RESOLUÇÃO DOS ESTUDOS DE CASO: SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS

1. Introdução

A segurança da informação em ambientes corporativos vai além da implementação de ferramentas tecnológicas. Ela depende de políticas organizacionais claras, infraestrutura de proteção (como firewalls e servidores proxy), bem como da conscientização dos colaboradores. Este trabalho apresenta a análise e resolução de dois estudos de caso abordando falhas e controles relacionados à criptografia, firewalls e proxies, conforme discutido por Whitman e Mattord (2022).

2. Estudo de Caso 1: Criptografia e Firewalls

2.1 Utilização de Criptografia no Servidor Web

O servidor Web da empresa Linen Planet utiliza criptografia do tipo SSL/TLS, conforme indicado pelo ícone de segurança (cadeado) no navegador da intrusa. Essa tecnologia garante:

- Confidencialidade: impede que terceiros leiam os dados transmitidos.
- Integridade: assegura que os dados não foram alterados durante a transmissão.
- Autenticidade: confirma que o cliente está se comunicando com o servidor legítimo.

Apesar disso, a violação da segurança ocorreu por meio de engenharia social e escuta física em ambiente público, evidenciando uma falha de segurança comportamental.

2.2 Medidas de Segurança Recomendadas

Para prevenir esse tipo de incidente, são recomendadas as seguintes medidas:

- Autenticação multifator (MFA);
- Proibição de compartilhamento de senhas;
- Treinamento contínuo em segurança da informação;
- Acesso remoto seguro por VPN;
- Utilização de senhas temporárias ou tokens;
- Monitoramento de acessos e alertas de segurança.

Esse caso ilustra que, mesmo com criptografia e firewalls, falhas humanas continuam sendo grandes ameaças.

3. Estudo de Caso 2: Servidores Proxy e Firewalls em Nível de Aplicação

3.1 Análise da Política de Uso da Web

A política de uso da internet da ATI, embora rígida, é justificada do ponto de vista organizacional. Ela protege os sistemas, controla o uso da largura de banda, previne riscos legais e mantém a produtividade. O uso de proxies permite filtrar conteúdos, controlar acessos e monitorar atividades online de forma eficaz.

3.2 Avaliação da Conduta de Ron

Ron Hall, embora com boas intenções, agiu de maneira imprudente ao violar conscientemente uma política de segurança da empresa. Mesmo sendo um funcionário confiável, ele tentou acessar sites bloqueados repetidamente, o que configura desrespeito às normas internas.

3.3 Ação Recomendada ao Gestor

Andy, supervisor de Ron, deve adotar uma abordagem equilibrada:
- Conversar com Ron sobre a importância de seguir políticas de segurança;
- Reforçar a confiança depositada no funcionário, sem ignorar a violação;
- Apoiar a participação de Ron no curso exigido;
- Comunicar ao setor de segurança, caso julgue o ato como não intencional.

Essa abordagem respeita tanto a política da organização quanto o histórico do funcionário.

4. Conclusão

Os estudos de caso demonstram que a segurança da informação é resultado de uma combinação entre tecnologia, políticas organizacionais e comportamento humano. Ferramentas como firewalls, criptografia e servidores proxy são eficazes, mas a educação e a cultura de segurança são fundamentais para mitigar riscos.