Ataques cibernéticos recentes

Com o aumento da digitalização nos setores público e privado, incidentes de segurança cibernética têm se tornado cada vez mais comuns e com impactos significativos. O Brasil, assim como outros países, tem sofrido ataques como ransomware e extorsão digital, gerando prejuízos financeiros, danos à reputação institucional e vazamentos de dados pessoais. A seguir são apresentados dois casos notórios ocorridos no país nos últimos anos, analisando tipo de ataque, vulnerabilidades exploradas, impactos e possíveis medidas de proteção.

Caso 1: Banco de Brasília (BRB) – ataque de ransomware

Data do ataque: início de outubro de 2022 (entre os dias 5 e 7 de outubro).

Tipo de ataque: Ransomware + extorsão de dados digitais.

Descrição do ataque: Os criminosos acessaram sistemas do banco, criptografaram arquivos ou sequestraram sistemas, e exigiram resgate em bitcoins. Exigiram cerca de 50 Bitcoins para não divulgarem os dados acessados. Houve instabilidade em site, aplicativo e demais serviços bancários.

Vulnerabilidade explorada: Não há na cobertura pública confirmação de um CVE específico ou falha documentada (por exemplo, software vulnerável, plugin sem patch, etc.). A descrição aponta uso de ransomware LockBit, possivelmente explorando fraquezas em segurança de sistemas internos e credenciais de funcionários.

Impactos/prejuízos: Pedido de resgate equivalente a cerca de R$ 5,2 milhões à época. Houve instabilidade nos serviços para os clientes; a reputação institucional foi afetada. Não foi confirmado vazamento de dados de contas correntes ou impacto financeiro direto aos clientes, segundo o banco.

Tipo de proteção que poderia ser aplicada:

1. Backup regular e off-line dos dados críticos;

2. Segmentação de redes internas para limitar o acesso de credenciais privilegiadas;

3. Políticas fortes de controle de acesso e autenticação multifator;

4. Monitoramento contínuo de anomalias nos sistemas;

5. Planos de resposta a incidentes bem testados.

Fontes:

https://www.tecmundo.com.br/seguranca/250306-banco-brb-sofre-ataque-ransomware-acaba-chantageado.htm

Caso 2: Rede Record / Record TV – ataque com ransomware BlackCat / AlphV

Data do ataque: 8 de outubro de 2022.

Tipo de ataque: Ransomware (BlackCat / AlphV) + extorsão / sequestro de arquivos.

Descrição do ataque: Hackers invadiram o sistema central da emissora, criptografaram arquivos, sequestraram parte do acervo jornalístico e de entretenimento, sistemas de edição, produção e partes internas. Houve alteração da programação por conta da indisponibilidade de conteúdos. Foi pedido um resgate de US$ 5 milhões, algo em torno de R$ 25–26 milhões na época. Dados pessoais de funcionários também foram acessados.

Vulnerabilidade explorada: Da reportagem, não há informação pública clara de um CVE específico. O ataque envolveu ransomware como serviço (RaaS), que sugere que hackers usaram software comercializado/compartilhado, possivelmente explorando falhas de configuração, falta de isolamento de sistemas, credenciais inseguras ou ausência de monitoramento.

Impactos/prejuízos: Prejuízo material e de operação: emissão de programas ao vivo prejudicada, parte da programação alterada, funcionários sem acesso a ferramentas de trabalho, interrupções de produção; impacto financeiro e de imagem. Resgate solicitado de cerca de US$ 5 milhões (≈ R$ 25-26 milhões). Vazamentos de dados de funcionários. Publicação de documentos confidenciais.

Tipo de proteção que poderia ser aplicada:

1. Manter backups actualizados, isolados e testados;

2. Utilizar segmentação de sistemas críticos para que um ataque não comprometa toda a infraestrutura;

3. Políticas de autenticação forte, privilégio mínimo, controle rigoroso de credenciais de funcionários;

4. Implementar detecção precoce de intrusão e resposta a incidentes;

5. Revisões regulares de segurança, auditorias de TI, treinamento para conscientização interna.

Fontes:

https://tecnoblog.net/noticias/record-confirma-que-dados-pessoais-de-ex-funcionarios-tambem-foram-vazados

https://www.welivesecurity.com/br/2022/10/10/rede-record-sofre-ataque-cibernetico-e-tem-programacao-afetada