de Sécurité des Systèmes d'Informations, l'ANSSI,

CONSIDERANT le 2° de l'article R. 2122-3 du Code de la Commande Publique qui spécifie que pour des raisons techniques l'acheteur peut passer un marché sans publicité ni mise en concurrence préalables,

CONSIDERANT que le groupement Cinétic-IT / X9000 titulaire du marché 2021-380 de support de l'infrastructure systèmes est la seule entité à pouvoir réaliser cette opération et son suivi dans le temps du fait de l'imbrication de l'opération de sécurisation avec les prestations de support du marché pré-cité,

CONSIDERANT que la Ville de Bron procède par groupement de commande avec le CCAS de Bron et que la clef de répartition retenue pour ce type de prestation est de 90 % des montants pour la Ville et de 10 % pour le CCAS,

DECIDE

Article 1 : de signer le marché public suivant :

- Titulaire : cotraitants Cinetic-IT et X9000, tous deux situés 69760 Limonest
- Objet : Plan de sécurisation de l'annuaire Active Directory
- Prix global et forfaitaire : 9 562,50 € HT
- Durée : fin prévisionnelle de la prestation au 30 novembre 2023

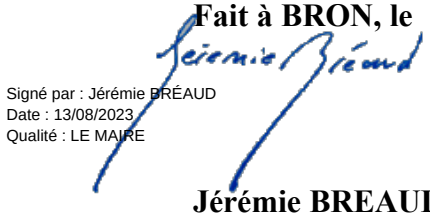
Article 2 : Monsieur le Directeur Général des Services de la Ville de Bron est chargé de l'exécution de la présente décision qui sera publiée sur le site Internet de la Ville.

Envoyé en préfecture le 16/08/2023
Reçu en préfecture le 16/08/2023
Publié le
ID : 069-216900290-20230813-20230810DEC098-AU

Article 3 : la présente décision peut faire l'objet d'un recours administratif devant Monsieur le Maire de Bron dans le délai de deux mois à compter de sa publication. L'absence de réponse dans un délai de deux mois vaut décision implicite de rejet.

Article 4 : un recours contentieux peut également être introduit devant le Tribunal Administratif de Lyon ou déposé sur www.telerecours.fr dans le délai de deux mois à compter de la publication de la décision ou à compter de la réponse de l'administration si un recours administratif a été préalablement déposé.

Fait à BRON, le



Signé par : Jérémie BRÉAUD
Date : 13/08/2023
Qualité : LE MAIRE

Jérémie BREAUD,

VILLE DE BRON

Sécurisation AD v2

Mémoire Technique et Financier

VILLE DE BRON

Christelle LEVERT - Ingénieur Commercial
christelle.levert@x9000.fr 06 03 51 91 92

Paolo De Oliveira- Consultant
p.deoliveira@cinetic-it.fr 06 17 01 56 32

Sommaire

Introduction

Objectifs du document

- Ce document a pour objectif de répondre au besoin exprimé par la Ville de Bron dans le cadre de son projet de sécurisation AD
- Nous démontrons ici la méthodologie rigoureuse utilisée par X9000 et CINETIC-IT pour :
  - Analyser le besoin avec des critères qualitatifs et quantitatifs
  - Identifier les objectifs de la DSI et de l'organisation tout entière
  - Définir une démarche projet pour la sécurisation de l'AD de la Ville de Bron
  - Présenter les composantes budgétaires du projet

Plan de sécurisation AD Rappel du contexte

Plan de sécurisation AD

Rappel du contexte

- Dans le cadre de la sécurisation de son SI, la ville de Bron a mandaté un audit de sécurité AD auprès de CAPGEMINI
- L'auditeur a présenté le résultat de cet audit et préconise des changements qui peuvent impacter le fonctionnement du SI
- La ville de Bron souhaite être accompagnée dans la démarche de remédiation
- CINETIC-IT/X9000 propose dans ce cadre une démarche afin d'implémenter les points relevés en collaboration avec le service informatique de la ville de Bron

Plan de sécurisation AD – Synthèse des points d'amélioration

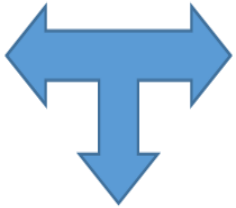
Plan de sécurisation AD

Synthèse des points d'amélioration

Il s'agit de regrouper par thème les points remontés dans l'audit :

Evolution / configuration de l'infrastructure :

- Machine dédiée à l'administration
- Préparation AD en révision 16 mini
- Niveau fonctionnel en Windows 2016
- Utilisation de DC en mode core Windows 2019
- Sauvegarde avec guest processing
- Mise en œuvre LAPS serveurs membre et PC
- Procédure annuelle de modification du mot de passe du compte krbtgt
- Sécurisation des protocoles



Gestion des comptes

- Politique de création de compte et nomenclature
- Processus d'entrée / sortie d'utilisateur
- Stratégie de mot de passe (changement et durcissement)
- Expiration des mots de passe
- Rectifications des comptes génériques en compte nommés
- Ménage dans les comptes standards et PC

Droits d'administration

- Politique liée à la gestion des droits d'administration
- Création de comptes d'administration nommés Internet et externe (adapter les privilèges aux usages)
- Ménage dans les groupes administratifs
- Protection des comptes administratifs
- Changement du mot de passe Administrateur et mise au coffre

Plan de sécurisation AD – Proposition du plan d'action

Plan de sécurisation AD

Proposition du plan d'action

- Objectifs
  - Présenter les actions correctives, leurs charges et leurs complexités
  - Echanger sur l'appui technique de CINETIC-IT/X9000 sur ces actions

Plan de sécurisation AD

Proposition du plan d'action

Evolution / configuration de l'infrastructure

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Machine dédiée à l'administration	Installation d'une machine dédiée à l'administration avec une publication de bureau à distance pour les administrateurs Installation des outils RSAT et licences RDS	+	2	1
Préparation AD en révision 16 mini	Définition de la version cible Sauvegarde des contrôleurs de domaine Extension de schéma et domainprep (peut être lié à la réinstallation de DC)	+	2	0,25
Niveau fonctionnel en Windows 2016	Vérification des OS présent sur le domaine Sauvegarde des contrôleurs de domaine Augmentation du niveau fonctionnel de la forêt et du domaine	+	2	0,25

Plan de sécurisation AD

Proposition du plan d'action

Evolution / configuration de l'infrastructure

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Utilisation de DC en mode core Windows 2019	Configuration de 2 nouveaux AD standardisés en mode Core (VMs) - Rédaction de la procédure de migration - Installation serveurs / Migration des rôles - Décomissionnement anciens AD	++	3	3
Sauvegarde avec guest processing	Création d'un compte pour la sauvegarde consistante VEEAM Test de la mise en œuvre du guest processing pour un DC	++	1	0,5
Mise en œuvre LAPS serveurs membre et PC	Mise en place LAPS pour la gestion des comptes Admin locaux - Définition du déploiement - Extension du schéma AD & installation - Configuration / recette	++	1	2

Plan de sécurisation AD

Proposition du plan d'action

Evolution / configuration de l'infrastructure

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Mot de passe du compte krbtgt	Procédure annuelle de modification du mot de passe du compte krbtgt / Modification de celui-ci	+	2	0,25
Sécurisation des zones DNS	Définir l'obligation des mises à jour sécurisées	+	1	-
Sécurisation des protocoles	Désactivation de LLMNR et Netbios Obligation de signature de SMB	++	1	0,5
Limitation de l'ajout au domaine	Suppression de la possibilité aux utilisateurs lambdas d'ajouter une machine au domaine	++	2	0,5

Plan de sécurisation AD

Proposition du plan d'action

Gestion des comptes

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Mot de passe du compte krbtgt	Procédure annuelle de modification du mot de passe du compte krbtgt / Modification de celui-ci	+	2	0,25
Sécurisation des zones DNS	Définir l'obligation des mises à jours sécurisées	+	1	-
Sécurisation des protocoles	Désactivation de **LLMNR et Netbios** Obligation de signature de SMB	++	1	0,5
Limitation de l'ajout au domaine	Suppression de la possibilité aux utilisateurs lambdas d'ajouter une machine au domaine	++	2	0,5

Plan de sécurisation AD

Proposition du plan d'action

Gestion des comptes

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Expiration des mots de passe	Réactivation de l'expiration des mots de passe par lots d'utilisateurs Gestion des problèmes liés aux services Windows	+	2	1
Rectifications des comptes génériques en compte nommés	Listing des comptes n'expirant jamais Identification de leur utilisateur Attribution de comptes nommés à tous les utilisateurs	++	1	0,5 à 3
Stratégie de mot de passe (changement et durcissement)	Définition de la stratégie (même politique pour tous les comptes ou PSO) Communication sur la stratégie de mot de passe Durcissement des mots de passe utilisateurs et administrateurs	+ ou ++	1	2 à 3
Ménage dans l'AD	Désactivation des comptes utilisateur et PC/Serveur non utilisé. Après 1 mois, suppression des comptes	+	3	3 à 5

Plan de sécurisation AD

Proposition du plan d'action

Droits d'administration

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Politique liée à la gestion des droits d'administration	Rédaction des procédures de gestion des droits administratifs. Définition des profils RBAC Compte inclus dans le groupe « Protected Users » Rédaction des processus d'attribution et de suppression	++	1	2 à 3
Création de comptes d'administration nommés Interne	Création des groupes correspondant aux rôles RBAC définis Création des comptes d'administration nommés pour chaque utilisateur le nécessitant.	+	1	1 à 2
Création de comptes d'administration nommés Prestataire	Récupération de la liste des intervenants par prestataire Création des groupes correspondant aux rôles RBAC définis Création des comptes d'administration nommés pour chaque utilisateur le nécessitant.	++	1	2 à 3

Plan de sécurisation AD

Proposition du plan d'action

Droits d'administration

Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge (jour/h)
Ménage dans les groupes administratifs	Retrait au fur et à mesure des utilisateurs appartenant aux groupes sensibles lors de la création des comptes administratifs	+	1	-
Protection des comptes administratifs	Protéger les comptes contre la suppression accidentelle	+	2	1
Changement du mot de passe Administrateur et mise au coffre	Audit de l'utilisation du compte administrateur Vérification des services et applicatifs sur les serveurs Remplacement par des comptes de services uniques le compte administrateur Modification du mot de passe Mise au coffre du mot de passe	+++	1	3 à 5

Plan de charge

Plan de charge

- Après échange avec la ville de Bron concernant le plan d'action proposé, il en découle le plan de charge suivant

Thème	Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge VdB (jour/h)	Charge Cinetic-IT (jour/h) - Profil Ingénieur	Charge Cinetic-IT (jour/h) - Profil Expert	Annotation
Infra	Machine dédiée à l'administration	Installation d'une machine dédiée à l'administration avec une publication de bureau à distance pour les administrateurs Installation des outils RSAT et licences RDS	+	2	1			Configuration des licences RDS
Infra	Préparation AD en révision 16 mini	Définition de la version cible Sauvegarde des contrôleurs de domaine Extension de schéma et domainprep (peut être lié à la réinstallation de DC)	+	2	0	0,5		
Infra	Niveau fonctionnel en Windows 2016	Vérification des OS présent sur le domaine Sauvegarde des contrôleurs de domaine Augmentation du niveau fonctionnel de la forêt et du domaine	+	2	0			
Infra	Limitation de l'ajout au domaine	Suppression de la possibilité aux utilisateurs lambdas d'ajouter une machine au domaine	++	2	0			
Infra	Sécurisation des protocoles	Désactivation de LLMNR et Netbios Obligation de signature de SMB	++	1		0,5		
Infra	Revue Config SMB NAS	Revue de la configuration SMB des NAS pour signer le protocole	+	2		0,25		
Infra	Sauvegarde avec guest processing	Création d'un compte pour la sauvegarde consistante VEEAM Test de la mise en œuvre du guest processing pour un DC	++	1	0	0,5		

Plan de charge

- Après échange avec la ville de Bron concernant le plan d'action proposé, il en découle le plan de charge suivant

Thème	Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge VdB (jour/h)	Charge Cinetic-IT (jour/h) - Profil Ingénieur	Charge Cinetic-IT (jour/h) - Profil Expert	Annotation
Infra	Mot de passe du compte krbtgt	Procédure annuelle de modification du mot de passe du compte krbtgt / Modification de celui-ci	+	2	0,25			
Infra	Sécurisation des zones DNS	Définir l'obligation des mises à jour sécurisées	+	1				
Infra	Vue voisinage réseau PC	Création d'une GPO pour désactiver la vue du voisinage réseau des postes Validation de la GPO sur un échantillon représentatif de PC	+	3		0,5		
Infra	Utilisation de DC en mode core Windows 2019	Configuration de 2 nouveaux AD standardisés en mode Core (VMs) Rédaction de la procédure de migration Installation serveurs / Migration des rôles Décomissionnement anciens AD	++	3	1		2	Préparation des VM par SI VdB
Infra	Mise en œuvre LAPS serveurs membre et PC	Mise en place LAPS pour la gestion des comptes Admin locaux Définition du déploiement Extension du schéma AD & installation Configuration / recette	++	1	2		2	Tâche effectuée avec SI VdB pour transfert de compétences

Plan de charge

- Après échange avec la ville de Bron concernant le plan d'action proposé, il en découle le plan de charge suivant

Thème	Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge VdB (jour/h)	Charge Cinetic-IT (jour/h) - Profil Ingénieur	Charge Cinetic-IT (jour/h) - Profil Expert	Annotation
Gestion comptes	Politique de création de compte et nomenclature	Vérification des OS présent sur le domaine Sauvegarde des contrôleurs de domaine Augmentation du niveau fonctionnel de la forêt et du domaine	++	3	2		0,5	Révision et commentaire politique par CINETIC-IT
Gestion comptes	Processus d'entrée / sortie d'utilisateur	Rédaction de la procédure d'entrée et de sortie des utilisateurs Hiérarchisation des droits Définition des actions (prêt de matériel, création du compte, qui autorise les accès par service…)	++	1	0,5			
Gestion comptes	Stratégie de mot de passe (changement et durcissement)	Définition de la stratégie (même politique pour tous les comptes ou PSO) Communication sur la stratégie de mot de passe Durcissement des mots de passe utilisateurs et administrateurs	+ ou ++	1	2			En cours, par Didier Gil
Gestion comptes	Expiration des mots de passe	Réactivation de l'expiration des mots de passe par lots d'utilisateurs Gestion des problèmes liés aux services Windows	+	2	1	0,25		Script pour le référencement
Gestion comptes	Rectifications des comptes génériques en compte nommés	Listing des comptes n'expirant jamais Identification de leur utilisateur Attribution de comptes nommés à tous les utilisateurs	++	1	1			
Gestion comptes	Ménage dans l'AD	Désactivation des comptes utilisateur et PC/Serveur non utilisé. Après 1 mois, suppression des comptes	+	3	1	0,25		Script pour le référencement

Plan de charge

Thème	Action	Description de l'action	Complexité (+ à +++)	Priorisation (1 à 3)	Charge VdB (jour/h)	Charge Cinetic-IT (jour/h) - Profil Ingénieur	Charge Cinetic-IT (jour/h) - Profil Expert	Annotation
Droits d'administration	Politique liée à la gestion des droits d'administration	Rédaction des procédures de gestion des droits administratifs. Définition des profils RBAC Compte inclus dans le groupe « Protected Users » Rédaction des processus d'attribution et de suppression	++	1	0,5		1	Définition avec le SI VdB Rédaction du document
Droits d'administration	Création de comptes d'administration nommés Interne	Création des groupes correspondant aux rôles RBAC définis Création des comptes d'administration nommés pour chaque utilisateur le nécessitant.	+	1	1	1		Appui technique
Droits d'administration	Création de comptes d'administration nommés Prestataire	Récupération de la liste des intervenants par prestataire Création des groupes correspondant aux rôles RBAC définis Création des comptes d'administration nommés pour chaque utilisateur le nécessitant.	++	1	2	0,5		Appui technique
Droits d'administration	Ménage dans les groupes administratifs	Retrait au fur et à mesure des utilisateurs appartenant aux groupes sensibles lors de la création des comptes administratifs	+	1				
Droits d'administration	Protection des comptes administratifs	Protéger les comptes contre la suppression accidentelle	+	2	1			Intégration dans groupe "Protected Users
Droits d'administration	Changement du mot de passe Administrateur et mise au coffre	Audit de l'utilisation du compte administrateur Vérification des services et applicatifs sur les serveurs Remplacement par des comptes de services uniques le compte administrateur Modification du mot de passe Mise au coffre du mot de passe	+++	1	2	2		Appui technique Script pour identifier les connexions administrateur Aide à la création de comptes de service / tâches planifiées
Projet	Suivi de projet	Chef de projet					2	
				Total	**18,25**	**6,25**	**7,5**	

Synthèse financière

Synthèse financière

L'ensemble des prestations ci-dessous est chiffré en heures et jours ouvrés

	Profil	Nombre de jours	Prix unitaire H.T.	Prix total H.T.
1	Journée tarif ingénieur – prestation sur site	2,75 jours	720 euros H.T.	1 980,00 euros H.T.
2	Journée tarif ingénieur – prestation à distance	3,5 jours	670 euros H.T.	2 345,00 euros H.T.
3	Journée tarif Expert – prestation sur site	3 jours	870 euros H.T.	2 610,00 euros H.T
4	Journée tarif Expert – prestation à distance	4,5 jours	820 euros H.T.	3 690,00 euros H.T.
	TOTAL	13,75 jours		10 625,00 euros H.T.

Dans le cadre du groupement de commande Ville de Bron / CCAS de Bron, la répartition des commandes se fera comme suit

- Commande Ville de Bron ratio 90% : 9 562,50 € HT
- Commande CCAS de Bron ratio 10% : 1 062,50 € HT

Conditions commerciales

Conditions commerciales

- Conditions générales
  - L'offre est valable jusqu'au 24 aout 2023.
  - Les tarifs sont fermes et les prestations sont forfaitaires.
  - Elles seront facturées en fin de prestation selon les clauses générales de paiement ci-après.

- Principe des interventions
  - Toutes les opérations se feront en limitant les temps d'indisponibilités aux agents de la Ville de Bron. Etant en charge du support de l'infrastructure systèmes et des serveurs, les opérations nécessitant un lien avec le support ne sont pas comptabilisées dans l'offre mais entrent dans le cadre du contrat de support existant sans surcoût.

- Délai intervention
  - Le délai d'intervention est soumis à planification en accord avec les plannings de la Ville de Bron, la fin de la prestation est prévue au 30 novembre 2023, sous réserve de la disponibilité des équipes de la Ville de Bron.

- Livrables
  - Hormis la réalisation du durcissement de l'annuaire MS-AD en lui-même, un compte rendu d'intervention sera fourni détaillant ce qui a été fait, et ce qui par la suite devra l'être afin de maintenir le niveau de sécurisation souhaité.
  - Tous les livrables seront fournis en format éditables et pdf.

- Clauses générales de paiement
  - Les sommes dues, seront payées dans un délai maximum de 30 jours à compter de la date de réception par la Ville des factures ou des demandes de paiement équivalentes, sauf désaccord du service gestionnaire du marché. Le mode de règlement de ce marché est le virement.
  - En cas de retard de paiement, le titulaire a droit au versement d'intérêts moratoires, ainsi qu'à une indemnité forfaitaire pour frais de recouvrement d'un montant de 40 €. Le taux des intérêts moratoires est égal au taux d'intérêt appliqué par la Banque centrale européenne à ses opérations principales de refinancement les plus récentes, en vigueur au premier jour du semestre de l'année civile au cours duquel les intérêts moratoires ont commencé à courir, majoré de huit points de pourcentage

Conditions commerciales

- Protection des données personnelles
  - Rappel sur le règlement européen sur la protection des données personnelles.
  - Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).
  - Dans le cadre de la prestation, des opérations visant à sécuriser les données annuaires comportant les coordonnées professionnelles des agents seront effectuées.
  - L'accès à ces données se fera sous contrôle de la DSIT de la Ville de Bron.
  - Les traitements en lien sont limités aux suivants :
    - Traitements d'import/export, de copies temporaires
    - Traitements de sauvegarde/restauration, réplication
    - Traitements de sécurisation : chiffrement/déchiffrement, pseudonymisation …
  - L'équipe en charge de la prestation devra disposer durant le temps de la prestation et dans la limite de ce que la prestation exige, des accès nécessaires à la réalisation des traitements pré-cités sous contrôle de la DSIT de la Ville de Bron.
  - Le respect de la confidentialité des données accédées est garanti.