**Atividade: Análise de fortalecimento de rede**

Nesta atividade, será apresentado a você um cenário sobre uma organização de mídia social que recentemente sofreu uma grande violação de dados causada por vulnerabilidades não detectadas. Para resolver a violação, você identificará algumas ferramentas comuns de proteção de rede que podem ser implementadas para proteger a segurança geral da organização. Em seguida, você selecionará uma vulnerabilidade específica que a empresa possui e proporá diferentes métodos de proteção de rede. Por fim, você explicará como os métodos e ferramentas escolhidos serão eficazes para gerenciar a vulnerabilidade e como evitarão possíveis violações no futuro.

**Cenário**

Você é um analista de segurança que trabalha para uma organização de mídia social. A organização sofreu recentemente uma grande violação de dados, que comprometeu a segurança das informações pessoais dos seus clientes, tais como nomes e endereços. Sua organização deseja implementar práticas robustas de proteção de rede que possam ser executadas de forma consistente para evitar ataques e violações no futuro.

Depois de inspecionar a rede da organização, você descobre quatro vulnerabilidades principais. As quatro vulnerabilidades são as seguintes:

* Os funcionários da organização compartilham senhas.
* A senha de administrador do banco de dados é definida como padrão.
* Os firewalls não possuem regras para filtrar o tráfego que entra e sai da rede.
* A autenticação multifator (MFA) não é usada.

Se nenhuma ação for tomada para resolver essas vulnerabilidades, a organização corre o risco de sofrer outra violação de dados ou outros ataques no futuro.

Nesta atividade, você escreverá uma avaliação de risco de segurança para analisar o incidente e explicar quais métodos podem ser usados ​​para proteger ainda mais a rede.

**Passo 1: Acesse o modelo**

Arquivo “*Relatório de avaliação de risco de segurança*”

**Passo 2: Acessar os materiais de suporte**

Arquivo “*2 SUPORTE Ferramentas de proteção de rede”*

**Passo 3: Selecione até três ferramentas e métodos de proteção para implementar**

Pense em todas as ferramentas e métodos de proteção de rede que você aprendeu neste curso e que podem proteger a rede da organização contra ataques futuros. Que tarefas de reforço seriam a forma mais eficaz de responder a esta situação?

**Passo 4: Documente o incidente**

Você recomendou uma ou duas práticas de reforço de segurança para ajudar a evitar que isso ocorra novamente no futuro. Explique por que a ferramenta ou método de reforço de segurança selecionado é eficaz para resolver a vulnerabilidade. Aqui estão algumas perguntas para você começar:

* Por que a técnica de reforço de segurança recomendada é eficaz?
* Com que frequência a técnica de endurecimento precisa ser implementada?

Escreva sua resposta na segunda parte da planilha.

**O que incluir em sua resposta**

Certifique-se de atender aos seguintes critérios em sua atividade concluída:

* Uma a três ferramentas e métodos de proteção de rede.
* As razões pelas quais as ferramentas e métodos selecionados são eficazes

**Exemplo Concluído**

Arquivo “*Security risk assessment report exemplar*”

**Avaliação do Exemplo**

Compare o exemplar com sua atividade concluída. Revise seu trabalho usando cada um dos critérios do exemplar. O que você fez bem? Onde você pode melhorar? Use suas respostas a essas perguntas para orientá-lo à medida que avança no curso.

**Nota**: O exemplo representa uma explicação possível para os problemas que a organização de mídia social enfrenta. Existem várias ferramentas e métodos corretos de reforço de segurança para usar. O importante é que você tenha identificado as medidas de fortalecimento da rede mais eficazes para gerenciar as vulnerabilidades selecionadas. Em sua função como analista de segurança, você e sua equipe explicariam suas decisões e argumentariam por que essas medidas serão eficazes para proteger a rede.

O exemplo foca na vulnerabilidade de um software desatualizado para um banco de dados local. Uma solução potencial para a vulnerabilidade é identificada e incluída no relatório para os supervisores diretos. O relatório explica como a empresa poderá ser comprometida no futuro se o banco de dados não for corrigido e se os funcionários continuarem a compartilhar senhas.

Na seção sobre a política de segurança da informação da organização, o relatório inclui informações sobre a adição de práticas gerais de reforço de segurança, uma recomendação sobre a frequência com que as práticas de reforço devem ser executadas e uma explicação sobre quais são as possíveis consequências se a política não for seguida. Este é um exemplo de como um relatório de avaliação de riscos de segurança pode ser analisado e como uma política de segurança da informação pode ser escrita.