53GUR4NC4 D4 INFORM4C40

INFORM4C40

J1y4n y4R1

1NFORM4C40

"As portas dos fundos são tão boas quanto às portas da frente."

0000 0100

1NFORM4C40

"Um sistema é tão seguro quanto o seu elo mais fraco."

0000 0100

1NFORM4C40

"Um atacante não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando sempre o ponto mais vulnerável."

Steve Bellovin (1992)

1NFORM4C40

"Threat", em inglês, é utilizado para definir ameaça. Segundo Shirey (2000) tem-se vários tipos de threat (ameaças):

- ameaça inteligente;
- ameaça;
- ameaça de análise;
- consequências de uma ameaça

1 NFORM4C40

Ameaça inteligente

Circunstância onde um adversário tem a potencialidade técnica e operacional para detectar e explorar uma vulnerabilidade de um sistema.

Exemplo: Uso de exploit por um atacante.

1NFORM4C40

Ameaça

Potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano.

Exemplo: Tentativa de login não autorizado no sistema

1 NFORM4C40

Ameaça de análise

Uma análise da probabilidade das ocorrências e das consequências de ações prejudiciais a um sistema.

Exemplo: Realização da análise de risco em uma empresa.

1 NFORM4C40

Consequências de uma ameaça

Uma violação de segurança resultado da ação de uma ameaça. Inclui:

- divulgação;
- usurpação;
- decepção;
- e rompimento.

1 NFORM4C40

Ameaças Involuntárias

Ameaças inconscientes, quase sempre causadas pelo desconhecimento.

Podem ser causados por:

- acidentes;
- erros;
- falta de energia;
- e etc.

0000 0100

1NFORM4C40

Ameaças Voluntárias

Ameaças propositais causadas por agentes humanos como:

- hackers;
- invasores;
- espiões;
- ladrões;
- criadores e disseminadores de vírus de computador;
- incendiários e etc.

1NFORM4C40

Ataque

Ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente, e pode ser ativo, passivo ou destrutivo.

1NFORM4C40

Ataque

Pode ser classificado em:

- ativo;
- passivo;
- ou destrutivo.

1NFORM4C40

Ataque

Pode ser classificado em:

- ativo;
- passivo;
- ou destrutivo.

1 NFORM4C40

Ataque ativo

Tipo de ataque que tem como finalidade e consequência, ou resultado, especificamente a alteração dos dados.

Exemplo:

Defacement – desfiguração de sites.

1NFORM4C40

Ataque passivo

Tem por finalidade e consequência, ou resultado, a liberação dos dados.

Exemplo:

roubo de dados pessoais ou dados de cartão de crédito de uma site de comércio eletrônico.

1NFORM4C40

Ataque destrutivo

Tem como finalidade e consequência, ou resultado, a negação do acesso aos dados ou serviços.

Exemplo:

Ataque de DDoS;

Alteração da senha de administrador/root.

1NFORM4C40

FORMAS DE ATAQUES

- INTERCEPTAÇÃO;
- INTERRUPÇÃO;
- MODIFICAÇÃO;
- E PERSONIFICAÇÃO.

1 NFORM4C40

Interceptação

Considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).

Exemplo:

Sniffing.

1NFORM4C40

Interrupção

Pode ser definida como a interrupção do fluxo normal das mensagens ao destino.

Exemplo:

DDoS

1NFORM4C40

Modificação

Consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.

Exemplo:

Alteração de dados ordem de pagamento

1 NFORM4C40

Personificação

Considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.

Exemplo:

Ataque Man-in-the-midlle

1NFORM4C40

Mecanismos para Controles de Segurança

Os mecanismos para controle de segurança da informação passam por dois conceitos específicos, que são:

- autenticação;
- autorização.

1NFORM4C40

Autorização

Processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acessos (Acess Control List - ACL), definindo quais atividades poderão ser realizadas, desta forma gerando os chamados perfis de acesso.

Exemplo:

Perfis de usuários

1NFORM4C40

Autenticação

Meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser. Serviço essencial de segurança, pois uma autenticação confiável assegura o controle de acesso, determina que está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

Exemplo:

Login de acesso a um sistema

1NFORM4C40

Tipos de autenticação

Os processos de autenticação estão baseados em três métodos distintos:

- identificação positiva;
- identificação proprietária;
- identificação biométrica.

1NFORM4C40

Identificação positiva

O que se sabe: o usuário possui o conhecimento de alguma informação utilizada no processo de autenticação.

Exemplo:

Senha de login no sistema.

1 NFORM4C40

Identificação proprietária

O que se tem: o usuário possui algo a ser utilizado no processo de autenticação.

Exemplo:

- cartão magnético;

- token;

- chip e etc.

1 NFORM4C40

Identificação biométrica

O que se é: o usuário possui alguma característica própria, pessoal e única.

Exemplo:

- biometria como:

- impressão digital;

- íris;

- passada e etc.