SEGURANÇA da INFORMAÇÃO

TIPOS DE CONTROLE

- Físico → portas, trancas, alarmes, crachás...
- Lógico → senhas, firewall, criptografia, biometria...

TERMINOLOGIAS

- Risco → probabilidade de concretização de um evento danoso (= Dano real)
- Ameaça → um dano em potencial
- Ataque → exploração de uma vulnerabilidade (fragilidade) por uma ameaça

PROCEDIMENTO DE BACKUP

CAI MUITO!

TIPO DE BACKUP	DADOS COPIADOS	VELOCIDADE DA CÓPIA	VELOCIDADE DA RESTAURAÇÃO	ESPAÇO DE ARMAZENAMENTO
COMPLETO	todos	lento	rápido	grande
INCREMENTAL	Apenas novos ou modificados	rápido	médio	pequeno
DIFERENCIAL	Tudo desde o último backup completo	médio	rápido	médio

PRINCÍPIOS/PROPRIEDADES

DECORE!

- Confidencialidade → a informação não será revelada a um indivíduo não autorizado
- Integridade → a informação estará exata e completa
- Disponibilidade → a informação estará acessível quando demandada
- Autenticidade → usuário é quem diz ser
- Irretratabilidade → o emissor de uma mensagem não pode negar posteriormente sua autoria
  (= não repúdio)

SEGURANÇA DA INFORMAÇÃO
segurança da informação
= CRIPTOGRAFIA =

CRIPTOGRAFA ASSIMÉTRICA
DECORE!

- Uso de 2 chaves
  - Pública: qualquer um pode ter
  - Privada: personalíssima
  - ↳ para leitura é necessária a chave do mesmo par
- Garante
  - Confidencialidade e
  - Autenticidade

CRIPTOGRAFIA SIMÉTRICA
Uso de uma mesma chave simétrica para codificar e decodificar a mensagem

↓

Há risco no envio da chave (Ambas as partes devem ter a mesma)

↳ Garante só a confidencialidade (Integridade e autenticidade, não!) PEGADINHA!

AUTENTICAÇÃO
- Métodos:
  - É (ex.: Biometria)
  - Sabe (ex.: Senha)
  - Tem (ex.: Crachá)

↳ uso de >1 (=) autenticação forte

Assinatura Digital (+) Hash

Garantem:
- Integridade
- Autenticidade
- Irretratabilidade

- Certificado tal:
  - (A) Certificado de assinatura digital
  - (S) Certificado de sigilo

↳ Por uma autoridade de certificadora
- terceira parte confiável que atesta a autoria da assinatura
- Publica a lista de certificados revogados

↳ ICP-BRASIL: Autoridade certificadora (+) Autoridade de registro

ALGORITMO DE HASH:

Dada uma **entrada de tamanho qualquer**, a transforma em uma saída de tamanho **fixo**

↳ Usar tamanho maior para evitar colisões

CRIPTOGRAFIA HÍBRIDA
(=) Usa criptografia assimétrica para a troca das chaves e a simétrica para informações

MALWARES

malwares

CAI MUITO!

WORM

- É ≠ dos vírus → ele não infecta outros arquivos, ele mesmo é o arquivo.
  - Replica-se automaticamente e envia cópias de si mesmo
- Consome muitos recursos com suas cópias
  - Diminue o desempenho das redes e pode lotar o disco rígido
  - (Independe de qualquer atuação do usuário)

VÍRUS

= Programa malicioso que se propaga

- infectando
- copiando-se
- anexando-se
- hospedando-se

→ em arquivos ou programas

depende da execução destes para se ativar

BOMBAS LÓGICAS

= Instaladas para causar danos ao hospedeiro quando de um determinado evento (data, ação...)

RETROVÍRUS

= Ataca o antivírus, excluindo a lista de assinaturas do vírus e deixando o PC vulnerável.

HIJACKER

= Software malicioso que assume o controle do navegador de internet da máquina atacada e modifica a apresentação do conteúdo

BOT E BOTNET

= Um programa que possibilita ao invasor controlar remotamente a máquina invadida (Zumbi)

- infecção e propagação similares às do worms

MALWARES

malwares

CAI MUITO!

TROJAN HORSE

= É um programa malicioso disfarçado como um aplicativo útil

↳ depende da execução do usuário!

SPYWARE

= Software espião que viola a privacidade do usuário

- envia dados da máquina a terceiros
- monitora as atividades de um sistema

- Dependem da execução do usuário!

↳ Tipos mais comuns

1. Keyloggers → capturam as teclas digitadas
2. Screenloggers → capturam a posição do cursor e a imagem da tela
3. Sniffers → monitoram o tráfego na rede (Capturam pacote de dados)
4. Addwares → exibem propagandas indesejadas

RANSON WARE

= Código malicioso que torna inacessíveis os dados de um equipamento, exigindo um resgate (ransom) normalmente em moedas digitais

ROOTKIT

= Programas e técnicas para manter o acesso indesejado a um PC, conforme necessidades de seu criador.

1. Remove evidências
2. Esconde atividades
3. Captura informações
4. Mapeia vulnerabilidade

BACKDOOR

= Permite o retorno de um invasor a um computador previamente comprometido.

(Abre as portas TCP)

ANTIMALWARE

antimalware

= FERRAMENTAS =

ANTIVÍRUS

- Remove vírus existentes e combate novas infecções
  - Gerações:
    1. Detecção baseada em assinatura
    2. Detecção baseada em heurística
    3. Interceptação de atividade
    4. Proteção completa

QUARENTENA

Arquivos identificados como possíveis vírus ficam em observação até sua identificação

(Podem ser recuperados!)

ANTISPAM

- Separa e-mails desejados dos indesejados
- Já vem integrado na maioria dos webmails e leitores de e-mails.

FIREWALL PESSOAL

- Protege o PC de acessos indesejados via internet
  - Analisa o conteúdo das conexões continuamente

  \+

  Filtra códigos maliciosos e impede comunicação dos já instalados com o invasor

ANTISPYWARE

- Detectam e removem *spywares*
- Há um nativo do Windows (= *Windows Defender*)

ataques e golpes

ENGENHARIA SOCIAL

- Uma pessoa tenta persuadir outra a executar determinadas ações por má-fé
  - Através de ingenuidade ou confiança das pessoas

FORÇA BRUTA

- Tentar adivinhar, por tentativa e erro nomes de usuário, senhas...
  - Uso de ferramentas automatizadas
- Pode resultar em negação de serviço devido à sobrecarga do sistema

IP SPOOFING

- O atacante clona o IP de um usuário legítimo para ganhar um acesso não autorizado
  - Ele manipula o campo de endereço de origem do pacote IP

DENIAL OF SERVICE (DoS)

- Objetivo é tirar de operação um → serviço / computador / rede
  - faz isso exaurindo os recursos e causando indisponibilidade

PING OF DEATH

- Envio de uma pacote pins > 65.536 bytes para outro dispositivo em outra rede que pode levar ao travamento da máquina
  - Excede o tamanho máximo do pacote ICMP

PHISHING SCAM

- O golpista tenta enganar um usuário para a obtenção de dados pessoais e financeiros
  - Ex.: envio de um e-mail que induza o usuário a clicar em um link malicioso

ATAQUES E GOLPES

ataques e golpes

PHARMING

- É um tipo específico de *phishing* que envolve o redirecionamento da navegação do usuário para sites falsos via alteração no servidor DNS.

MAN IN THE MIDDLE

- Os dados trocados são interceptados por um terceiro
  - Também podem ser registrados e até alterados pelo atacante
- As vítimas não percebem as alterações e tomam os dados como válidos

HOAX (BOATOS)

- Mensagem com conteúdo falso ou alarmante e, geralmente, aponta como autor uma empresa, órgão ou instituição importante (FAKE NEWS!)
  - Normalmente têm alguma finalidade difamatória ou de manipulação
- Se aproveitam da boa vontade e confiança de quem recebe e repassa.

DEFACEMENT

- Altera a apresentação de uma página na web
  - Geralmente a página principal, mas pode ser feito nas internas também
- Técnicas:
  1. Explorar as vulnerabilidades da linguagem e de pacotes de desenvolvimento web
  2. Invadir o servidor hospedeiro
  3. Explorar erros da aplicação web.