TERMES DE RÉFÉRENCE

Titre du Projet: Technologies de l'Information et de la Communication

Énoncé des travaux: Services de conseil pour mener des tests de vulnérabilité et de pénétration sur le réseau d'ECREEE.

Date de début : Dès que possible.

1. Contexte

Le Centre de la CEDEAO pour les Énergies Renouvelables et l'Efficacité Énergétique (ECREEE) a été créé en 2010, en réponse à la crise énergétique à laquelle sont confrontés les États membres de la région de l'Afrique de l'Ouest. L'objectif global d'ECREEE est de contribuer au développement économique, social et environnemental durable en Afrique de l'Ouest, en améliorant l'accès à des services énergétiques modernes, fiables et abordables, la sécurité énergétique et la réduction des émissions de gaz à effet de serre énergétique (GES, pollution locale) liées à l'énergie. Plus spécifiquement, ECREEE vise à créer des conditions-cadres favorables pour les marchés régionaux des Énergies Renouvelables (EnR) et de l'Efficacité Énergétique (EE) en soutenant les activités visant à atténuer les obstacles technologiques et financiers existants.

Dans le cadre de son mandat, ECREEE a acquis divers systèmes d'information et de communication à son siège, afin de soutenir efficacement ses opérations d'affaires. Compte tenu de la tendance actuelle en matière de cybersécurité, il est important de protéger ces systèmes et les informations qui y sont liées contre les cyberattaques et autres menaces pour la sécurité. L'un de ces moyens consiste à évaluer périodiquement leur vulnérabilité et leurs faiblesses, afin d'atténuer efficacement la probabilité d'une attaque. À cette fin, ECREEE recherche les services d'un professionnel qualifié en TI pour effectuer une évaluation de la sécurité de son réseau.

2. Objectifs

Le consultant mènera une évaluation de la vulnérabilité du réseau et un test de pénétration pour déterminer les faiblesses et l'exposition du réseau d'ECREEE. Il/elle effectuera une analyse et un examen indépendants sur la sécurité et les processus du réseau d'ECREEE, afin d'identifier les vulnérabilités du réseau, ses forces et ses faiblesses dans la détection et la prévention des attaques contre le réseau.

3. Portée des travaux

Les tâches à effectuer comprendront une évaluation complète de la vulnérabilité du réseau externe et interne et des tests d'intrusion, sans se limiter à: l'évaluation de la Téléphonie, de la politique de sensibilisation à la sécurité, de la sécurité physique, de la conception d'architectures de réseaux, de la DMZ, du sans fil, de l'infrastructure virtuelle, du serveur, du pare-feu, du routeur, des commutateurs, des imprimantes, des ordinateurs, de la biométrie et d'autres configurations des systèmes du réseau.

3.1 L'évaluation de la vulnérabilité doit comprendre, sans s'y limiter, les éléments suivants:

L'évaluation des mesures de sécurité internes et externes. Effectuer des scans de vulnérabilité pour identifier toute faille de sécurité;

1. Évaluation de la sécurité sans fil;
2. Examen de tous les actifs des Technologies de l'Information;
3. L'évaluation de la sécurité de l'architecture actuelle du réseau;
4. L'évaluation de la sécurité des applications;
5. Évaluation de la sensibilisation à la sécurité du personnel d'ECREEE;
6. Évaluation de l'état général des mesures de sécurité par rapport aux menaces actuelles en matière de Cyber-sécurité.

3.2 Les services de tests d'intrusion couvriront, sans s'y limiter, les éléments suivants:

1. Tests d'intrusion dans le réseau;
2. Tests des applications Web;
3. Tests des applications des systèmes internes;
4. Tests d'ingénierie sociale.

3.3 Réseau d'ECREEE

Le réseau d'ECREEE est un réseau de taille petite à moyenne composé de quelques serveurs, pare-feux et commutateurs en grappes. Le réseau s'étend sur 4 étages avec des commutateurs de couche d'accès dans chaque étage. Il dispose d'un réseau sans fil composé de points d'accès à chaque étage, tous en grappe, et les ordinateurs comptent jusqu'à 50 points d'accès opérationnels.

4. Livrables

Les livrables comprennent:

1. Rapport et présentation de l'évaluation de la vulnérabilité du réseau.
2. Rapport et présentation des tests de pénétration.
3. Un rapport général détaillé et des présentations sur les résultats et les recommandations, incluant les risques identifiés, leur impact et les actions correctives. Ces actions seront détaillées et classées par ordre de priorité en fonction de leur impact et de leur importance, avec des étapes détaillées pour atténuer tous les risques.

5. Qualification et Expérience

Exigences minimales

- ✓ Posséder au minimum un Baccalauréat en Sécurité Informatique, Cybersécurité, Systèmes d'Information sur Ordinateur, Systèmes d'Information de Gestion ou dans tout autre domaine pertinent.
- ✓ Au moins Six (6) ans d'expérience dans l'évaluation des vulnérabilités de sécurité et dans les tests de pénétration.
- ✓ Excellentes aptitudes en communication verbale et écrite en anglaise

exigences essentielles

- ✓ Certifications pertinentes en matière de cybersécurité et d'audit de sécurité

- ✓ Excellente expérience démontrée dans l'évaluation et l'élaboration de stratégies d'atténuation pour les réseaux, les systèmes d'exploitation et les applications
- ✓ Expérience en sécurité offensive, avec la capacité de penser comme un adversaire
- ✓ Solide expérience dans le renforcement de la sécurité des systèmes d'exploitation et des applications et dans les meilleures pratiques
- ✓ Expérience avec plusieurs solutions de Microsoft, Cisco et leurs applications virtuelles connexes
- ✓ Expérience avérée du travail avec des organisations gouvernementales, régionales ou internationals
- ✓ Connaissance pratique du français et/ou du portugais;
- ✓ Une expérience de travail dans la région de la CEDEAO et des connaissances ou une expérience pertinente dans le secteur de l'énergie constituent un avantage.

6. Candidature et Évaluation

Les candidats doivent soumettre les documents suivants en Anglais,

i. Une proposition technique qui saisit a) la méthodologie pour mener à bien la mission et le calendrier détaillé de mise en œuvre.
ii. Une proposition financière en US$, y compris tous les coûts et taxes (c'est-à-dire un diagramme détaillé du temps de travail, indiquant les taux journaliers pour chaque membre de l'équipe).
iii. Le CV du consultant;
iv. Copies des certificats académiques et de tous autres documents pertinents.

L'évaluation sera basée sur les qualifications et les expériences du consultant, la qualité et la pertinence de la proposition, et le coût.

7. Date limite de dépôt des candidatures

8. **Les candidats sont priés de soumettre leurs propositions, au plus tard à 23h59 (GMT) le 22 novembre 2022, à l'adresse: itsecurity@ecreee.org**
9. Pour de plus amples informations, veuillez envoyer un courriel à: jabdulrahman@ecreee.org, en mettant en copie: adeoliveira@ecreee.org

Clause de non-responsabilité : Le consultant doit explicitement accepter que toute information collectée et analysée pendant la période contractuelle soit soumise à une clause de confidentialité des données et à un accord de non-divulgation. Tous les produits et services livrés en vertu du présent contrat deviendront la propriété exclusive d'ECREEE, y compris tous les droits d'utilisation et de distribution qui y sont liés .