Relatório de avaliação de risco de segurança

Análise de fortalecimento de rede

Introdução

Coletar informações sobre o cenário e verificar as necessidades, após análise, com base nos problemas de segurança que serão apresentados, deve-se apresentar ferramentas e soluções e explicar o do porquê de cada decisão.

Cenário

Você é um analista de segurança que trabalha para uma organização de mídia social. A organização sofreu recentemente um grande vazamento de dados, que comprometeu a segurança das informações pessoais de seus clientes, como nomes e endereços. Sua organização deseja implementar práticas fortes 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 têm 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.

Relatório de avaliação de risco de segurança

Análise de fortalecimento de rede

Parte 1

Selecione até três ferramentas e métodos de proteção para implementar:

1. Treinamento sobre segurança para os funcionários, com o foco de entender os riscos e como utilizar recursos de segurança.
2. Usar o Terminal para administrar as portas em cada dispositivo com o iptables.
3. Utilizar ferramenta SIEM para acompanhar o tráfego de redes dos funcionários.

Parte 2

Explique suas recomendações:

1. É importante treinar todos os usuários para mostrar os riscos em compartilhar suas senhas, e também, ensiná-los a como criar senhas seguras e como administrá-las, e por fim, ensinar a utilizar recursos adicionais de segurança como a MFA, para que haja ainda mais segurança na empresa.
2. No iptables você pode determinar quais portas entram e saem, por vias de segurança absoluta, é interessante bloquear todas as portas de entrada, fazendo com que apenas haja saída nas portas do dispositivo, porém, é importante também selecionar portas especificas de saída, como por exemplo, HTTPS 443, HTTP 80, DNS 53 e outra caso seja necessário. Assim, fica muito mais estruturada a segurança da rede, dispositivos e funcionários.
3. A ferramenta SIEM pode ser a critério de escolha da equipe de segurança, porém, a ideia é ter uma para monitorar a atividade dos funcionários e o tráfego de dados, para que, caso haja alguma anomalia na rede, ou algum possível ataque, esse monitoramento pode fazer com que a equipe de segurança esteja preparada para lidar com o probelma.