Atividade 1 - Clique aqui para entregar

Atividade 1

Contexto

Um dos clientes – uma loja de eletrônicos do sistema para vendas oferecido pela empresa de desenvolvimento de *software* onde você trabalha – relatou problemas graves com o banco de dados. Os problemas foram os seguintes:

- Um acesso indevido aconteceu no banco de dados. As hipóteses são de SQL *injection* ou de uso indevido de *login* e senha de funcionário.
- O acesso indevido apagou dados das tabelas de venda e pagamento.
- Um dos funcionários da loja emite periodicamente alguns relatórios com consultas diretas ao banco de dados. Essa pessoa, ao tentar ajudar, acabou removendo ainda duas tabelas. Nota-se que ela usava usuário **root**.
- O último *backup* anterior ao desastre aconteceu duas semanas antes. Houve perda de dados, embora, felizmente, a partir das notas fiscais físicas, a loja tenha conseguido recadastrar boa parte das vendas desse período.

Diante dessa situação, a equipe de desenvolvimento precisa agir baseada em procedimentos que diminuam os riscos de um desastre semelhante acontecer no futuro.

Atividade

Crie, em sua máquina, o banco de dados definido pelo *script* disponível em **Conteúdo > Material complementar** e analise e execute as seguintes ações de segurança:

1. Crie um usuário específico para relatórios. Crie *role* para ele, com acesso apenas à consulta em tabelas (nem dados, nem estrutura podem ser alterados).
2. Crie usuário e *role* para funcionário, o qual pode manipular as tabelas de venda, cliente e produto, mas não deve ter acesso (nem para consulta) a funcionário e cargo e não deve ser capaz de realizar alterações de estrutura em nenhuma tabela.
3. Escolha um método de criptografia ou *hash* para aplicar às senhas dos usuários. Atualize a tabela "usuário" aplicando a criptografia ou *hash* ao campo de senha em todos os registros.
4. Elabore um plano de *backups* regular, montando um *script* de servidor Linux para rodar periodicamente (especifique o período) ou um agendamento usando uma ferramenta automatizada.

Para os itens 1, 2 e 3, grave em **scripts .sql** os comandos utilizados. Para o item 4, envie um relatório com evidências do plano de *backup*, informando ainda a periodicidade recomendada.

Entrega

Envie um arquivo compactado (ZIP, RAR ou 7z), contendo os *scripts* criados e o relatório de *backup*, no local destinado à entrega da atividade, até a data indicada no cronograma de estudos.

Dica de leitura

Para esta atividade, leia os seguintes materiais:

- Recuperação de dados
- Segurança do banco de dados

Avaliação

Nesta atividade, você será avaliado nos indicadores:

- *Mantém rotina de* backup *e restauração de acordo com parâmetros de segurança definidos para o sistema.*
- *Monitora segurança do banco de dados de acordo com parâmetros definidos para o sistema.*