Aula 7 - Estudo de caso 1

Criptografia e Firewalls*

Padma Santhanam, a CTO da Linen Planet, estava se deslocando para o trabalho de sua maneira habitual – pegando o trem da estação suburbana perto de sua casa para seu escritório em uma área comercial do outro lado da cidade. Ao virar a página do jornal da manhã, seu celular tocou. Ela olhou para o identificador de chamadas e viu que era seu assistente, David Kalb.

"Olá, David. E aí?"

“Oi, Padma. Crise aqui como sempre. Nosso representante de atendimento ao cliente na ATI está na outra linha. Ele diz que você precisa fazer login no sistema de ordem de serviço e aprovar a solicitação de alteração o mais rápido possível ou eles perderão a próxima janela de alteração para a nova versão do nosso aplicativo de crédito online.”

Padma disse: “Tudo bem. Estarei no escritório em 25 minutos ou mais. O trem acabou de sair da estação Broadmore.”

“Ele diz que eles não podem esperar tanto tempo. Você deveria fazer isso anteontem, e de alguma forma foi esquecido. Eles dizem que precisam agora ou perderemos uma semana esperando pela próxima janela de mudança.”

Padma suspirou. Então ela disse: “Tudo bem. Eu quero que você navegue no site da ordem de serviço, você sabe o que usamos em linhoplanet.biz/wo, e faça login para mim. Você pode aprovar o pedido de alteração e não perderemos a janela. Vou mudar minha senha quando chegar lá. Meu nome de usuário é papa, serra, alfa, novembro, tango, alfa. Percebido?"

David disse “Entendi. Senha?" Olhando para os dois lados primeiro, Padma abaixou um pouco a voz e disse: “Romeu, lima, oito, quatro, bang, zulu, índia, vencedor, cifrão.”

David repetiu de volta. Ele disse: “OK, estou logado agora e acabei de aprovar a ordem de serviço. Vou dizer ao nosso representante que estamos prontos para ir.”

“Obrigado, Davi.”

Na fila atrás de Padma, Maris Heath fechou o bloco de notas e fechou a caneta esferográfica. Sorrindo, ela ergueu a bolsa do laptop e se levantou para sair do trem na

próxima estação, que ela sabia que ficava bem ao lado de um cibercafé. Maris abriu seu laptop e conectou seu navegador ao servidor Linen Planet Web. O firewall pediu seu nome de usuário e senha. Ela abriu o bloco de notas e digitou os dados que havia anotado enquanto escutava a ligação do celular de Padma. Seu navegador conectou em um instante. 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. Pelo menos nenhum outro hacker poderia observá-la enquanto ela colocava um backdoor nos servidores da Web do Linen Planet.

Ela passaria várias horas nos próximos dias explorando a rede e planejando seu ataque...

Questões
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?

Resposta:
Sim, o caso descreve que havia criptografia ativa entre o navegador e o servidor Web.

Evidência: “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 o uso de SSL/TLS (Secure Sockets Layer / Transport Layer Security), protocolo que garante confidencialidade e integridade dos dados transmitidos.

Portanto, o firewall e o servidor Web estavam fornecendo proteção de comunicação criptografada (HTTPS), impedindo que terceiros interceptassem o tráfego.

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

Resposta:
O problema central não foi a ausência de criptografia, mas sim o vazamento de credenciais (usuário e senha ditados em público).
Medidas que poderiam tornar o acesso mais seguro:

- Autenticação multifator (MFA): exigir além da senha um token, código SMS ou aplicativo autenticador.
- Uso de VPN corporativa: restringir acessos externos apenas via rede segura.
- Política de gestão de credenciais: nunca compartilhar senhas verbalmente; usar cofres de senha ou sistemas de delegação de acesso.

- Treinamento de conscientização em segurança: evitar exposição de informações sensíveis em locais públicos.
- Tokens temporários ou certificados digitais: para autenticação mais robusta e menos dependente de senhas fixas.