**MECANISMOS DE SEGURANÇA**

**Controles Físicos:**

São barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. Mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas, etc.

**Controles Lógicos:**

São barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal-intencionado.

**Honeypot**

É uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor.

**AMEAÇAS À SEGURANÇA:**

* Perda de confidencialidade.
* Perda de integridade.
* Perda de disponibilidade.

**TIPOS DE ATAQUES A APLICAÇÕES WEB**

Devido a algumas tecnologias adotadas em algumas páginas web, diversas vulnerabilidades podem ser exploradas, e os problemas causados são diversos:

**SQL Injection**

É uma técnica onde, através da entrada de dados de uma página web, usuários maliciosos podem injetar comandos SQL no banco de dados de uma aplicação.

**CSRF**

Cross- site request forgery, ou simplesmente falsificação de solicitações entre sites, é um tipo de ataque no qual comandos não autorizados são transmitidos a partir de um usuário que possui acesso a aplicação. Neste ataque, uma aplicação envia solicitações para um site se passando por um usuário logado esperando que a aplicação execute sua requisição.

**XSS**

Cross - site scripting, é um tipo de ataque de injeção de código malicioso em aplicações web. Este tipo de ataque geralmente acontece em função da falha na validação nos dados de entrada de um usuário, permitindo que um script malicioso seja executado no navegador do cliente.

**CAMADAS E MECANISMOS DE SEGURANÇA**

A grosso modo, a segurança em camadas consiste na disposição de várias etapas de proteção à operacionalidade de uma empresa, de modo a blindar seus arquivos e dados mais sensíveis contra-ataques cibernéticos.

**AS PRINCIPAIS CAMADAS QUE COMPÕEM ESSE TIPO DE ESTRATÉGIA**

## Firewall

O objetivo desse tipo de proteção é digitalizar o tráfego de rede e filtrar dados e acessos. Dessa forma, sempre que há uma interação externa, o sistema tende a bloqueá-la se for suspeita.

**Dados**

O bloqueio de dados é muito importante nessa estratégia de segurança, pois prioriza a proteção das informações corporativas. Nesse aspecto, uma perda de equipamento, seja por defeito ou ataque cibernético, se restringiria a um prejuízo físico e toda documentação seria recuperada.

**Rede**

A camada de rede protege o sistema de uma eventual falha de defesa na firewall.

Dessa forma, a ameaça pode ser neutralizada ainda que ultrapasse o estágio anterior. integridade do acesso às informações será sempre preservada se

**DNS**

(Domain Name Service) é um serviço de nomes de domínio fornecido pelo ISP (Internet Service Provider). Esse tipo de camada funciona como uma agenda que protege as informações na busca por sites.

**Backup**

mais que uma camada, essa medida deve ser rotina de qualquer organização que se preze.

**QUAIS AS MELHORES PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO?**

* Prevenção e antecipação de falhas;
* Atualização contínua de sistemas de proteção;
* Identificação de vulnerabilidades;
* Implementação de consultoria especializada.