SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE IV – SEGURANÇA DOS DADOS

PUC Minas
Virtual

4.2 – TRATAMENTO DE DADOS SENSÍVEIS NAS ORGANIZAÇÕES

PUC Minas
Virtual

4.2.3 – MASCARAMENTO DE DADOS

OS AMBIENTES

- Quando falamos de segregação dos ambientes, fato muito importante é o tratamento dos dados presentes.
- Aquela estória de cópia dos dados de produção para o ambiente de desenvolvimento/homologação e testes em tempos de LGPD não é recomendada.

FONTE: BERGAMI,2014.

MASCARAMENTO DE DADOS

- O **mascaramento ou camuflagem de dados**, visa proteger **informações sensíveis (LGPD)** de um banco de dados, como número de cartão de crédito ou documentos, substituindo o valor por outro realista, porém fictício.
- Os ambientes não produtivos representam a maior exposição ao risco de um empresa, sendo que podem haver inúmeras cópias para fins não produtivos.
- Sabemos que para testar adequadamente, é essencial ter dados realistas, mas todos sabem que dados reais podem aumentar muito os riscos de segurança.

MASCARAMENTO DE DADOS

- O mascaramento de dados também elimina o risco de exposição de dados pessoais, o que garante **adequação** com as leis de proteção de dados.
- Não existe uma forma única de mascaramento de dados, porém para ocorrer é importante:
    a) Classificar os dados entre sensíveis e não sensíveis;
    b) Criar regras de autenticação
    c) Criar mecanismos de proteção.

MASCARAMENTO DE DADOS

- A criptografia é uma forma muito comum de mascaramento de dados. Acontece pelo embaralhamento dos dados, de forma que apenas quem possui uma chave de acesso possa descriptografá-los.

- **Vamos falar sobre métodos e técnicas de mascaramento!**

METODOS DE MASCARAMENTO DE DADOS

Mascaramento interno: leitura de um **destino** e, em seguida, atualização do destino com dados mascarados, sobrescrevendo quaisquer informações sigilosas.

Mascaramento externo: leitura de uma fonte (ex.: ambiente produtivo) e gravação dos dados mascarados em um destino (geralmente ambiente não produtivo).

Mascaramento de dados estático: o mascaramento de dados no armazenamento elimina quaisquer rastros, como registros ou alterações em capturas de dados.

Mascaramento de dados dinâmico: essa técnica temporariamente oculta ou substitui dados sensíveis em trânsito, deixando os dados originais em repouso intactos e inalterados.

METODOS DE MASCARAMENTO DE DADOS

- **Geração de dados sintéticos:** essa técnica gera novos dados no lugar de dados existentes, mantendo a estrutura dos dados intacta e é uma técnica muito utilizada é usada em situações como desenvolvimento inicial de aplicações.

- Estes métodos podem ser implementados através de scripts puros, que podem ser desenvolvidos pelos responsáveis pelos testes ou pelos analistas de requisito pois precisam ter os dados válidos para o sistema.

- Mas há possibilidade de utilização de ferramentas no mercado, na modalidade *open source* ou pagas.

TÉCNICAS DE MASCARAMENTO DE DADOS

Criptografia: esse método codifica os dados oferecendo proteção somente enquanto as respectivas chaves de criptografia estão seguras. Neste caso, não existe uma chave-mestra, então não é possível retornar os dados codificados aos valores originais.

Tokenização: é uma variação da criptografia, que gera tokens com estado e sem estado que podem ser identificados.

Codificação: essa técnica envolve a codificação de caracteres ou números, o que não protege adequadamente dados sensíveis.

Anulação ou exclusão: altera as características dos dados e remove qualquer utilidade dos dados.

Embaralhamento: migração de dados ao longo de linhas da mesma coluna.

REQUISITOS DAS FERRAMENTAS

- **Integridade referencial** para que as cópias sejam válidas para testes.
- **Realista** o mascaramento de dados deve permitir que você gere dados realistas porém fictícios, específicos para os negócios.
- **Irreversibilidade:** a solução deve ofertar recursos que após os dados terem sido mascarados, não seja possível obter os valores originais nem fazer engenharia reversa nos dados.
- **Extensibilidade e flexibilidade:** deve tratar diversas fontes de dados simultaneamente.

VANTAGENS DE APLICAÇÃO

- Maximiza o aproveitamento dos dados de diversos ambientes de forma totalmente segura;
- Mitiga os riscos de vazamento de informações sensíveis;
- Atende aos mecanismos de regulamentação e às leis de proteção de privacidade.
- As estratégias de ***Test Data Management*** **(TDM)** reduzem falhas e se integram com o novo mundo **DEVOPS!**

REFERENCIAS BIBLIOGRÁFICAS

LEBLANC Jonathan. MESSERSCHMIDT, Tim. Identity and Data Security for Web Development. O'Reilly, 2016.

HIT,2022. Mascaramento de dados: o que é e como funciona? Disponível em: <https://www.hti.com.br/blog-mobile/556-mascaramento-de-dados-o-que-e-e-como-funciona>. Acesso em:14 Nov. 2022.

KALTI ,2017. Mascaramento de dados: o que é e qual a sua importância? Disponível em: <http://kalti.com.br/mascaramento-de-dados-o-que-e-e-qual-sua-importancia-2/>. Acesso em: 02 Nov. 2022.

DRS9, 2020. Afinal, o que é mascaramento de dados? Disponível em: <https://www.dsr9.com/afinal-o-que-e-mascaramento-de-dados/>. Acesso em: 12 Nov. 2022.


PUC Minas
Virtual