TERMOS DE REFERÊNCIA

Título do Projeto: : Tecnologia de Informação e de Comunicação

Declaração de Trabalho: Serviços de consultoria para realizar testes de vulnerabilidade e penetração na rede do ECREEE.

Data de início: O mais cedo possível.

1. Contexto

O Centro da CEDEAO para as Energias Renováveis e Eficiência Energética (ECREEE) foi criado em 2010, em resposta à crise energética enfrentada pelos Estados-membros da região da África Ocidental. O objectivo global do ECREEE é contribuir para o desenvolvimento económico, social e ambiental sustentável na África Ocidental, através da melhoria do acesso aos serviços energéticos modernos, fiáveis e acessíveis, do aumento da segurança energética bem como através da redução das emissões de gases com efeito de estufa (GEE, poluição local) relacionadas com a energia. Mais especificamente, ECREEE visa criar condições-quadro favoráveis aos mercados regionais de Energias Renováveis (ER) e Eficiência Energética (EE) através do apoio a actividades destinadas a mitigar as barreiras tecnológicas e financeiras existentes.

No âmbito do seu mandato, o ECREEE adquiriu vários sistemas de informação e comunicação na sua sede, com vista a apoiar de forma eficaz as suas operações empresariais. Considerando a tendência actual em termos de Segurança Cibernética, é importante proteger estes sistemas, assim como as informações a eles relacionadas contra ataques cibernéticos e outras ameaças à segurança. Um desses meios é avaliar periodicamente os seus pontos vulneráveis e fracos, a fim de mitigar de forma efectiva a probabilidade de qualquer ataque. Neste sentido, o ECREEE está a procurar os serviços de um profissional qualificado em TI para realizar uma avaliação de segurança na sua rede.

2. Objetivos

O Consultor irá realizar uma avaliação de vulnerabilidade de rede e testes de penetração para determinar os pontos fracos e a exposição da rede do ECREEE. Conduzirá também uma análise e revisão independente sobre a segurança e os processos da rede do ECREEE, a fim de identificar as vulnerabilidades da rede, pontos fortes e fracos na detecção e prevenção de ataques contra a rede.

3. Escopo do trabalho

As tarefas a serem executadas incluirão uma avaliação completa da vulnerabilidade da rede externa e interna e testes de penetração, não se limitando a: Avaliação de Telefonia, Política de Sensibilização para a Segurança, Segurança Física, Concepção da Arquitectura de Rede, DMZ, Wireless, Infra-estruturas Virtuais, Servidor, Firewall, Roteador, Comutadores, Impressoras, Computadores, Biometria, e outras Configurações de Sistemas de Rede.

3.1 A avaliação da vulnerabilidade deve incluir, mas não se limitar a:

Avaliação das medidas de segurança Internas e Externas. Executar verificações de vulnerabilidade para identificar quaisquer falhas de segurança;

1. Avaliação da segurança sem fios;
2. Revisão de todos os activos das Tecnologias de Informação;
3. Avaliação da segurança da actual arquitectura da rede;
4. Avaliação de Segurança em Aplicativos ;
5. Avaliação da sensibilização do pessoal do ECREEE em matéria de segurança;
6. Avaliação do estado geral das medidas de segurança em relação às actuais ameaças à ciber-segurança.

3.2 Os serviços de testes de penetração abrangerão, mas não se limitarão ao seguinte:

1. Testes de Penetração na Rede;
2. Testes de Aplicações Web;
3. Testes de Aplicações de Sistemas Internos;
4. Testes de Engenharia Social.

3.3 Rede do ECREEE

A rede do ECREEE é uma rede de pequeno-médio porte composta por alguns servidores, firewalls e comutadores em clusters (agrupados). A rede estende-se por 4 andares com comutadores de camada de acesso em cada um. Possui uma rede sem fios composta por pontos de acesso em cada andar, todos em cluster, e os computadores dispõem de até 50 pontos de acesso operacionais.

4. Produtos a serem entregues

Os produtos a entregar incluem:

1. Relatório e apresentação da avaliação da vulnerabilidade da rede.
2. Relatório e apresentação dos testes de penetração.
3. Um relatório geral detalhado e apresentações dos resultados e recomendações, incluindo os riscos identificados, seu impacto e acções correctivas. Estas acções serão detalhadas e priorizadas de acordo com o seu impacto e importância, com medidas detalhadas para mitigar todos os riscos.

5. Qualificação e Experiência

Requisitos mínimos

- ✓ Possuir, no mínimo, um Bacharelato em Segurança de Informações, Segurança Cibernética, Sistemas de Informação de Computação, Sistemas de Informação de Gestão ou em qualquer outra área relevante.
- ✓ Possuir, no mínimo, Seis (6) anos de experiência em avaliação de vulnerabilidades de segurança e testes de penetração.
- ✓ Excelente domínio do idioma inglês, tanto escrito quanto falado.

Requisitos preferenciais

- ✓ Certificações relevantes de segurança cibernética e auditoria de segurança
- ✓ Experiência comprovada na avaliação e desenvolvimento de estratégias de mitigação para redes, sistemas operacionais e aplicações
- ✓ Experiência em segurança ofensiva, com capacidade de pensar como um adversário

- ✓ Sólida experiência no reforço da segurança dos sistemas operacionais e aplicações e melhores práticas
- ✓ Experiência com múltiplas soluções da Microsoft, Cisco, e suas aplicações virtuais relacionadas
- ✓ Experiência comprovada de trabalho com organizações governamentais, regionais ou internacionais
- ✓ Conhecimento prático da língua francesa e/ou portuguesa;
- ✓ Experiência de trabalho na região da CEDEAO e conhecimentos ou experiência relevante no sector da energia são uma vantagem.

6. Candidatura e Avaliação

Os candidatos devem submeter os seguintes documentos em inglês,

i. Uma proposta técnica que capta a) a metodologia para levar a cabo a atribuição e o calendário detalhado de execução.
ii. Uma proposta financeira em US$, incluindo todos os custos e impostos (ou seja, um diagrama detalhado do tempo de trabalho-experimental indicando as taxas diárias para cada membro da equipe).
iii. Curriculum Vitae do Consultor;
iv. Cópias de certificados académicos e quaisquer outros documentos relevantes

A avaliação será baseada nas qualificações e experiências do Consultor, na qualidade e relevância da proposta, e no custo.

7. Data-limite de entrega das candidaturas

8. **Os candidatos devem apresentar as suas candidaturas até às 23:59 hrs (GMT) do dia 22 de Novembro de 2022, através do endereço: itsecurity@ecreee.org**
9. Para informações adicionais, por favor envie um email para:jabdulrahman@ecreee.org e copie: adeoliveira@ecreee.org

Declaração de exoneração de responsabilidade: O Consultor deve concordar explicitamente que qualquer informação recolhida e analisada durante o período contratual está sujeita a uma cláusula de confidencialidade de dados e a um acordo de não-divulgação. Todos os produtos e serviços fornecidos ao abrigo deste contrato passarão a ser propriedade exclusiva do ECREEE, incluindo todos os direitos de utilização e distribuição associados ao mesmo.