

RESUMO DE PROVA CAPITULO 1

SEGURANÇA CIBERNÉTICA: A segurança cibernética é o esforço contínuo para proteger esses sistemas em rede e todos os dados de usos não autorizados ou prejudiciais.

O ESPAÇO CIBERNÉTICO: Tornou-se outra dimensão importante da guerra, onde nações podem ter conflitos sem confrontos com tropas tradicionais e máquinas.

DADOS: Qualquer informação sobre você pode ser considerada, Essa informação pessoal pode identificá-lo unicamente como um indivíduo.

DADOS CORPORATIVOS: incluem informações de funcionários, propriedades intelectuais e informações financeiras.

CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE (CIA)

CONFIDENCIALIDADE: A confidencialidade garante a privacidade dos dados, restringindo o acesso através de autenticação por criptografia, com a confidencialidade as políticas da empresa devem restringir o acesso às informações ao pessoal autorizado e verificar se apenas os indivíduos autorizados visualizam esses dados. Os dados podem ser divididos de acordo com a segurança ou o nível de confidencialidade da informação.

METODO DA CONFIDENCIALIDADE

- Os métodos para garantir a confidencialidade incluem criptografia de dados.
- ID de usuário e senha.
- Autenticação de dois factores
- Diminuição da exposição de informações confidenciais.

INTEGRIDADE: A integridade garante que as informações sejam precisas e confiáveis, Os dados devem permanecer inalterados durante o trânsito e não modificados por entidades não autorizadas. As permissões e controle de acesso de usuário podem impedir o acesso não autorizado a arquivos.

DISPONIBILIDADE: A disponibilidade garante que as informações possam ser acessadas por pessoas autorizadas, para se utilizar Manutenção de equipamentos, reparos de hardware, actualização de software e sistemas operacionais e criação de backups, deve ter uma disponibilidade da rede e dos dados para usuários autorizados.

AS CONSEQUÊNCIAS DE UMA VIOLAÇÃO DE SEGURANÇA

Se os invasores hackearem uma empresa haverá consequência porque as informações das empresas virá a publico e manchará a reputação dela, perderá as receitas (dinheiro) remover o site da empresa, e a empresa ficar inactiva poderão perder a credibilidade, segredos corporativos podem vazar,

TIPOS DE INVASORES

Os invasores são indivíduos ou grupos que tentam explorar vulnerabilidades para ganho pessoal ou financeiro. Os invasores estão interessados em tudo, de cartões de crédito a projectos de produtos e qualquer coisa com valor.

- **AMADORES** – São normalmente invasores com pouca ou nenhuma qualificação profissional, muitas vezes usando ferramentas atuais ou instruções encontradas na Internet para lançar ataques. Eles podem estar usando ferramentas básicas, mas os resultados ainda podem ser devastadores.

HACKERS

HACKER: este grupo de invasores entra em computadores ou redes para obter acesso.

Dependendo da intenção da invasão, esses invasores são classificados:

- **WHITE HAT:** Os invasores **White Hat** entram em redes ou sistemas de computador para descobrir fraquezas, com o objectivo de melhorar a segurança. Essas invasões são feitas com prévia autorização e todos os resultados são relatados ao proprietário.
- **BLACK HAT:** aproveitam qualquer vulnerabilidade para ganho pessoal, financeiro ou ganho político.
- **GRAY HAT:** Os invasores **GREY HAT** podem encontrar uma vulnerabilidade em um sistema. Os hackers **GREY HAT** poderão relatar a vulnerabilidade aos proprietários do sistema se essa acção coincidir com sua agenda. Alguns hackers **GRAY HAT** publicam os fatos sobre a vulnerabilidade na Internet para que outros invasores possam explorá-la.

HACKERS ORGANIZADOS: Esses hackers incluem empresas de criminosos virtuais, hacktivistas, terroristas e hackers patrocinados pelo Estado.

- **OS CRIMINOSOS VIRTUAIS:** Geralmente são grupos de criminosos profissionais, focados em controle, poder e riqueza.
- **OS HACKTIVISTAS:** Fazem declarações políticas para sensibilizar para questões que são importantes para eles.
- **OS INVASORES PATROCINADOS:** Pelo estado reúnem informações ou cometem sabotagem em nome de seu governo.

AMEAÇAS À SEGURANÇA INTERNA

Ameaças internas também têm o potencial de causar maior dano que as ameaças externas, pois os usuários internos têm acesso directo ao edifício e a seus dispositivos de infra-estrutura. Os funcionários também têm conhecimento sobre a rede corporativa, seus recursos e seus dados confidenciais, além de diferentes níveis de usuário ou privilégios administrativos.

AMEAÇAS À SEGURANÇA EXTERNA

Ameaças externas de amadores ou invasores habilidosos podem explorar vulnerabilidades na rede ou em dispositivos de computação ou usar a engenharia social para obter acesso.