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

4.2.1 – SEGURANÇA DE DADOS

MECANISMOS DE GARANTIA DOS DADOS

- Independente da tecnologia e da organização existente dos dados de um determinado negócio, o valor que as informações apresentam para os negócios e como percebe-se o risco de falhas em quaisquer sistemas, nos remete à manutenção do **backup.**

- Portanto, manter **backups** atualizados de **bancos de dados** e outras informações importantes é **fundamental** para a **resiliência** no caso de um **ataque de segurança**, **falha de equipamento ou erro humano.**

MECANISMOS DE GARANTIA DOS DADOS

- **Backup:** é uma cópia das informações de seus sistemas para outro dispositivo para recuperação ou arquivamento.
- **Em caso de falha o processo de restauração pode ser acionado.**
- **IMPORTANTE: Implemente um sistema de verificação periódica para garantir que os backups estejam ocorrendo corretamente e que sejam recuperáveis!**
- Mantenha os backups em armazenamento externo **longe dos sistemas originais**, para que não estejam sujeitos aos mesmos danos de falhas ou ataques.

MECANISMOS DE GARANTIA DOS DADOS

- Questão importante é fazer com que os procedimentos de recuperação sejam e resposta a algum evento incapacitante seja definido e conhecido por todos da empresa.
- Os **Planos de Continuidade de Negócios (PCN)**, são o centro da preservação da **resiliência** organizacional durante crises extremas.
- Do outro lado temos o **Plano de Recuperação de Desastres (DR),** e este sim, define questões como: a forma de comunicação dos funcionários, para onde os funcionários irão, manutenção das funções **principais operacionais** no caso de um ataque grave.

MECANISMOS PROTETIVOS

- De acordo com o **NIST** *Framework:*
  - "As soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência de sistemas e ativos, consistentes com as políticas, procedimentos e acordos relacionados" (LeBlanc, Messerschmidt, 2016) .
- A mídia removível é frequentemente usada para injetar malware de forma consciente ou inocente em praticamente todos os tipos de sistema.
- Mantenha o princípio da menor funcionalidade: **1 dispositivo para 1 processo!**

IDENTIDADES

- Ao usar a **Internet**, um indivíduo estabelece uma identidade online que representa determinados elementos ou características dessa pessoa.
- Há uma classificação dos tipo de identidade que segundo em um compilado de autores são: **identidade social**, i**dentidade concreta** e **identidade magra.**
- São consideradas identidades federadas e são aplicados por meio de tecnologias como **SAML**, **OpenID**, **OAuth** e **tokenização** que são frequentemente aplicados por meio de logon único, conhecido como **SSO (Single Sign-on)**, o Gerenciamento de Identidade Federado.

IDENTIDADES

- **Identidade Social:** surgiu com o surgimento das redes sociais e pode ser vista como uma forma muito moderada de identidade que as pessoas tendem a compartilhar de forma bastante casual.
- Serviços como **Facebook** ou **Google** permitem que os usuários acessem rapidamente outros serviços usando seus perfis já preenchidos e se tornou uma forma preferida de autenticação, especialmente em telefones celulares, porque fornece um grande aumento na conveniência e ajuda a evitar os problemas de utilização de dispositivos.

IDENTIDADES

- **Identidade Concreta:** exigem um perfil mais concreto que forneça informações úteis, por exemplo, e-mail, endereço, número de telefone, idiomas falados ou documentos do usuário.
- Banco on-line ou comércio eletrônico são ótimos exemplos e serviços como o PayPal, Amazon Payments ou Google Wallet permitem que os usuários insiram informações valiosas em um só lugar e as reutilizem em vários sites.
- Ao *tokenizar* credenciais, como detalhes de pagamento, o checkout é acelerado.

IDENTIDADES

- **Identidade Magra:** significa simplesmente autenticação de usuário sem obter acesso às informações do perfil é um conceito antigo que está ganhando popularidade novamente.
- Na prática eles utilizam seu número de telefone como meio de fazer login onde o bit de identificação é o número de telefone da pessoa.
- Assim substitui-se as senhas simples outros serviços semelhantes visam por outro fator que é universalmente utilizado desta forma possibilitando a implantação do MFA (Múltiplo Fator de Autenticação) enviando um SMS para o celular por exemplo.

REFERENCIAS BIBLIOGRÁFICAS

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

E-TRUST,2022. O que é SSO ou Single Sign-On?. Disponível em: https://www.e-trust.com.br/o-que-e-sso-ou-single-sign-on/>. Acesso em: 02 Nov. 2022.

FILIPE, Jefereson,2019. DMZ o que é e para que serve. Disponível em: <https://falati.com.br/dmz-o-que-e-e-para-que-serve/>. Acesso em: 02 Nov. 2022.


PUC Minas
Virtual