

INTRODUÇÃO A SEGURANÇA EM REDES

Prof. Msc. Hélio Esperidião

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.



PRINCIPAIS TIPOS DE ATAQUE A SISTEMAS DE REDE

- DOS
- Spam.
- Phishing Scam.
- DNS Poisoning.
- Ataques Força Bruta.
- Falhas em Aplicações e SOs.
- Botnets.
- Packet Sniffing.
- Varreduras.



DENIAL OF SERVICE (DOS)

- Consistem em tentativas de fazer com que servidores tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas.
- Neste tipo de ataque não há invasão do servidor ou infecção com malwares.
- O autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de não conseguir responder.
- O computador fica tão sobre carregado que nega serviço. (Denial of Service).



DENIAL OF SERVICE (DOS)

- Imagine um elevador moderno que é capaz de transportar até 12 pessoas ou 1200 kg.
- Este elevador possui a capacidade de identificar o peso.
- Caso o peso ultrapasse seu limite o elevador se nega a fazer o serviço.



DDOS (DISTRIBUTED DENIAL OF SERVICE)

- É um tipo de ataque DoS.
- Possui grandes dimensões
 - utiliza muitos computadores para atacar uma determinada máquina.
 - A ação é distribuída entre varias máquinas.
 - É um dos tipos de ataque mais comum na internet.
- Historicamente, servidores da CNN, Amazon, Yahoo, Microsoft e eBay já foram vítimas.



DDoS

- Em dezembro de 2010 os sites da Visa, Mastercard e Paypal sofreram ataques DDoS de um grupo defendendo a liberdade na internet
- Em fevereiro de 2012, ataques foram executados contra sites de bancos brasileiros por motivos semelhantes.



DDOS

- Para que ataques do tipo DDoS sejam bem sucedidos, é necessário um exercito de maquinas para participar da ação.
- Uma das melhores formas de adquirir este exercito é inserir programas de ataque DDoS em vírus ou em softwares maliciosos que se espalham pela rede.
- O usuário de uma maquina recrutada dificilmente fica sabendo que sua máquina está sendo utilizada para tais fins.



COMBATENDO ATAQUES DOS OU DDoS

- Não há fórmula mágica que funcione em todas as implementações.
- É difícil identificar o problema.
- Pode-se utilizar filtros que identificam e bloqueiam pacotes com endereços IP falsos.
- Outra idéia consiste em utilizar ferramentas que identificam padrões que caracterizam um ataque.



DoS

- Outra forma é tentar identificar padrões humanos e padrões de acesso que podem ser de robôs.
- Cada caso deve ser analisado separadamente e muitos fatores são levados em consideração.
 - Sistema operacional
 - Tipo de serviço oferecido
 - Valor da informação
 - Etc.



CONCLUINDO - DDOS

- Ataques DDoS apenas "derrubam" servidores.
- Capturar dados ou descaracterizar sites ou servidores é muito mais difícil.





SPAM

- Spam é o termo que referir-se a e-mails não solicitados
- Geralmente são enviados para um grande número de pessoas.
- Possui conteúdo exclusivamente comercial.



SPAM ZOMBIES

- Computadores de usuários comuns que foram comprometidos por códigos maliciosos.
- Uma vez instalados os códigos maliciosos, permitem a utilização da máquina para o envio de spam, sem o conhecimento do usuário.
- Maquinas zombies dificultam a identificação da origem do spam e dos autores também.



COMO IDENTIFICAR?

- Cabeçalhos suspeitos podem aparecer
 - Incompleto, sem o remetente ou o destinatário.
 - Aparecer como apelidos ou nomes genéricos.
 - amigo@
 - suporte@
- Campo Assunto (Subject) suspeito
 - A maioria dos filtros anti-spam está preparada para barrar assuntos considerados suspeitos.
 - spammers adaptam-se e tentam enganar os filtros colocando no campo assunto conteúdos enganosos.



COMO IDENTIFICAR?

- Campo Assunto (Subject) suspeito
 - Costumam colocar textos atraentes e/ou vagos demais, confundindo os filtros e os usuários.
- Opções para sair da lista de divulgação
 - É um dos artifícios usados pelos spammers para validar a existência dos endereços de e-mail.
 - “Caso não tenha se cadastrado, não clique para sair”.
 - Também é importante jamais clicar em um link enviado por e-mail. Sempre digite a URL no navegador.



COMO IDENTIFICAR ?

○ Golpes e fraudes

- Muitas vezes e-mails de spam não tem característica comercial mas, são portadores de fraudes e golpes.
- São simulados e-mails de entidades financeiras ou governamentais pedindo seus dados pessoais ou bancários para atualização.



SPAN

- Leis e regulamentações

- Não existem leis brasileiras referentes à prática de spam.



PHISHING.

- O termo “Phishing” é relativamente novo, e sua criação data de meados de 1996, por
- hackers que praticavam roubo de contas da **America Online (AOL)**, fraudando senhas de usuários.
- Este termo origina-se da palavra *fishing* – pescar e *password* (senha) fazendo alusão à pescaria de senhas.
- É Caracterizado pelo envio de mensagens falsas(Spans) que simulam instituições reais de modo a convencer o alvo a disponibilizar informações sensíveis.



PHISHING.

- É um ataque bastante flexível, podendo empregar e-mails, sites ou mensagens de voz fraudulentas para tentar induzir o usuário a divulgar ao atacante informações.
- De acordo com o Anti-Phishing Working Group
 - os ataques têm nível alto de sucesso, ultrapassando os 5%.



PHISHING

- Utilizam um conjunto de práticas na tentativa de *persuadir* indivíduos a realizar ações que favoreçam o atacante.
- Por se tratar de um ataque que é conduzido a nível psicológico, não há aplicativos que possam impedi-lo.



COMO IMPEDIR?

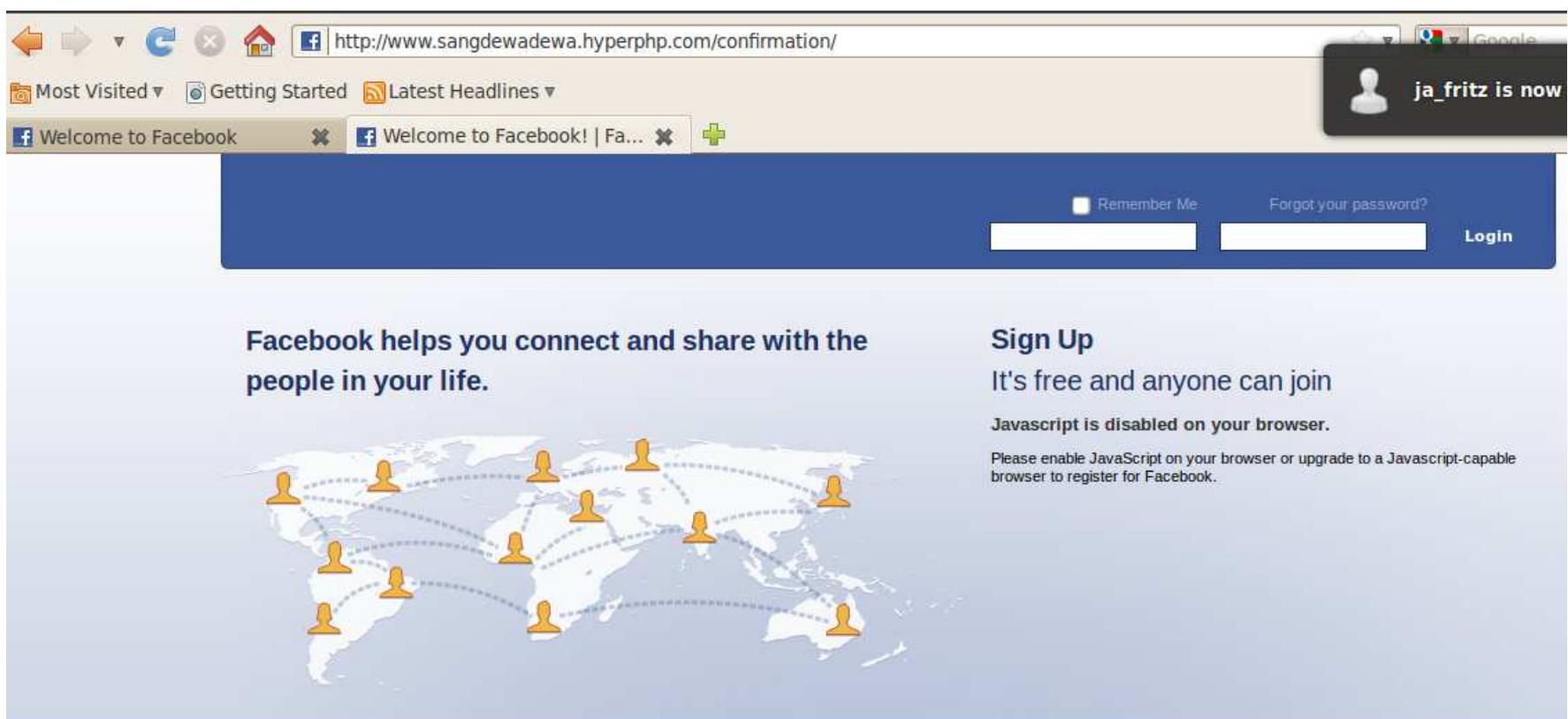
- Verifique com a instituição real a autenticidade da mensagem.
- Verifique se o remetente e o site é realmente da instituição.
- Verifique se a pagina possui HyperText Transfer Protocol Secure(HTTPs).
 - Permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais.



EXEMPLOS DE PHISHING



EXEMPLOS DE PHISHING



EXEMPLOS

Mensagem

Recadastramento Banco real - Mensagem (HTML)

Responder Responder Encaminhar a Todos
Responder

Excluir Mover para Pasta
Criar Regra Outras Ações

Bloquear Remetente Listas de Confiança

Lixo Eletrônico Não é Lixo Eletrônico

Categorizar Acompanhamento Marcar como Não Lida

Opções Localizar Relacionadas

Selecionar Localizar Enviar para o OneNote OneNote

De: infoemail@santander.com.br
Para:
Cc:
Assunto: Recadastramento Banco real
Enviada em: qui 10/02/2011 12:23

BANCO REAL

Atenção: Prezado Cliente, após a unificação com Banco Santander. Verificamos que seu dispositivo de segurança encontra-se desativado em nossos sistemas.

Este recurso só é ativado em seu computador se você aceitar a autenticação a partir de servidores certificados.
<http://www.menusbarcelona.com/platos/456/dolar.php?App=98,4355,3321,111,0,0>
Clique para seguir o link

CONFIRMAR

Supporte Técnico 0800 728 0200

Nenhum vírus encontrado nessa mensagem.
Verificado por AVG - www.avgbrasil.com.br
Versão: 10.0.1204 / Banco de dados de vírus: 1435/3434 - Data de Lançamento: 02/10/11

DNS POISONING.

○ DNS Cache?

- Os endereços ips vinculados a nomes não são muito voláteis, ou seja, não mudam a cada instante, portanto é interessante como forma de economia de recurso armazenar tabelas DNS.



DNS POISONING.

- Poisoning significa envenenamento, ou seja, envenenamento do DNS.
- Está técnica atua diretamente no cache DNS.
- Visa trocar de forma maliciosa os destinos.
 - Desta forma se o ip 190.98.170.44 faz referencia ao nome www.google.com.br. O endereço de ip é trocado, levando os usuários para outro local diferente do pretendido.



ATAQUES FORÇA BRUTA.

- Estes ataques são fundamentados na tentativa de quebrar as senhas dos usuários para obterem acesso ao sistema.
- O termo força bruta vem da idéia de tentar descobrir a senha do usuário por meio de bancos de dados de senhas mais comuns ou tentativa e erro.



ATAQUES FORÇA BRUTA.

- Faça um programa que tente descobrir uma senha de 4 dígitos, não leve em consideração caracteres especiais nas senhas, só números e caracteres comuns. Verifique quanto tempo vai demorar para 5, 6, 7 e 8 dígitos.
- Muito comum atualmente o ataque força bruta contra servidores SSH.



COMO EVITAR ATAQUES DE FORÇA BRUTA

- A maioria dos sistemas deixa que seus usuários erreem apenas um numero limitado de vezes suas senhas.
- Caso um usuário erre mais uma determinada quantidade de vezes o sistema bloqueia novas tentativas ou bloqueia a conta.



FALHAS EM APLICAÇÕES E SOS.

- Os sistemas operacionais modernos são softwares extremamente grandes.
- Garantir que não haja nenhuma falha é impossível.
- Todo sistema computacional possui falhas



FALHAS EM APLICAÇÕES E SOS.

- Os invasores criam “exploits” para explorar essas falhas
- Exploit:
 - Programa malicioso projetado para explorar uma vulnerabilidade existente em um software de computador.
- Com o tempo é comum que os sistemas operacionais de uma mesma versão se tornem mais estáveis.
 - Isso ocorre por meio de atualizações.
 - As atualizações visam corrigir problemas encontrados



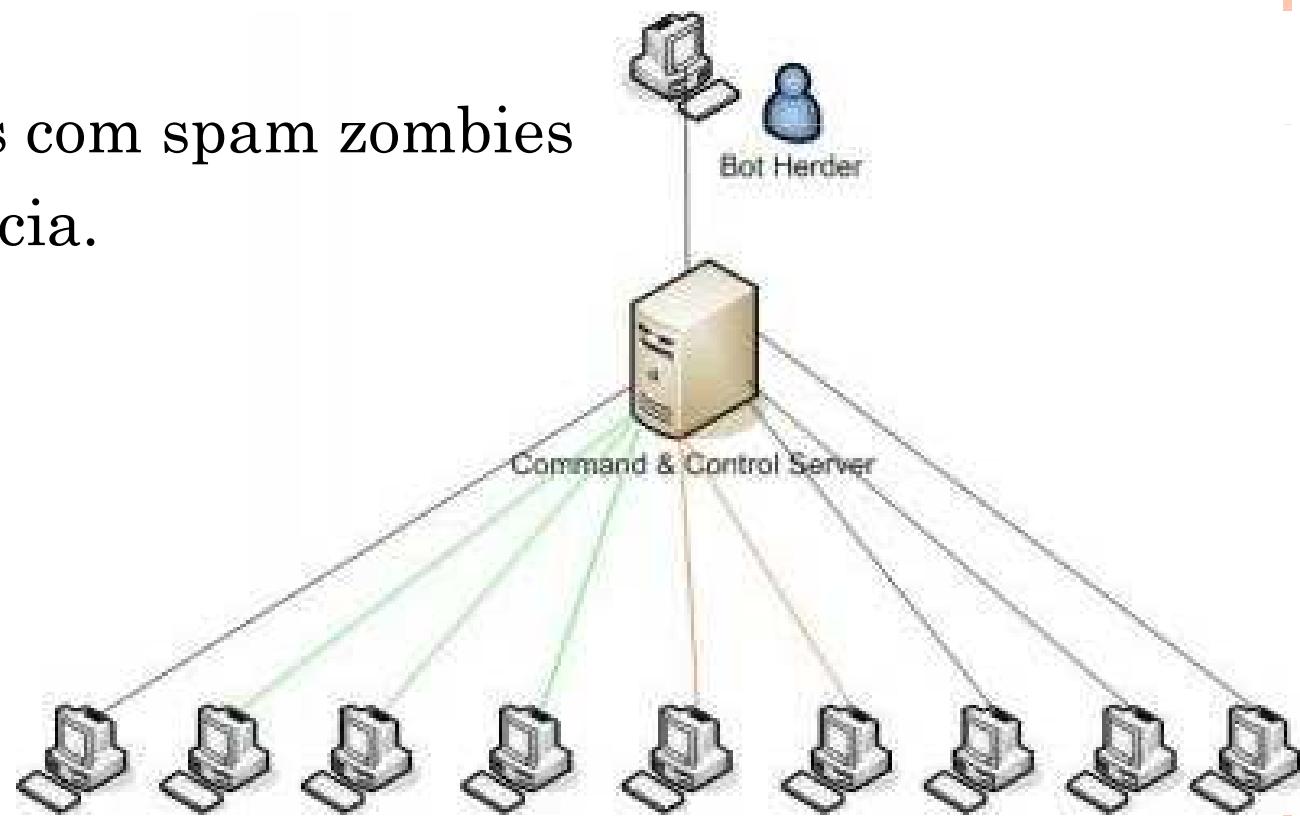
BOTNETS.

- Um aplicativo capaz de se comunicar com os invasores que o colocaram em sua máquina.
- Da mesma forma que acontece com muitos tipos de vírus, o bot pode ser um programa independente, agindo e se propagando através do seu computador.



BOTNETS

- Geralmente o atacante se esconde atrás de um computador de controle, que também é controlado por um bot.
- Semelhanças com spam zombies
Não é consciência.



COMO EVITAR BOTNETS?

- Podem ser usadas em ataques DOS, envio de SPAM, fraudes e etc.
- Este tipo de robô é detectado por antivírus, anti-spywares etc.
- Mantenha seus sistemas antivírus atualizados.



PACKET SNIFFING (FAREJAMENTO DE PACOTES).

- Almeja coletar informações não criptografadas transmitidas pela rede. (nome de usuários, senhas e etc).
- Em redes que utilizam hubs os pacotes são transmitidos a todos os micros da rede.
- Em teoria, somente a placa de rede destinatária leria o pacote, as demais os ignorariam.



PACKET SNIFFING

- Como todos os outros micros recebem os pacotes, não é tão difícil assim burlar este frágil sistema, passando a ter acesso a todos os dados transmitidos através da rede.



PACKET SNIFFING

- Como poderia ser evitado?



VARREDURAS.

- Detectam a estrutura da rede:
 - quais aplicações estão acessíveis
 - informações como versão do sistema operacional
 - versão das aplicações que estão rodando



E AGORA, COMO EVITAR TUDO ISSO?

- Atualize seus sistemas!!!!
- Tenha uma boa política de uso
- Procure observar se o sistema esta mais lento do que o normal.
- Analise os logs do sistema.
 - Log?
- Jamais utilize a conta de administrador/root sem necessidade.
- Para transações importantes utilize ferramentas de criptografia.



DIMINUINDO MAIS OS RISCOS

- Antivírus.
- Anti-spyware.
- Filtro Anti-Spam.
- Firewall.
- Criptografia.
- Backup dos Dados



EDUCAÇÃO DO USUÁRIO FINAL

- Grande parte dos ataques se baseiam em aproveitar da “inocência” do usuário final.
- Adote uma Política de Uso e Segurança.



O ANTIVÍRUS

- Somente útil quando ele está atualizado.
 - Centenas de vírus são criados todos os dias, inclusive por estudantes.
- Serve para detectar e eliminar vírus e outros tipos de malwares.
- Mantenha a ética profissional, não utilize seu conhecimento técnico para criar e vírus.



PRINCIPAIS DISPONÍVEIS NO MERCADO

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



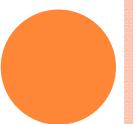
ANTI-SPYWARE

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



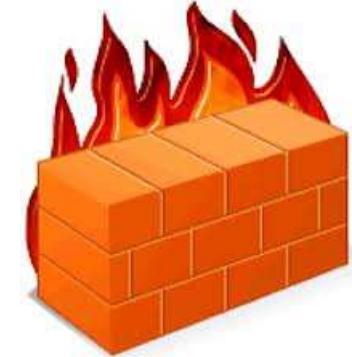
FILTRO ANTI-SPAM

- 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 | 110 - POP3 |
| 23 – Telnet | 143 – IMAP |
| 25 – SMTP | 3306 - mysql |
| 80 – HTTP | |
| 443 - HTTPS | |

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.



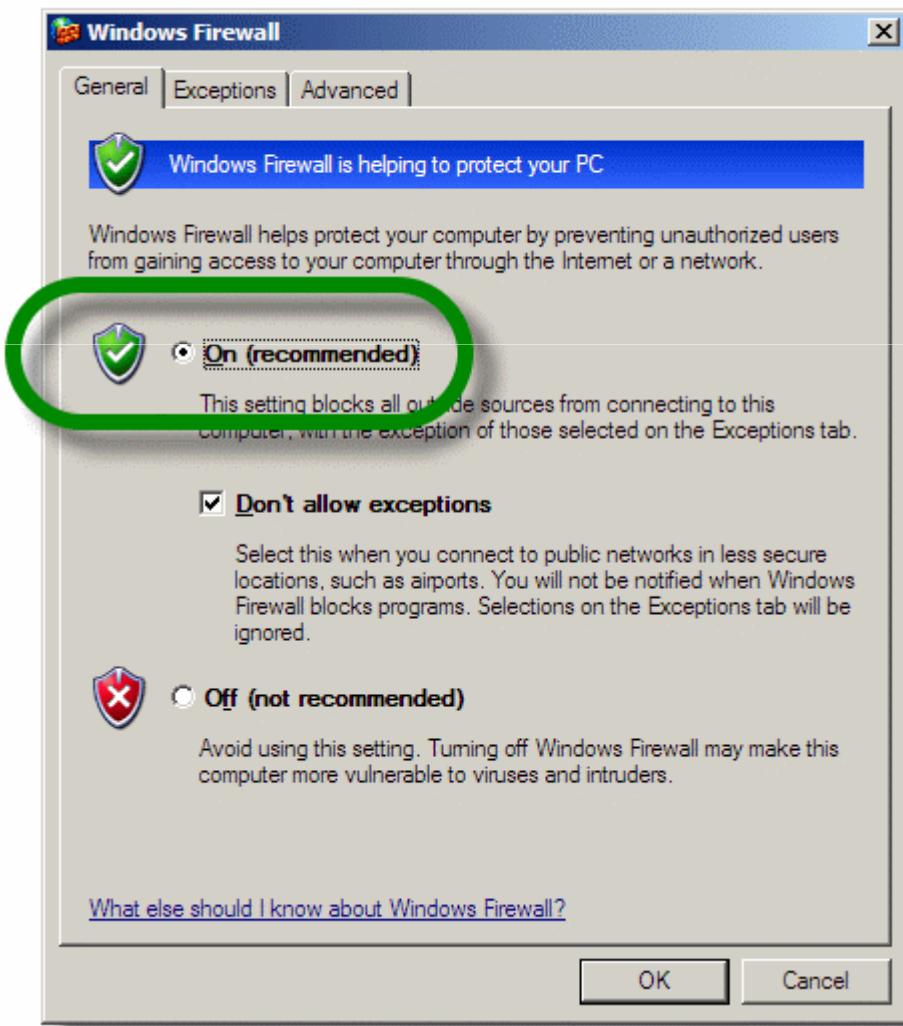
CISCO ASA5505 ADAPTIVE SECURITY ASA5505-SEC-BUN-K9

○ 830,00 €



WINDOWS FIREWALL

- Acompanha o Windows



ZONE ALARM

- Gratuito

