Universidade São Judas Tadeu

Eduardo Cecilio Alves Santos – RA:824224719

Projeto A3 - UC Ambientes Computacionais e Conectividade

Estudo De Caso 1

São Paulo

2025

Questão 1. O firewall e o servidor Web usados pela Linen Planet fornecem serviços de criptografia?

Em caso afirmativo, que tipo de proteção estava em vigor?

R:Sim.
A evidência está na frase:

“Ela notou que o ícone de segurança estava aparecendo na parte inferior da janela do navegador. A criptografia entre seu navegador e o servidor estava agora em vigor.”

Isso indica que a conexão entre o navegador de Maris e o servidor da Linen Planet estava protegida por criptografia TLS (Transport Layer Security), que é a tecnologia padrão para proteger dados transmitidos pela web (o famoso “HTTPS”).

Tipo de proteção em vigor:

- Confidencialidade: os dados transmitidos entre cliente e servidor são criptografados e, portanto, não podem ser facilmente interceptados por terceiros.
- Integridade: garante que os dados não foram modificados no caminho.
- Autenticidade: assegura que o servidor é realmente quem afirma ser (via certificados digitais).

Questão 2. Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?

R:Apesar da criptografia estar presente, a falha ocorreu no nível humano (engenharia social). Algumas formas de melhorar a segurança:

a) Evitar compartilhamento de senhas por voz (ou qualquer canal inseguro):

Padma compartilhou login e senha por telefone, em um ambiente público, correndo risco de ser ouvida — como de fato foi. Isso é extremamente inseguro.

b) Implementar autenticação multifator (MFA):

Mesmo que alguém obtenha o login e senha, o acesso só seria permitido mediante um segundo fator (ex: código via app autenticador, token físico ou biometria).

c) Uso de autenticação delegada com escopo limitado:

Em vez de compartilhar a senha principal, Padma poderia ter fornecido a David um acesso temporário ou token de acesso específico apenas para aprovar aquela solicitação, com validade limitada.

d) Monitoramento e alertas de segurança:

Sistemas de detecção de intrusos (IDS) ou de comportamento anômalo poderiam detectar acessos suspeitos (como um login vindo de IP incomum, ou ações fora do perfil esperado).

e) Treinamento em segurança para todos os funcionários:

É essencial que todos saibam identificar riscos, como chamadas ou situações que podem parecer urgentes mas são armadilhas — o clássico ataque de engenharia social.