**Casos Reais de Ataques Cibernéticos: Impactos e Soluções**

A seguir, apresento três casos reais de ataques cibernéticos, suas consequências e como as empresas conseguiram resolver ou mitigar os problemas causados:

**1. Caso do ransomware WannaCry – 2017**

O ataque do WannaCry foi um dos maiores da história. Ele afetou empresas do mundo todo, inclusive hospitais do Reino Unido, onde sistemas foram bloqueados e cirurgias precisaram ser adiadas. Esse vírus sequestrava os arquivos das máquinas e exigia pagamento em bitcoin para liberá-los.

*Consequências:* Paralisação de serviços, prejuízo financeiro e perda de dados importantes.  
*Como foi mitigado:* As empresas precisaram restaurar backups, atualizar sistemas operacionais e aplicar patches de segurança. Além disso, aumentaram o investimento em antivírus e firewalls.

**2. Ataque à empresa JBS – 2021**

A JBS, uma das maiores empresas de alimentos do mundo, foi vítima de um ataque cibernético que afetou suas operações nos Estados Unidos e na Austrália. O grupo de hackers exigiu um pagamento para liberar os sistemas.

*Consequências:* Interrupção temporária das atividades, risco de desabastecimento e prejuízo milionário.  
*Como foi mitigado:* A empresa acabou pagando um resgate em criptomoedas, mas depois reforçou suas medidas de segurança e criou planos de resposta a incidentes.

**3. Vazamento de dados do Facebook – 2019**

Neste caso, dados de mais de 500 milhões de usuários do Facebook vazaram, incluindo nomes, números de telefone e e-mails. A falha foi causada por má configuração de um banco de dados em nuvem.

*Consequências:* Exposição de informações pessoais, perda de confiança dos usuários e problemas com a legislação de proteção de dados (como a LGPD no Brasil).  
*Como foi mitigado:* O Facebook revisou suas práticas de segurança, notificou os usuários e ajustou as permissões de acesso às suas APIs e servidores.

Esses casos mostram como os ataques cibernéticos podem causar grandes prejuízos e como é essencial que as empresas invistam em segurança da informação, planos de contingência e conscientização dos funcionários.