Auvergne Rhône-Alpes Entreprises

Appel à prestataire

Audit de sécurité des plateformes Web et deux tests d'intrusion

Novembre 2020

SOMMAIRE

Article 1 - Objet du marché

L'agence sollicite un prestataire qualifié dans le domaine de la sécurité informatique pour :

- Auditer les solutions Web de l'Agence et évaluer leur pertinence technique en termes de sécurité et de maintenabilité.
- Identifier les éléments les plus vulnérables et apporter des réponses techniques et des procédures associées
- Réaliser des tests d'intrusion avancés sur deux plateformes

Contexte et présentation

L'Agence économique régionale Auvergne-Rhône-Alpes Entreprises est née de la volonté de la Région de rassembler les structures économiques de l'ensemble de son territoire pour soutenir les entreprises, en lien avec les EPCI et les Départements.

Financée principalement par la Région, Auvergne-Rhône-Alpes Entreprises est une association, sans but lucratif, présente sur tous les territoires grâce à 11 antennes locales et 130 collaborateurs.

L'Agence économique régionale oriente et accompagne les entreprises industrielles et des services à l'industrie à toutes les étapes de leur développement : investissement, formation et emploi, innovation, export, accès aux financements et projets européens...

Auvergne-Rhône-Alpes Entreprises a également pour mission de promouvoir la région à l'international et de valoriser ses multiples atouts pour attirer de nouvelles entreprises sur son territoire.

Dans le cadre des missions qui lui sont confiés, l'Agence s'appuie sur des plateformes Web dans le but de diffuser et d'échanger des informations avec les entreprises. Afin de bénéficier des avancées techniques en la matière, certaines plateformes ont récemment été migrées sous de nouvelles solutions, plus adaptées aux attentes des entreprises. Chaque plateforme répond à des restrictions d'accès en fonction de la nature des contenus diffusés. Ces plateformes étant un vecteur de communication, l'Agence souhaite également en garantir le niveau d'intégrité et de disponibilité.

Une démarche ISO 27001 ayant été initiée, l'Agence a déjà fait réaliser des audits et tests d'intrusion, et souhaite poursuivre ces actions à fréquence régulière.

Article 2 - Condition d'exécution

2.1. Définition des missions du prestataire

Le prestataire aura pour mission d'évaluer la pertinence en termes de sécurité des nouvelles plateformes ainsi que de l'environnement associé aux à ces dernières, via un audit.

Evaluation des plateformes web

Le prestataire devra **évaluer les solutions techniques utilisées** en tenant compte entre autres :

- De la réputation des solutions dans le cadre d'usages similaires
- Du suivi des solutions
- De la régularité et réactivité de mise à disposition des patchs de sécurité
- De la facilité d'applicabilité de ces correctifs dans un contexte de production
- De la robustesse de l'architecture utilisée et des éléments qui la composent
- Des langages de programmation exploités
- De la prise en compte des aspects de sécurité dans la conception même des solutions
- De l'existence de modules spécifiques pour limiter la perméabilité aux attaques les plus répandues (injections, brute force,…)
- Des environnements cibles nécessaires à la production des sites en résultant

A l'issue de cet audit, le prestataire devra livrer un rapport identifiant les forces, faiblesses de chaque solution ainsi qu'un processus de revue de sécurité tenant compte de ces éléments.

Les axes d'amélioration feront l'objet d'une rubrique spécifique.

Test d'intrusion avancé

Le prestataire devra également réaliser deux tests d'intrusion sur des plateformes Web de l'Agence.

Ces tests seront à réaliser à minima en environnement dit « boîte noire ». En fonction de la pertinence évaluée, le prestataire pourra proposer d'élargir les tests dans des environnements ou selon des méthodologies plus larges.

Afin de procéder aux tests dans des conditions les plus réalistes possibles tout en préservant l'intégrité et la continuité des services, un environnement spécifique pourra être mis à disposition du prestataire : il lui incombera de s'assurer que l'environnement présenté lui permette de mener à bien le test dans des conditions conformes et sans risque d'impact sur les systèmes en production.

Méthodologie et outils

Le prestataire réalisera la prestation en respectant à minima les recommandations de l'OWASP (v4 en vigueur au 10/11/2020).

Afin de juger de la difficulté d'exploitation des vulnérabilités employées, chaque outil utilisé devra être communiqué.

Livrables attendus

Le résultat de chaque test d'intrusion devra faire l'objet d'un rapport détaillé, répondant aux contraintes suivantes :

- État de vulnérabilité globale de la plateforme
- Forces
- Faiblesses
- Liste des vulnérabilités identifiées, s avec preuve apportée(captures d'écran,…) et les scénarii d'exploitation potentiels
- Détail d'exploitation des vulnérabilités et détail de l'action corrective à mettre en œuvre
- Matrice des risques synthétiques
  Tableau de priorisation de traitement des correctifs, dans une logique de facilité de mise en œuvre / niveau de risque

Restitution des résultats

A l'issue de la prestation, une restitution des résultats sous format réunion physique ou visio sera présentée aux acteurs pertinents identifiés au sein de l'Agence.

Mise à disposition des informations techniques détaillées

Sous réserve de validation d'un accord de non divulgation, un document technique détaillant les plateformes web utilisées ainsi que les environnements de production pourra être remis aux candidats. Le souhait de disposer de ces éléments devra être signifié par courriel, à si@auvergnerhonealpes-entreprises.fr.

2.2. Lieux d'exécution des prestations

Selon les besoins liés aux méthodologies des tests, la prestation pourra être réalisée à distance et / ou dans les locaux de l'Agence. Les modalités de cette organisation devront cependant intégrer les contraintes internes et externes à l'entreprise.

2.3. Délai d'exécution

Compte tenu de l'objectif, le prestataire retenu s'engage à réaliser la prestation selon le planning suivant :

Lancement de la prestation : Décembre 2020

Livrable audit du socle de développement Web : fin Décembre 2020

Réalisation livrables tests d'intrusion : Janvier 2021

2.4 Date limite et modalités de dépôt

Les dossiers de réponses complets pourront être transmis jusqu'au 07 décembre 2020, 12h00.

Compte-tenu du contexte sanitaire, les dossiers pourront être déposés par mail à l'adresse si@arae.fr.

Article 3 – Contenu des offres et critères d'évaluation

Auvergne-Rhône-Alpes Entreprises attend des prestataires consultés une grille tarifaire détaillant **le coût** de chacune des prestations attendues (devis à option), listées précédemment, et repris ci-dessous sachant que toute proposition complémentaire sera étudiée avec la plus grande attention :

-

Le coût, bien que très important (30%), ne sera pas le seul critère de sélection du prestataire.
La valeur technique de l'offre (70% ?) sera étudiée , notamment au regard des éléments suivants :

- Références sur la réalisation de missions similaires
- Certifications
- Pertinence de la méthodologie employée
- Compétences des intervenants et interlocuteurs
- Présentation claire et précise du déroulement des différentes phases des prestations demandées
- Pertinence, transparence et exploitabilité des livrables proposés

Nous attendons enfin des prestataires consultés un dossier présentant leur structure et les moyens humains et techniques qui seront mis à notre disposition pour chacune des prestations, ainsi que des références sur chacune des prestations proposées.

L'Agence se réserve la possibilité d'engager une négociation :

- Soit avec l'ensemble des candidats ayant présenté une offre
- Soit – sous réserve d'un nombre suffisant de candidats – avec les 2 candidats ayant obtenu les meilleures notes à l'issue d'un premier classement, au vu des critères de jugement des offres

Toutefois, l'Agence pourra attribuer le marché sur la base des offres initiales sans négociation. Il est donc dans l'intérêt du candidat d'optimiser son offre dès la remise de celle-ci.

Les négociations pourront prendre la forme d'un entretien ou d'un échange de mails.

Les candidats admis à la négociation seront informés des modalités et des échéances de la négociation par voie électronique.

La négociation pourra, si besoin, se dérouler en plusieurs phases. Elle portera sur tous les éléments de l'offre, y compris le prix.

En outre, indépendamment de toute négociation, l'Agence se réserve la possibilité de demander au candidat toute précision qu'elle jugera nécessaire à la bonne compréhension de son offre (sans que cela ne modifie l'offre émise par le candidat). Ces éléments devront être fournis dans les 5 jours suivant l'envoi d'une demande.

Article 4 – Intervenants

Le pouvoir adjudicateur est l'Agence Auvergne-Rhône-Alpes Entreprises, représentée par sa Directrice Générale en exercice.

Adresse : Immeuble Empreinte, 30 quai Perrache, 69002 Lyon

Dossier suivi par :

- Hervé MIALON, Chef de projet hmialon@arae.fr
- Yohan MENA, chef de projet ymena@arae.fr

La structure contractante signataire du marché est désignée ci-après par le « titulaire ».

Article 5 - Type de contrat et procédures

Le présent contrat est un marché sans publicité ni mise en concurrence, passé en application de l'article R. 2122-8 du Code de la commande publique (« CCP » ci-après). Le besoin satisfait par ce contrat, et par conséquent son montant, sont inférieurs à 40 000 € HT.

Article 6 - Durée du marché

La **durée du marché** est fixée à 3 mois à compter de sa notification. L'entrée en vigueur du marché débute à compter de la date de notification.

Le marché n'est pas reconductible.

Article 7 - Prix du marché

7.1. Paiement du marché

Le règlement des dépenses se fera par chèque ou par virement bancaire.

Le délai pour régler les sommes dues est de 30 jours fin de mois ou 60 jours à compter de la date d'émission de la facture.

7.2. Détermination du prix

Les prix du marché sont réputés établis sur la base des conditions économiques du mois de réception des offres. Les prix ne sont pas révisables.

Le montant total du marché n'excèdera pas 40 000€ HT.

7.3. Application de la TVA

Il sera fait application des taux de TVA en vigueur au jour d'émission de l'ordre d'exécution des prestations, sauf disposition réglementaire contraire.

Article 8 – Présentation des demandes de paiement

Les factures seront établies au nom d'Auvergne-Rhône-Alpes Entreprises et adressées à l'adresse : Immeuble Empreinte – 30 quai Perrache – 69002 LYON.

Les factures comporteront les mentions suivantes :

- Date de l'émission de la facture
- Désignation de l'émetteur et du destinataire de la facture
- Les références du marché ou le numéro du bon de commande émis par l'Agence
- La date d'exécution des prestations
- La quantité et la dénomination précises des prestations réalisées
- Le prix unitaire HT des prestations
- Le montant total HT et TTC

Les modalités de facturation pourront être revues pendant le marché et feront éventuellement l'objet d'un avenant.

Article 9 – Assurance

Le titulaire doit contracter les assurances permettant de garantir sa responsabilité à l'égard du pouvoir adjudicateur et des tiers, victimes d'accidents ou de dommages causés par l'exécution des prestations.
Le titulaire doit justifier, dans un délai de quinze jours à compter de la notification du marché et avant tout début d'exécution de celui-ci, qu'il est titulaire de ces contrats d'assurances, au moyen d'une attestation établissant l'étendue de la responsabilité garantie.

À tout moment, durant l'exécution du marché, le titulaire doit être en mesure de produire cette attestation, sur demande du pouvoir adjudicateur et dans un délai de quinze jours à compter de la réception de la demande.

Article 10 - Pénalités – Résiliation

Toute défaillance grave constatée dans l'accomplissement du marché, qu'elle mette en cause le comportement d'un employé ou l'organisation du travail par le titulaire, notamment à partir de faits ou de comportements contrevenant aux instructions ou obligations définies au présent contrat peut donner lieu de la part du pouvoir adjudicateur à l'application de pénalités.

Toute défaillance donnant lieu à pénalité doit être confirmée par courrier avec Accusé de Réception adressé au titulaire par le représentant de l'Agence dans les 15 jours suivant les faits constatés.

10.1. Pénalités d'inexécution

En cas d'inexécution totale ou partielle de la mission prévue, une pénalité forfaitaire de 100 € par jour pourra être appliquée, sans mise en demeure préalable, sur le montant HT des prestations, en cas de non-respect des délais contractuels.

Lorsque le montant des pénalités atteindra un montant global de 500 €, le pouvoir adjudicateur se réserve la possibilité de rompre le marché aux torts exclusifs du titulaire entrainant l'exécution à ses frais et risques ainsi que d'exclure définitivement celui-ci du marché.

De même, Auvergne-Rhône-Alpes Entreprises peut résilier le marché pour faute du titulaire notamment dans les cas suivants :

A. Le titulaire contrevient aux obligations légales ou réglementaires relatives au travail ou à la protection de l'environnement ;

B. Le titulaire ne s'est pas acquitté de ses obligations dans les délais contractuels ;

C. Le titulaire a fait obstacle à l'exercice du droit de contrôle par le pouvoir adjudicateur ;

D. Le titulaire n'a pas produit les attestations d'assurances dans les conditions prévues par le présent contrat (article 9);

E. Le titulaire déclare ne pas pouvoir exécuter ses engagements ;

F. Le titulaire s'est livré, à l'occasion de l'exécution du marché, à des actes frauduleux ;

G. L'utilisation des résultats par le pouvoir adjudicateur est gravement compromise, en raison du retard pris par le titulaire dans l'exécution du marché.

H. Postérieurement à la signature du marché, le titulaire a fait l'objet d'une interdiction d'exercer toute profession industrielle ou commerciale ;

Sauf dans les cas prévus aux E et H ci-dessus, une mise en demeure, assortie d'un délai d'exécution, doit avoir été préalablement notifiée au titulaire et être restée infructueuse. Dans le cadre de la mise en demeure, le pouvoir adjudicateur informe le titulaire de la sanction envisagée et l'invite à présenter ses observations.

Dans le cas prévu au C ci-dessus, les stipulations prévues à l'article 11 ci-dessous s'appliquent.

La résiliation du marché ne fait pas obstacle à l'exercice des actions civiles ou pénales qui pourraient être intentées contre le titulaire.

10.2. Règlement des pénalités

Les pénalités viendront en déduction de la facture suivant leur constatation ou du marché pendant la réalisation duquel a eu lieu le fait générateur.

En cas de non prise en compte par le titulaire lors de la facturation, l'établissement concerné effectuera lui-même la réduction de prix correspondante lors de la réception de la facture.

Le montant des pénalités pouvant être infligé au prestataire n'est pas plafonné.

Article 11 – Contrôle – Suivi du marché

Auvergne-Rhône-Alpes Entreprises se réserve le droit de contrôler à tout moment la bonne exécution des prestations du prestataire par le biais d'un de ses représentants.

Toute non-conformité observée dans l'exécution du marché donnera lieu à l'émission d'une fiche ou lettre de non-conformité éditée par Auvergne-Rhône-Alpes Entreprises et communiquée au prestataire, transmise, selon l'urgence, par tous les moyens à disposition (courriel, lettre avec AR).

La fiche comprend une partie strictement réservée au prestataire. Celui-ci est tenu d'y répondre dans les plus brefs délais (selon l'urgence) et au plus tard sous 3 jours francs, en précisant les mesures correctives qu'il aura prises afin que la non-conformité ne se renouvelle plus. La réponse doit être adressée à Auvergne-Rhône-Alpes Entreprises.

Au regard du dysfonctionnement lié à la non-conformité observée, de non-réponse aux fiches ou de non amélioration de la prestation, une mise en demeure sera envoyée au prestataire. Le prestataire est tenu de présenter ses observations dans un délai de 7 jours.

Après une seconde lettre de mise en demeure, le marché sera résilié aux torts du prestataire, sans que celui-ci puisse prétendre à des indemnités.

11.1. Modification dans la structure des prestataires

En cas de changement important dans la structure du prestataire, entraînant ou non la création d'une nouvelle personne morale, de tout projet de fusion ou d'absorption de la structure juridique du prestataire et de tout projet de cession, le prestataire s'engage à en informer Auvergne-Rhône-Alpes Entreprises sous huit jours.

Cession / Transfert du marché :

Dans le cas où le prestataire entend céder le contrat, il ne pourra le faire qu'après avoir obtenu l'accord de Auvergne-Rhône-Alpes Entreprises.

Celle-ci se réserve le droit de ne pas accepter le transfert de contrat en cas de cession partielle.

En cas d'acceptation de la cession du contrat par Auvergne-Rhône-Alpes Entreprises, elle fera l'objet d'un avenant constatant le transfert au nouveau prestataire.

Redressement et liquidation judiciaires :

Le prestataire doit aviser Auvergne-Rhône-Alpes Entreprises dès qu'un jugement de redressement ou de liquidation judiciaire est prononcé à son égard.

Le marché est résilié si la personne chargée de l'administration, de la cession ou de la liquidation n'use pas de la faculté qui lui est offerte par la loi de poursuivre l'exécution du marché.

La résiliation prend effet à la date, soit de la décision de ladite personne de renoncer à la poursuite de l'exécution du marché, soit à l'expiration du délai fixé par la mise en demeure adressée, par lettre recommandée avec avis de réception à cette personne si cette dernière n'a pas fait part de sa décision.

La résiliation peut donner lieu à des dommages-intérêts au profit de Auvergne-Rhône-Alpes Entreprises.

11.2. Confidentialité

Le prestataire est tenu au secret professionnel et à l'obligation de discrétion pour tout ce qui concerne les faits, informations, études et décisions relatifs à des interlocuteurs - personnes morales ou physiques - dont il aura eu connaissance au cours de l'exécution des travaux et sans limitation de durée après la fin de ceux-ci. Il s'interdit notamment toute communication écrite ou verbale relative à cette prestation et toute remise de documents à des tiers sans l'accord préalable de Auvergne Rhône-Alpes Entreprises.

Article 12 – Modifications et litiges

Le présent marché pourra être modifié par avenant.

Il est formellement spécifié qu'en aucun cas ou pour quelque motif que ce soit, les contestations qui pourraient survenir entre Auvergne-Rhône-Alpes Entreprises et les prestataires ne pourront être invoquées par ces derniers comme cause d'arrêt ou de suspension même momentanée, des prestations à effectuer.

En cas de litige, le droit français est seul applicable. Les tribunaux français sont seuls compétents et plus précisément le Tribunal Judiciaire de Lyon.

Fait en un exemplaire original à :
Le candidat : Le : Mention manuscrite « Lu et accepté » Cachet de la structure et signature
Auvergne-Rhône-Alpes Entreprises : Le : Cachet de la structure et signature