Atividade Aula 3 –

**Ataque à Secretaria da Fazenda de São Paulo (2020)**

**Data do ataque (aproximada):**

O ataque ocorreu no final de 2020.

**Tipo de ataque:**

Ransomware.

**Descrição do ataque ou como aconteceu:**

Hackers invadiram os sistemas da Secretaria da Fazenda de São Paulo (SEF-SP) utilizando ransomware, criptografando os dados da instituição e exigindo um resgate para liberar o acesso a essas informações. O ataque impactou diversos serviços fiscais, como a consulta e emissão de documentos fiscais e a plataforma de declaração do Imposto de Renda.

**Vulnerabilidade explorada:**

O ataque pode ter explorado uma vulnerabilidade específica do sistema, mas não há informações claras sobre um CVE específico para esse incidente. Os ataques de ransomware geralmente exploram vulnerabilidades não corrigidas em sistemas desatualizados ou configurados inadequadamente.

**Impactos e/ou prejuízo (estimado):**

Paralisação de serviços fiscais: A paralisação de serviços essenciais causou transtornos significativos para cidadãos e empresas. Não há uma estimativa precisa de valores financeiros, mas a interrupção de serviços pode ter causado perdas econômicas consideráveis.

Risco de exposição de dados sensíveis: Embora os dados não tenham sido confirmados como comprometidos, o risco de roubo de informações fiscais e financeiras dos cidadãos foi uma grande preocupação.

**Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**

Implementação de backups mais robustos e sistemas de recuperação de desastres.

Treinamento contínuo em segurança cibernética para a equipe da Secretaria da Fazenda.

Atualização constante e monitoramento de sistemas para detectar vulnerabilidades.

Uso de software de proteção contra ransomware e sistemas de detecção de intrusões.

**Ataque à Conta de Neymar (2019)**

**Data do ataque (aproximada):**

O ataque ocorreu em 2019.

**Tipo de ataque:**

Phishing.

**Descrição do ataque ou como aconteceu:**

Criminosos enviaram uma mensagem falsa, se passando por uma empresa confiável ou pessoa próxima de Neymar, com um link malicioso. Neymar, sem perceber, acessou o link que levava a uma página falsa de login do Instagram e forneceu suas credenciais de acesso. Com essas credenciais, os hackers invadiram sua conta, acessaram suas fotos e mensagens privadas e começaram a manipular a conta.

**Vulnerabilidade explorada:**

O ataque explorou a falha de segurança do usuário ao não verificar a autenticidade do link recebido. Não foi uma falha no sistema em si, mas uma falha na segurança humana (engenharia social).

**Impactos e/ou prejuízo (estimado):**

Exposição de informações pessoais: Embora o foco do ataque tenha sido manipular a conta, havia o risco de exposição de dados pessoais sensíveis.

Impacto na imagem pública: O incidente gerou uma preocupação temporária sobre a segurança nas redes sociais e afetou a imagem pública de Neymar.

Possibilidade de fraude e chantagem: A conta foi usada para enganar amigos e familiares de Neymar, tentando obter informações ou até realizar solicitações financeiras.

**Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**

Ativação da autenticação de dois fatores (2FA) em todas as contas online para proteger as credenciais.

Cuidado redobrado com links desconhecidos ou de fontes suspeitas.

Uso de ferramentas de verificação de segurança de links antes de clicar em URLs desconhecidos.

Conscientização sobre os riscos de phishing e treinamentos sobre segurança cibernética.