

Atividade

Prática

03

Angelo Rodrigues

824139676

Cauã de Cerqueira Ferreira

824110637

Erick Domingues Soares

82414486

Wellington de Oliveira Sousa

8241445818

Ataque Cibernético ao STJ em 2020

Em 3 de novembro de 2020, o Superior Tribunal de Justiça (STJ) sofreu um ataque cibernético que interrompeu seus serviços por vários dias. O ataque foi causado por um ransomware, um tipo de malware que criptografa dados e exige resgate para desbloqueá-los.

Como aconteceu

O ransomware se espalhou pelos servidores do STJ, criptografando processos e documentos judiciais. Isso forçou a suspensão das atividades da corte, incluindo julgamentos e acesso aos sistemas. A falha de segurança explorada não foi oficialmente divulgada, mas acredita-se que os invasores usaram uma brecha em servidores ou protocolos de rede.

Impactos e prejuízos

O ataque paralisou o tribunal por quase uma semana, causando grandes prejuízos, tanto financeiros quanto operacionais. Embora o valor exato do prejuízo não tenha sido divulgado, a interrupção dos serviços causou grande transtorno para o funcionamento da Justiça.

Tipo de Proteção que poderia ter sido aplicada para evita-lo

Backups seguros para restaurar os dados sem pagar resgate;

Autenticação forte com múltiplos fatores;

Monitoramento de atividades suspeitas e aplicação de atualizações de segurança com regularidade.

Esse ataque destacou a necessidade de medidas robustas de segurança em órgãos públicos.

Ataque ao Banco Central do Brasil, que atingiu o sistema de PIX.

Como aconteceu

Em junho de 2021, o Banco Central divulgou que houve um vazamento de dados relacionados a chaves PIX de cerca de 160 mil usuários. Embora o ataque não tenha comprometido transações financeiras, ele envolveu o acesso indevido a informações sensíveis, como dados cadastrais (nome, CPF, e-mail, telefone).

Tipo de ataque

O incidente foi um vazamento de dados. Os invasores exploraram uma brecha de segurança em um banco participante do sistema PIX, e os dados foram expostos indevidamente.

Impactos

Embora não tenha havido roubo direto de dinheiro ou desvio de recursos, o ataque causou preocupação sobre a privacidade e segurança dos dados dos usuários. O vazamento minou a confiança no sistema PIX, que é amplamente utilizado no Brasil para pagamentos e transferências rápidas.

Tipo de Proteção que poderia ter sido aplicada para evita-lo

Criptografia de dados mais forte para proteger informações pessoais.

Monitoramento contínuo de possíveis brechas de segurança.

Auditorias regulares de segurança nos sistemas dos participantes do PIX para identificar falhas potenciais.

Esse caso mostrou a vulnerabilidade de sistemas financeiros e o impacto de vazamentos de dados, mesmo que não envolvam transações financeiras diretas.