Paulo Henrique Luiz do Monte

RA: 82325475

Atividade proteção de dados

Ataque 1: Lojas Renner

1. Data do Ataque

O ataque ocorreu em **19 de agosto de 2021**.

2. Tipo de Ataque

Ataque de Ransomware. Neste tipo de ataque, os criminosos criptografam os dados da vítima e exigem o pagamento de um resgate (geralmente em criptomoedas) para fornecer a chave de descriptografia e restaurar o acesso.

3. Descrição do Ataque

O grupo de ransomware REvil (também conhecido como Sodinokibi) explorou uma brecha nos sistemas da Lojas Renner e conseguiu criptografar os servidores do seu data center. A ação foi rápida e impactou significativamente as operações da empresa.

O ataque tirou do ar os sites e aplicativos da Renner, Camicado e Youcom, além de ter paralisado os sistemas internos das lojas físicas. A empresa teve que suspender parte de suas operações enquanto sua equipe de TI trabalhava para restaurar os sistemas a partir de backups. A Renner afirmou publicamente que não negociou nem pagou o resgate exigido pelos criminosos.

4. Vulnerabilidade Explorada

A empresa não divulgou detalhes técnicos específicos sobre a vulnerabilidade explorada. No entanto, ataques de ransomware como o do REvil geralmente se iniciam através de:

- **Phishing:** Envio de e-mails falsos para enganar funcionários e obter credenciais de acesso.

- **Vulnerabilidades em sistemas expostos à internet:** Falhas de segurança não corrigidas (sem patch) em servidores ou serviços como VPN e RDP (Remote Desktop Protocol).
- **Credenciais comprometidas:** Uso de senhas fracas ou vazadas em outros incidentes.

A principal falha, portanto, está mais ligada a **processos de segurança e configurações** do que a um CVE específico publicamente conhecido para este caso.

5. Impactos e Prejuízos

- **Interrupção das Operações:** As vendas online foram completamente paralisadas e as operações das lojas físicas foram severamente afetadas por cerca de 48 horas, resultando em perdas de receita significativas.
- **Danos à Reputação:** Embora a empresa tenha sido elogiada por sua resposta rápida e transparente, o incidente expôs a vulnerabilidade de uma das maiores varejistas do país.
- **Custos de Remediação:** A Renner teve custos elevados para investigar o incidente, fortalecer sua infraestrutura de segurança e recuperar os sistemas afetados. O prejuízo, embora não totalmente revelado, é estimado na casa das **dezenas de milhões de reais** devido à paralisação das vendas e aos custos de recuperação.

6. Tipo de Proteção Aplicável

- **Educação e Conscientização:** Treinamento contínuo para funcionários sobre como identificar e-mails de phishing e outras tentativas de engenharia social.
- **Gerenciamento de Vulnerabilidades (Patch Management):** Manter todos os sistemas e softwares constantemente atualizados para corrigir falhas de segurança conhecidas.
- **Soluções de EDR (Endpoint Detection and Response):** Utilizar ferramentas avançadas que monitoram comportamentos suspeitos nos computadores e servidores para detectar e bloquear a ação de ransomwares antes que a criptografia comece.
- **Backups Imutáveis:** Manter uma política de backups robusta, com cópias isoladas da rede principal (offline ou em nuvem com imutabilidade), garantindo uma recuperação rápida sem a necessidade de pagar o resgate.

Fonte: Site das Lojas Renner sai do ar após ataque hacker

Fonte 2: Site da Renner sai do ar após ataque hacker – entenda o caso | CNN Brasil

Ataque 2: Megavazamento de Dados (Caso Serasa Experian)

1. Data do Ataque

A descoberta e divulgação do vazamento ocorreram em **janeiro de 2021**. A data exata da extração dos dados é incerta, mas acredita-se que tenha ocorrido ao longo de 2020.

2. Tipo de Ataque

Vazamento de Dados em Massa (Data Leak). Este tipo de incidente envolve a exposição, roubo e divulgação não autorizada de informações confidenciais ou pessoalmente identificáveis.

3. Descrição do Ataque

Um enorme banco de dados contendo informações de **223 milhões de brasileiros** (incluindo falecidos) foi colocado à venda em fóruns na dark web. Os dados vazados eram extremamente detalhados, incluindo:

- Dados básicos: Nome completo, CPF, RG, data de nascimento, endereço.
- Dados financeiros: Score de crédito, renda, cheques sem fundo, histórico de compras.
- Outras informações: E-mail, telefone, escolaridade, e até fotos de rosto em alguns casos.

A origem exata do vazamento nunca foi confirmada publicamente, mas a Autoridade Nacional de Proteção de Dados (ANPD) abriu um processo investigativo e apontou a **Serasa Experian** como a provável fonte dos dados, embora a empresa negue. A

suspeita é de que uma base de dados interna tenha sido acessada e copiada indevidamente.

4. Vulnerabilidade Explorada

A investigação aponta para uma possível **falha na segurança de uma API** (Interface de Programação de Aplicações) ou um **acesso indevido a um banco de dados interno**. A vulnerabilidade não foi um CVE, mas sim uma **fragilidade no controle de acesso e na proteção do perímetro de dados** da empresa detentora das informações. Isso permitiu que um volume gigantesco de dados fosse extraído ao longo do tempo sem que os sistemas de segurança detectassem a atividade anômala.

5. Impactos e Prejuízos

- **Exposição da População:** Praticamente toda a população brasileira teve seus dados pessoais expostos, tornando-se alvos fáceis para golpes de phishing, fraudes financeiras, roubo de identidade e extorsão.
- **Crise de Confiança:** O incidente gerou uma enorme crise de confiança em empresas que manipulam grandes volumes de dados pessoais (bureaus de crédito).
- **Consequências Regulatórias:** Este foi um dos maiores casos a serem analisados sob a vigência da Lei Geral de Proteção de Dados (LGPD). A Serasa Experian foi multada pela Senacon (Secretaria Nacional do Consumidor) e enfrenta processos judiciais que podem resultar em multas ainda maiores aplicadas pela ANPD. O prejuízo total é incalculável, mas as multas e indenizações podem chegar a cifras bilionárias.

6. Tipo de Proteção Aplicável

- **Data Loss Prevention (DLP):** Implementar soluções de DLP para monitorar, detectar e bloquear a extração não autorizada de dados sensíveis da rede.
- **Segurança de APIs:** Proteger APIs com autenticação forte, autorização e limites de taxa (rate limiting) para impedir a coleta massiva de dados.
- **Princípio do Acesso Mínimo:** Garantir que apenas sistemas e funcionários autorizados tenham acesso aos dados estritamente necessários para suas funções.
- **Monitoramento e Análise de Comportamento:** Utilizar sistemas que analisam o comportamento de usuários e sistemas (UEBA - User and Entity Behavior Analytics) para identificar atividades suspeitas, como um acesso incomum a um grande volume de registros.

Fonte: MPF requer da Serasa o pagamento de multa superior a R$ 200 milhões por vazamento de dados pessoais — Procuradoria da República em São Paulo

Fonte 2: O mega vazamento de dados do SERASA - Instituto SIGILO