CONCEITOS GERAIS SOBRE SEGURANÇA NA TECNOLOGIA DA INFORMAÇÃO

Prof. Me. Hélio Esperidião

CONCEITOS GERAIS SOBRE SEGURANÇA NA TECNOLOGIA DA INFORMAÇÃO

- O conceito de segurança envolve formas de proteção e garantias de que uma dada informação será preservada e utilizada apenas pelas pessoas de direito.

- Como garantir a integridade física de dados?

- Como garantir que os dados sejam acessados apenas por pessoas de direito?

Por que se preocupar com a segurança?

- Senhas, números de cartões de crédito
- Conta de acesso à internet
- Dados pessoais e comerciais
- Danificação do sistema
- Disponibilidade do sistema
- Disponibilidade da informação.

CONCEITOS GERAIS SOBRE SEGURANÇA NA TECNOLOGIA DA INFORMAÇÃO

- Vírus:
  - É um programa malicioso que, tal como um vírus biológico, infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores.

- BACKDOOR
  - Permite que hackers controlem o micro infectado pela "porta de trás". O vírus, que abre um caminho da máquina para que o autor do programa passe a controlar a máquina de modo completo ou restrito.

CONCEITOS GERAIS SOBRE SEGURANÇA NA TECNOLOGIA DA INFORMAÇÃO

- Vírus de BOOT
  - Infecta na área de inicialização de discos rígidos. Essa área é onde se encontram arquivos essenciais ao sistema Operacional.
- CAVALO DE TRÓIA (TROJAN)
  - São programas aparentemente inofensivos que trazem embutidos um outro programa (o vírus) maligno.
- ENCRIPTADOS
  - Tipo recente que, por estarem codificados, dificultam a ação dos antivírus.

CONCEITOS GERAIS SOBRE SEGURANÇA NA TECNOLOGIA DA INFORMAÇÃO

- Vírus de MACRO
  - Infecta as macros (códigos executáveis utilizados em processadores de texto e planilhas de cálculo para automatizar tarefas) de documentos, desabilitando funções como Salvar, Fechar e Sair.
- MULTIPARTITE
  - Vírus que infecta registro mestre de inicialização, trilhas de boot e arquivos.
- MUTANTE
  - Vírus programado para dificultar a detecção por antivírus. Ele se altera a cada execução do arquivo contaminado.

ANTI-VÍRUS

- Panda
- AVG
- AVAST
- Microsoft Security Essentials
- Avira
- Kaspersky
- Bit Defender
- Symantec Norton
- Zone Alarm

INTEGRIDADE DE DADOS

- Como é possível garantir que um dado não seja perdido?
  - Criar cópias dos dados em diversas mídias diferentes.
- Quais as mídias e formas de armazenamento disponíveis?
  - Pen drives, Cds, DVDs.
- Armazenar na internet é uma boa solução?
- Antivírus pode ajudar a garantir a integridade dos dados?

SERVIÇOS ESPELHO OU REPLICADOS

- Em serviços de auto desempenho é como o uso de serviços espelho.
- Os serviços em espelho são caracterizados por possuírem réplicas da informação em equipamentos diferentes.
- Em alguns casos dependendo do valor da informação os dados são armazenados em dispositivos com localização geográfica diferente.

Disponibilidade em sistemas replicados.

- Os sistemas replicados também são utilizados para garantir disponibilidade da informação como por exemplo em sistemas de banco de dados de grande web sites onde a informação é armazenada em diversos servidores espalhados pelo mundo, caso um dos servidores falhe o outro assume o comando.

- A troca por um servidor que está em funcionamento perfeito geralmente é transparente ao usuário.

Acesso a dados

- Como garantir o acesso de direito?
  - Senhas
  - Criptografias
- Escolha de sistemas operacionais seguros?
  - Linux
  - Unix
  - Solares

Principais disponíveis no mercado

- Panda
- AVG
- AVAST
- Microsoft Security Essentials
- Avira
- Kaspersky
- Bit Defender
- Symantec Norton
- Zone Alarm

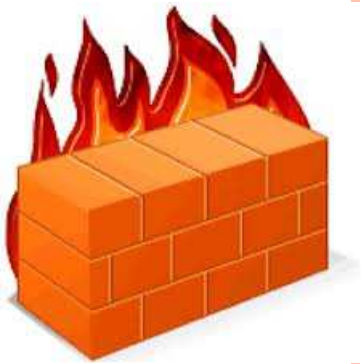
Anti-Spyware

- Permite controlar alterações no registro do SO.
- Evita a instalação de Spywares.
- Alguns antivírus possuem Anti-Spyware

Filtro Anti-Spam

- Separa as mensagens conforme regras pré-definidas.
- Serve para separar os email válidos dos Spams
- Não são eficientes 100%
  - Algumas vezes identificam mensagens verdadeiras como spam e vice versa.
- Diversas técnicas são utilizadas inclusive existem alguns estudos sobre IA (Inteligência artificial)

FIREWALL



- Dispositivo para controlar o acesso entre computadores e redes de computadores
- São aplicativos ou equipamentos que ficam entre um link de comunicação e a rede, checando e filtrando todo o fluxo de dados.
- Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede mas também a confidencialidade deles

FIREWALL

- Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados.

- Permitem o bloqueio de portas que não são utilizadas
  - Portas e aplicações:

21 – FTP
23 – Telnet
25 – SMTP
80 – HTTP
443 - HTTPS

110 - POP3
143 – IMAP
3306 - mysql

Firewall

- Não há razão para deixar porta abertas que não estejam sendo utilizadas.

- Portas abertas são uma janela para aplicativos de má intenção.

TIPOS DE FIREWALL

- Firewall em forma de software utilizam recursos do computador, memória, processador etc

- Firewalls em forma de hardware são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais

SOFTWARE X HARDWARE

- Hardware: A vantagem de usar equipamentos desse é dada no fato do hardware ser dedicado e não compartilha recursos com outros aplicativos e o sistema operacional .

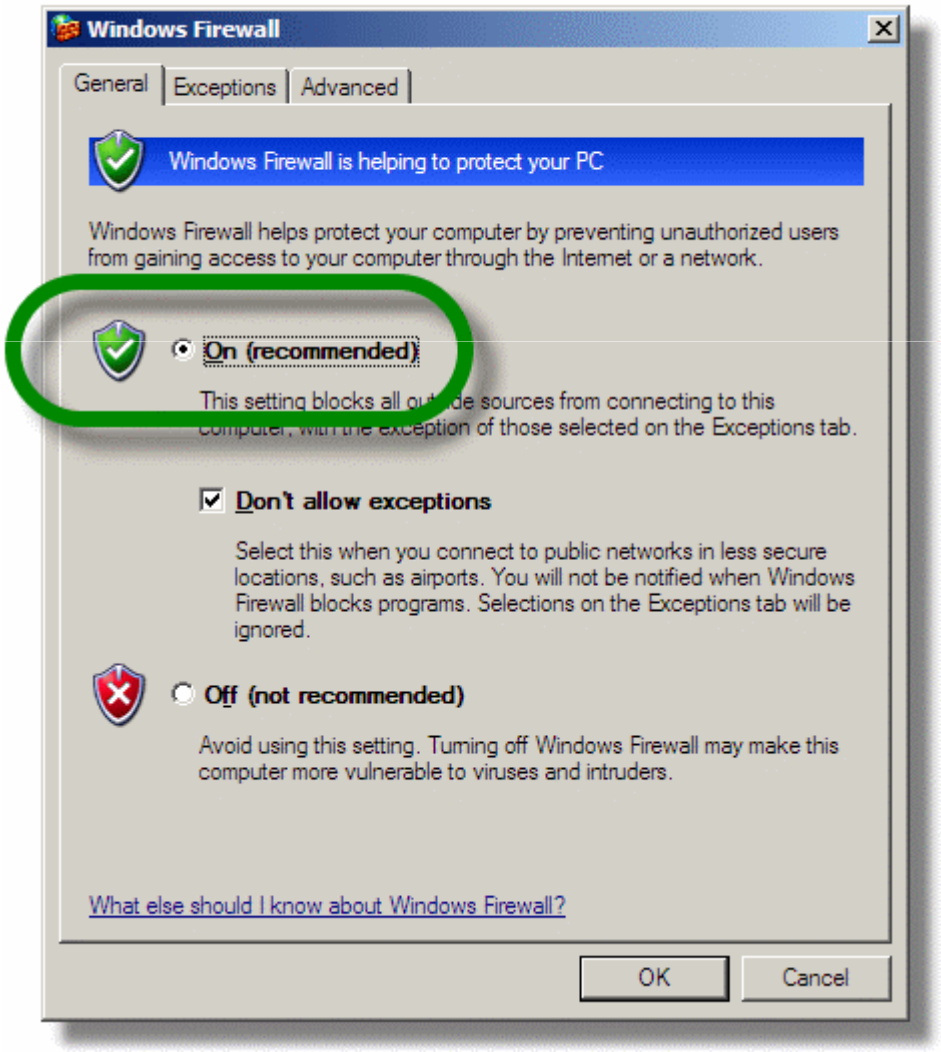
- Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

Cisco ASA5505 Adaptive Security ASA5505-SEC-BUN-K9

- **830,00 €**

Windows Firewall

- Acompanha o Windows



ZONE ALARM

- Gratuito