Estudo de Casos

1. Introdução

Proteger informações em empresas envolve mais do que apenas instalar recursos tecnológicos. Isso requer diretrizes internas bem definidas, estrutura de defesa como firewalls e servidores intermediários (proxy), além de uma equipe de funcionários bem orientada. Este documento analisa e propõe soluções para dois cenários práticos que tratam de falhas de segurança e controles envolvendo criptografia, firewalls e proxies, conforme os conceitos de Whitman e Mattord (2022).

2. Estudo de Caso 1: Criptografia e Firewalls

2.1 Utilização de Criptografia no Servidor Web

A empresa Linen Planet adotou criptografia SSL/TLS em seu servidor web, como indicado pelo ícone de cadeado no navegador da atacante. Essa tecnologia assegura:

- Privacidade: impede que terceiros visualizem os dados em trânsito;
- Consistência: garante que as informações cheguem sem modificações;
- Verificação de identidade: confirma que o usuário está se comunicando com o servidor verdadeiro.

Entretanto, o ataque à segurança foi possível por meio de manipulação social e escuta presencial em local público, revelando um problema relacionado ao comportamento humano.

2.2 Medidas de Segurança Recomendadas

Para evitar situações semelhantes, são indicadas as seguintes práticas:

- Uso de autenticação com múltiplas etapas (MFA);
- Proibição de dividir senhas entre colaboradores;
- Capacitação contínua sobre segurança digital;
- Acesso remoto seguro via rede privada virtual (VPN);
- Emprego de códigos temporários ou dispositivos de autenticação;

- Registro e monitoramento constante dos acessos e eventos suspeitos.

Esse exemplo evidencia que, mesmo com recursos como criptografia e firewalls, o fator humano ainda representa um dos maiores riscos à segurança.

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

3.1 Análise da Política de Uso da Web

As regras de navegação da empresa ATI, mesmo sendo rigorosas, têm sua razão de ser dentro do contexto corporativo. Elas ajudam a manter a segurança da infraestrutura, otimizam o uso da rede, reduzem riscos legais e promovem a eficiência no trabalho. O uso de servidores proxy permite bloquear conteúdos inadequados, limitar acessos e observar os hábitos online dos usuários.

3.2 Avaliação da Conduta de Ron

Embora Ron Hall não tivesse más intenções, sua atitude foi arriscada ao violar propositalmente as diretrizes da empresa. Mesmo sendo um colaborador confiável, ele insistiu em acessar sites não permitidos, contrariando as normas estabelecidas.

3.3 Ação Recomendada ao Gestor

Andy, o gestor responsável, deve adotar uma postura equilibrada diante da situação:

- Ter um diálogo com Ron explicando a importância de obedecer às regras de segurança;
- Reforçar a confiança existente, sem deixar de reconhecer o erro;
- Incentivar que Ron participe do curso de reciclagem exigido;
- Notificar a equipe de segurança caso entenda que a ação foi inconsciente.

Essa conduta permite alinhar a política da empresa com a consideração pelo histórico positivo do colaborador.

4. Conclusão

Os casos analisados evidenciam que a proteção da informação depende de uma sinergia entre soluções tecnológicas, diretrizes internas e atitudes conscientes. Ferramentas como firewalls, criptografia e proxies são essenciais, mas a chave para reduzir ameaças está no conhecimento e na cultura organizacional voltada à segurança.