SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE IV – SEGURANÇA DOS DADOS

PUC Minas
Virtual

4.1 – GERENCIAMENTO DE INFAESTRUTURA E REDES DE USUÁRIOS

PUC Minas
Virtual

4.1.1 – CONTROLE DE ACESSO

SEGURANÇA NA PRÁTICA - INFRAESTRUTURA

- Criar proteção e controles de segurança nas redes e ativos da empresa é o objetivo e uma boa prática que pode ser seguida é a proposta do NIST como dissemos anteriormente.
- Quando se fala em infraestrutura o *Framework for Improving Critical Infrastructure Cybersecurity*, apresenta uma proposta adaptável e qualquer tipo de negócio e, mais que isto, oferecem uma norteadora para proteção do ambiente.

SEGURANÇA NA PRÁTICA - INFRAESTRUTURA

- De acordo com as melhores práticas do NIST Framework, para que possamos proteger a organização devemos seguir **seis** etapas:

1. Controle de acesso
2. Conscientização e Treinamento
3. Segurança de dados
4. Processos e Procedimentos de Proteção da Informação
5. Manutenção
6. Tecnologia de Proteção

CONTROLE DE ACESSO

- O primeiro e mais importante passo para proteger as redes e os ativos da sua organização.
- É o processo onde a organização garante que um usuário **autenticado** tenha acesso apenas ao que está **autorizado** a acessar e nada mais.
- Lembrando que **autenticação** é o ato ou processo de determinar que um usuário **é quem ele diz ser** e coletar informações sobre **como ele está acessando seus sistemas** exemplo: Acesso da rede corporativa ou através da Internet.

CONTROLE DE ACESSO

- E **autorização** é o ato de determinar o nível de acesso que um usuário autorizado tem a sistemas e dados.
- Desta forma, deve-se definir quais os sistemas é necessário controlar o acesso e de acordo com a estratégia e quais os níveis de acesso devem ser considerados e, para tal precisamos considerar alguns fatores como:
    - Tipo de conexão, Aplicação de CRUD, horário de acesso, Autorizações em cascata, Permissões globais além da combinação dos privilégios.

CONTROLE DE ACESSO

- Recomenda-se utilizar como objetivo da autorização o emprego do princípio do **menor privilégio** que nada mais é do que liberar apenas as permissões (privilégios) necessários para concluir as operações definidas em sua organização.
- É muito importante destacar que identidades e credenciais são **emitidas**, **gerenciadas**, **verificadas**, **revogadas** e **auditadas** para **dispositivos**, **usuários** e **processos** autorizados.

CONTROLE DE ACESSO

- Existem controles mais sofisticados além do fornecimento puro de senha que são:
  - ✓ restrição por **tempo** (temporário),
  - ✓ restrição por **geografia** (acesso externo),
  - ✓ restrição por **fonte** (listas de controle de acesso) e
  - ✓ restrição por **certificado** (pareamento de chave pública/privada para que apenas mensagens criptografadas específicas possam ser acessadas)

CONTROLE DE ACESSO

- A força deste processo está no gerenciamento do ciclo de vida das contas do **sistema** e do **aplicativo**, incluindo sua criação, uso, **inatividade** e **exclusão**, o que deve minimizar as oportunidades para os invasores.
- O rastreamento dos acessos e a integração com os processos corporativos é fundamental para que a gestão do ciclo de vida funcione corretamente.
- **Atenção para a gestão das contas temporárias!**

CONTROLE DE ACESSO

- A ideia de se utilizar o princípio da menor autoridade juntamente com a separação de funções corporativas é uma bora dica para a empresa esteja protegida contra golpes.
- Um golpe que acontece bastante se chama *spear phishing* onde acontece o comprometimento de e-mail comercial.
- O invasor se passa pelo Presidente da empresa ou pelo Diretor financeiro solicitando transferências em para determinadas contas. Se optarmos por um solicita e o outro aprova seria necessário 2 pessoas serem vítima do golpe para que ele desse certo.

SERVIÇO PARA VERIFICAÇÃO DE CONTAS

- https://haveibeenpwned.com/
- Este serviço pode ajuda-lo a identificar problemas com sua conta de email pessoal ou corporativa.

REFERENCIAS BIBLIOGRÁFICAS

DEFENDER, 2021. Tipos de Pentest. Disponível em: <https://www.sitedefender.com.br/tipos-de-pentest/?gclid=EAIaIQobChMIg_G11KeQ-wIVyBOtBh217wWnEAAYASAAEgIg0fD_BwE>. Acesso em: 02 Nov. 2022.

MICROSERVICE,2022. O que é análise de vulnerabilidade e qual sua importância?. Disponível em: <https://www.microserviceit.com.br/analise-vulnerabilidade/>. Acesso em: 02 Nov. 2022.

SESTREM, Thatiana**.** Matriz de risco: o que é e como implementar na sua empresa. Disponível em: <https://qualyteam.com/pb/blog/matriz-de-risco/>. Acesso em: 25 Out. 2022.


PUC Minas
Virtual