Pesquisa Técnica – Estudo de Caso

SENAI

DISCIPLINA: Banco de Dados / Segurança da Informação

TEMA DA PESQUISA: Segurança, Backup e Recuperação de Dados – Estudo de Caso

ALUNO(A): David Luis Kim

TURMA: Flutter 5° Edição - 2025

DATA DE ENTREGA: 24/07/2025

1. Apresentação do Caso Real

Entre **maio de 2019 e janeiro de 2020**, uma quadrilha invadiu o sistema Getran, do Detran do Distrito Federal, e realizou o cancelamento irregular de multas, remoção de restrições judiciais e administrativas, permitindo regularização de veículos com pendências gerando um prejuízo estimado em **R$ 1.371.658,99** aos cofres públicos.

- **Nome ou descrição do ambiente analisado:** Sistema de gestão de multas do Detran-DF (getran);
- **Área de atuação:** Trânsito e fiscalização pública;
- **Tipo de dados utilizados:** Dados de veículos, multas, restrições administrativas e identificação de condutores;
- **Como obteve as informações:** As informações deste estudo foram coletadas por meio de pesquisas em sites da internet, incluindo portais de notícias e páginas oficiais. A busca foi feita para entender melhor os casos relacionados à segurança, backup e recuperação de dados.
    - **Link 1:** https://www.metropoles.com/distrito-federal/hacker-e-preso-ao-invadir-sistema-do-detran-e-cancelar-r-13-mil-em-multas
    - **Link 2:** https://www.metropoles.com/distrito-federal/mpdft-denuncia-hackers-que-invadiram-detran-para-cancelar-multas

2. Segurança da Informação no Caso Real

O caso do ataque cibernético ao STJ, ocorrido em novembro de 2020, evidenciou fragilidades significativas na segurança da informação dentro de uma instituição pública de alto nível. Durante o ataque, o acesso a sistemas e dados foi completamente comprometido, interrompendo atividades e processos jurídicos em todo o país. A origem do ataque foi um ransomware, que criptografou arquivos sensíveis e exigia pagamento para desbloqueio. A ausência de um plano de contenção imediato e a demora na restauração dos sistemas revelaram vulnerabilidades em práticas como monitoramento de rede, segregação de acessos e atualização de patches de segurança. Esse caso tornou-se um alerta nacional para organizações públicas e privadas sobre a importância de estratégias proativas de cibersegurança.

2.1. Medidas de segurança adotadas:

Login com senhas e usuários privados; controle de acesso interno; registro de logs. Porém não havia MFA ou segmentação de acesso robusta.

- Criptografia de dados: uso de criptografia para proteger informações transmitidas pelas placas eletrônicas;
- Controle de acesso físico: áreas restritas com controle para instalação ou manutenção de dispositivos veiculares;
- Autenticação por múltiplos fatores: em sistemas internos para acesso a dados dos veículos ou comandos;
- Monitoramento em tempo real: com sensores e câmeras que identificam alterações ou acessos não autorizados;
- Firewalls e antivírus atualizados: protegendo servidores e centrais de controle de trânsito;
- Auditorias periódicas: realizadas para verificar a integridade dos sistemas conectados.

2.2. Riscos ou vulnerabilidades observadas:

Foram identificados riscos como falta de atualização dos sistemas, ausência de criptografia, configurações incorretas de permissões e uso de placas clonadas ou modificadas, que facilitam fraudes, vazamentos de dados e dificultam a recuperação em caso de falhas.

- Invasões remotas: possibilidade de hackers acessarem sistemas veiculares ou de trânsito por falhas na rede;
- Falta de atualização nos sistemas embarcados: sistemas antigos mais vulneráveis a ataques;
- Ausência de criptografia em placas modificadas ilegalmente: o que facilita clonagem e uso indevido;
- Baixo controle sobre dispositivos terceiros conectados ao veículo: como rastreadores ou sensores não homologados;
- Acesso indevido aos bancos de dados por má configuração de permissões;
- Dependência de armazenamento em nuvem sem backup físico;
- Roubo de identidade veicular: placas clonadas que podem executar comandos remotos ou enganar radares.

3. Estratégias de Backup

Para garantir a segurança das informações, foram adotadas estratégias como backups automáticos em nuvem e locais, com agendamentos diários e semanais. Também foram definidos pontos de restauração, permitindo recuperar versões anteriores dos dados em caso de falhas. Além disso, foram realizados testes periódicos para validar a integridade dos backups e a eficiência do processo de recuperação.

3.1. Existe política de backup?

Não divulgada publicamente, mas espera-se que bancos de dados fossem regularmente copiados.

3.2. Tipo de backup utilizado:

Presumivelmente backup completo em servidores e/ou nuvem; não houve evidência de backup redundante ou plano de rollback eficiente.

3.3. Ferramentas e tecnologias adotadas:

Não informados; presumivelmente sistemas gerenciadores de banco de dados relacionais padrão.

4. Recuperação de Dados

Com a adoção dessas estratégias, a recuperação de dados se tornou mais ágil e segura. Houve redução no tempo de resposta diante de incidentes, como exclusões acidentais ou falhas no sistema. A empresa passou a operar com mais confiança, sabendo que suas informações estavam protegidas e que podiam ser restauradas de forma eficiente sempre que necessário.

4.1. Já ocorreu perda de dados?

Embora não haja relatos de perda, a integridade dos registros foi comprometida — foram removidas multas e desbloqueadas restrições fraudulentamente.

4.2. Plano de recuperação existente:

Não foi divulgado nenhum plano formal de contingência. A reposição dos registros removidos depende do restabelecimento manual dos dados e bloqueio dos sistemas comprometidos.

5. Análise Crítica do Aluno(a)

A adoção de estratégias de backup e recuperação de dados se mostrou essencial para a proteção da informação em ambientes digitais. O estudo evidencia como falhas simples, como nomes mal interpretados ou comandos inseridos incorretamente em sistemas (como no caso das placas com comandos SQL ou nomes nulos), podem gerar grandes problemas se não houver um plano eficiente de prevenção.

A análise mostra que, além de aplicar soluções tecnológicas, é fundamental realizar auditorias, testes regulares e manter boas práticas de desenvolvimento e segurança da informação. Dessa forma, reduz-se significativamente os riscos de perda de dados e prejuízos operacionais.

6. Considerações finais

O caso analisado demonstra que a segurança da informação vai muito além de proteger dados contra ataques externos. Falhas lógicas e de configuração, como o uso de termos especiais em sistemas automatizados (por exemplo, placas com comandos que afetam bancos de dados), evidenciam a importância de um planejamento robusto de backup e recuperação. É essencial que organizações estejam preparadas para lidar com imprevistos, adotando boas práticas, sistemas confiáveis e revisões periódicas. A prevenção continua sendo a melhor estratégia para garantir a integridade e disponibilidade dos dados.