Fundação Universidade do Oeste de Santa Catarina
UNOESC – Campus Videira
Prof: Fabiano Wonzoski
Acadêmico: Kauan Degenhart Dos Santos

ESTUDO DE CASO

Você trabalha em uma empresa de segurança de informação, e foi contratado para fazer a auditoria de segurança de informação, cujo o cenário é seguinte:

- A empresa tem um servidor linux
- Algum usuário mal intencionado acessou o servidor da empresa e modificou o senha do root do servidor que era @@@senha###, atualmente os profissionais da empresa não sabem mais a senha e como acessar.
- Existem dois usuários que tem credenciais de acesso ao servidor (Paulo, Pedro), mas inicialmente não se sabe se foram eles que podem ter fornecido as senha
- O dono da empresa não sabe dizer se o servidor está rodando algum serviço desnecessário, mas sabe-se que foi disponibilizada uma página em algum dos servidores com um conteúdo indicando que a empresa foi invadida.
- Foram roubadas várias senhas, não somente do ambiente computacional, mas também de outros controles de acesso da empresa.

Diante da situação apresentada, e você como profissional da segurança da informação, pode apontar quais foram os princípios da segurança da informação foram violados?

Resolução do Estudo de Caso – Segurança da Informação

Fundamentação Teórica Aplicada

Para a elaboração da presente resolução, foram utilizados como base os princípios fundamentais da Segurança da Informação, conforme definidos por normas como a ISO/IEC 27001 e 27002. Esses princípios são fundamentais para proteger ativos de informação e orientar decisões em situações de risco. Os pilares considerados foram:

- Confidencialidade: Garantia de que a informação é acessível apenas por pessoas autorizadas.
- Integridade: Garantia da exatidão e completude da informação e dos métodos de processamento.
- Disponibilidade: Garantia de que usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário.
- Autenticidade: Garantia de que a informação é proveniente de fonte confiável.
- Responsabilidade (accountability): Rastreabilidade das ações de usuários para atribuição de responsabilidades.

Análise da Situação e Princípios Violados

A seguir, são destacados os principais princípios da segurança da informação que foram violados na situação apresentada:

- Confidencialidade:

Houve roubo de senhas, tanto do ambiente computacional quanto de outros sistemas da empresa. Isso indica que informações sensíveis foram expostas a agentes não autorizados.

- Integridade:

A alteração da senha do root sem autorização representa uma modificação indevida em um ativo crítico do sistema. A publicação de uma página informando que a empresa foi invadida também viola a integridade dos sistemas.

- Disponibilidade:

A equipe não consegue acessar o servidor, pois a senha do root foi modificada. Isso compromete a continuidade dos serviços e o funcionamento normal da empresa.

- Autenticidade:

A presença de uma página falsa ou modificada no servidor compromete a autenticidade das informações divulgadas pela empresa.

- Responsabilidade:

A ausência de registros e controles impede a identificação do responsável pela ação. Faltam mecanismos de rastreamento, como logs e autenticação robusta.

Considerações Finais e Recomendações

A situação apresentada reflete uma grave falha na governança da segurança da informação, incluindo:

- Falta de políticas de controle de acesso e autenticação;
- Ausência de monitoramento de atividades e logs;
- Negligência na gestão de riscos e ativos de informação.

Como recomendações iniciais, propõe-se:
- Levantamento de serviços ativos no servidor para identificar vulnerabilidades;
- Aplicação de auditoria de acessos e análise de logs;
- Restabelecimento da senha root via modo de recuperação (rescue mode);
- Reforço nas políticas de senhas e controle de acesso;
- Implantação de sistemas de detecção de intrusão (IDS) e sistemas de gestão de identidade.