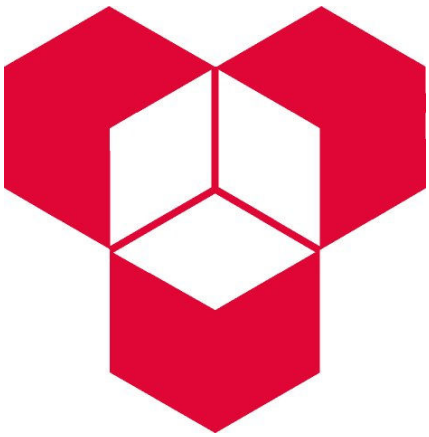
Introdução à Informática



Segurança dos computadores

Escola Superior de Tecnologia e Gestão

Instituto Politécnico de Bragança

Janeiro de 2007

Segurança - necessidade

- Cada vez mais, a economia mundial depende da informática e das comunicações
- Imagine-se como seria hoje o funcionamento dos bancos e das bolsas de valores, por exemplo, sem o recurso a essas tecnologias
- Estas tecnologias, talvez pelo facto de serem relativamente recentes, são bastante vulneráveis a questões de segurança
- A segurança dos computadores e das respectivas redes é, por isso, um tema cada vez mais actual e importante

Porquê preocupar-me?

- Os computadores domésticos são utilizados para realizar inúmeras tarefas:
  - transacções financeiras (bancárias, compra de produtos e serviços, …)
  - comunicação, por exemplo, através do envio de *e-mails*
  - armazenamento de dados (pessoais ou comerciais)
  - …
- É importante que um utilizador se preocupe com a segurança do seu computador, pois, provavelmente, não gostaria que:
  - Senhas e números de cartões de crédito lhe fossem furtados
  - A conta de acesso à Internet fosse utilizada por alguém não autorizado
  - Os dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por estranhos
  - O seu computador fosse utilizado nalguma actividade ilícita, para esconder a real identidade e localização de quem o "invade"
  - O seu computador fosse utilizado para lançar ataques contra outros computadores
  - Um vírus de computador lhe fosse propagado

Segurança dos computadores

- De uma forma simplista, diz-se que um computador é seguro se garante três requisitos básicos:
  - Disponibilidade
    - Os serviços/recursos do sistema estão disponíveis sempre que forem necessários
    - Exemplo de violação: O fornecedor de Internet sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo o utilizador fica impossibilitado de enviar a sua Declaração de IRS à DGCI
  - Confidencialidade
    - A informação só está disponível para aqueles devidamente autorizados
    - Exemplo de violação: Alguém obtém acesso não autorizado ao computador de outro utilizador e lê todas as informações contidas na sua Declaração de IRS
  - Integridade
    - A informação não é destruída ou corrompida e o sistema tem um desempenho correcto
    - Exemplo de violação: Alguém obtém acesso não autorizado ao computador de outro utilizador altera informações da Declaração de IRS deste, momentos antes de enviá-la à DGCI
- A garantia destes três factores pode ser posta em causa por deficiências dos sistemas, por utilização indevida ou por utilização malévola

Utilização malévola

- *Malware* - Todo o tipo de programa cuja finalidade é executar alguma actividade maliciosa ou não solicitada pelo utilizador
  - *Vírus*
  - *Worm*
  - *Spyware*
  - *Hijackers*
  - *Trojans Horses* (Cavalos de Tróia)
- *Hackers*
- *Crackers*
- *Phishing Scam*
- *Denial of Service Attack* – Negação de Serviço

Vírus

- Um vírus é um pedaço de software que é misturado no código de um programa executável
  - Os vírus ocultam-se em ficheiros executáveis, ou seja, em programas com as extensões *.EXE* ou *.COM*, ou de bibliotecas partilhadas, de extensão *.DLL*
- Para o vírus estar activo, não lhe basta estar no computador, mas sim executar o programa que o contém
- Quando o utilizador executa o programa (por desconhecimento do que ele traz de mau), o vírus é activado e copia-se a si próprio para outros ficheiros ou programas executáveis existentes no computador
- Se um destes ficheiros infectados for transferido para outro computador, este também vai passar a ter um vírus alojado, esperando o momento para infectá-lo, ou seja, quando for também executado – capacidade de auto-replicação parecida a um ser vivo
- Os vírus propagam-se de computador para computador através dos ficheiros: por disquete, por *download*, por e-mail, etc.

Tipos de vírus

- Vírus de disco
  - afectam o *BOOT-SECTOR* - parte do disco responsável pela manutenção dos ficheiros
- Retrovírus
  - atacam o programa que permite detectar vírus
- Vírus polimórficos
  - alteram a sua forma para não serem reconhecidos
- Vírus de e-mail
  - programas executáveis anexos a mensagens de correio electrónico
- Vírus de macro
  - Feito na linguagem das macros, para funcionar dentro do programa ao qual está ligado. Ao abrir um documento de Word infectado com um vírus de macro, o vírus é activado, criando macros que substituem boa parte dos comandos normais do Word:
    - aparecem palavras sem serem digitadas e imediatamente desaparecem, o computador fica a "trabalhar" (ampulheta) sem ninguém lhe ter pedido para fazer nada, …
- Todos os vírus infectam apenas programas executáveis e nunca ficheiros de dados
  - O ficheiro tem de ser executado para que o vírus seja activado
- Cerca de 95% dos vírus são benignos, isto é, não passam de brincadeiras irritantes sem grandes consequências

Worm

- É um programa malévolo que se replica a ele próprio pelo disco e pela memória de um computador
- Um *Worm* difere de um vírus precisamente por ser um programa e não apenas um pedaço de *software* dissimulado num programa
- Tipo de *malware* que usa a rede para se espalhar
- Muito famosos por causarem um grande número de computadores infectados em pouco tempo, usando anexos de e-mail e forjando e-mails aparentemente legítimos
- Outros *worms* usam a rede local para serem instalados em diferentes computadores
- Exemplos: MyDoom, Blaster, ILoveYou

Spyware

- Programas espião instalados no computador sem o consentimento do utilizador que, em vez de serem úteis, tentam rastrear alguma informação pessoal do computador para fazer propaganda ou mesmo oferecer serviços
  - Tipos de sites em que o utilizador navega
  - Músicas que escuta
  - Programas que possui e outras informações do computador
- *Spywares* podem vir acompanhados de *hijackers*
  - O browser do computador fica com a página inicial alterada ou janelas de pop-up aparecem num site que, normalmente, estaria limpo

Cavalos de Tróia

- Um *Trojan Horse* é um programa que faz algum tipo de actividade maléfica porém não se espalha automaticamente
- Geralmente, *trojans* são *malware* simples de se remover comparado aos *worms* e vírus
- A maioria dos *trojans* incluem o *backdoor*
  - permite que o computador infectado seja controlado totalmente ou parcialmente através de um canal de IRC ou via conexão com uma porta

Hackers

- Inicialmente qualquer pessoa que fosse "barra" em qualquer assunto poderia ser considerado um *Hacker*
- O termo hacker de computador apareceu com a ajuda do cinema americano:
  - No filme *War Games*, onde um miúdo, brincando com o seu *modem*, acede (por "acidente") ao NORAD e tenta descobrir a *password* do suposto "jogo"
- Uma pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes com um computador. Ele sabe perfeitamente (como todos nós sabemos) que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando as técnicas mais variadas
- A grande maioria dos *hackers* são jovens (têm mais tempo para estudar e aprender) e acabam por trabalhar na área da segurança de computadores ou… serem presos
- Quase todos os *Hackers* depois da fase da adolescência possuem habilitações literárias universitárias. O *Hacker* que aprendeu sozinho é sempre considerado (pelo menos para os outros *Hackers*) como mais motivado, e pode ser mais respeitado que o seu equivalente com o canudo

Crackers

- Possui tanto conhecimento quanto os *Hackers*, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar códigos, e descobrir falhas
- Consegue um acesso não autorizado a um computador, podendo comprometer a disponibilidade do sistema ou a integridade ou a confidencialidade dos dados
  - Eles precisam deixar um aviso de que estiveram lá, geralmente com recados malcriados, algumas vezes destruindo partes do sistema, e até destruindo o que encontram. Também são atribuídos aos *Crackers* actos muitas vezes relacionadas com a pirataria
  - Descoberta de *passwords* na rede ou por tentativas, exploração de defeitos (*bugs*) do software, *trapdoors* (entradas secretas destinadas a funções particulares), *trojan horses* (um vírus que não se replica mas abre portas ao *Cracker*), etc.
- Algumas pessoas definem a diferença entre *hacker* e *cracker* dizendo que *hacker* invade apenas para "olhar", enquanto o *cracker* invade para destruir não havendo grande fundamento nessa definição (que, aparentemente, visa ilibar *hackers*)

Phishing

- Mensagens fraudulentas que tentam passar por avisos reais de grandes empresas, como bancos, antivírus e cartões de crédito
- Mensagens desse tipo possuem um *link*
- Caso se clique no *link*, este *link* pode tentar roubar alguma informação do utilizador (se preencher um formulário) ou conter um *trojan* que irá capturar tudo que é feito no computador para roubar contas de banco e outros dados
- As mensagens podem ser enviadas por exemplo via e-mail

DoS - Denial of Service Attack

- Um *Denial of Service Attack* é um ataque que consiste em inundar uma rede ou um servidor com tantos pedidos de serviços que o tráfego normal é atrasado ou mesmo temporariamente interrompido
- Um *Distributed Denial of Service Attack* (DDOS) utiliza múltiplos computadores previamente infectados para atacar, aumentando assim a quantidade de tráfego malévolo
- Ao contrário dos vírus e dos *Crackers*, os *denial of service attack* não comprometem a integridade nem a confidencialidade dos dados mas apenas a disponibilidade dos sistemas

Armas de prevenção

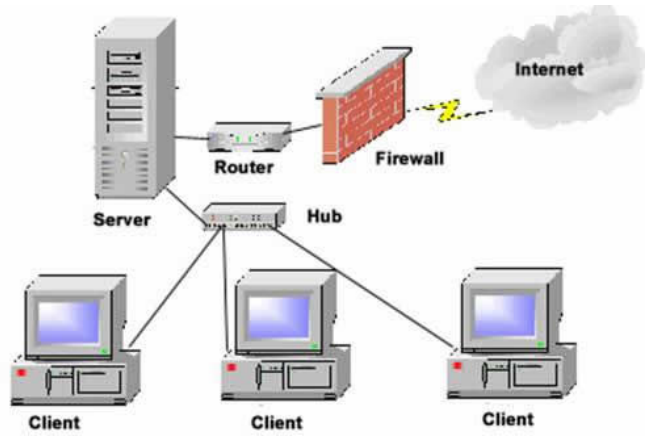
- Antivírus e *antispyware*
- *Firewall*
- Criptografia
- Boas práticas

Antivírus

- Os antivírus constituem uma protecção indispensável em qualquer computador
- A sua função é a de detectar e eliminar ou isolar os vírus ou w*orms* antes que eles causem algum prejuízo no computador infectado
- Os antivírus procuram dentro dos ficheiros executáveis as assinaturas digitais (sequências de código binário) dos vírus conhecidos
- À medida que novos vírus vão sendo descobertos, a base de dados do antivírus tem de ser actualizada para que a protecção continue a ser real

Firewall

- Uma *firewall* é uma aplicação que procura manter uma rede protegida de intrusos
- Permite isolar a rede interna de uma empresa, filtrando o tráfego que entra e sai segundo critérios de segurança
- São muito usados para filtrar o acesso à Internet dos funcionários e para isolar os servidores WWW (de acesso público) da restante rede interna da empresa
- Também podem ser utilizados para isolar determinados segmentos dentro da rede interna



Criptografia

- A criptografia é um processo que permite transformar dados comuns num código secreto dificilmente decifrável
- Nos computadores, a criptografia é utilizada para guardar as *passwords*, para envio de informação pela rede de forma segura, e ainda para construção de assinaturas e certificados digitais
- Trata-se de uma importante arma para garantir a confidencialidade dos dados e, simultaneamente, diminuir a vulnerabilidade aos Crackers

Manter o computador seguro

- Utilizar um antivírus e *anti-spyware* actualizados diariamente, bem como uma *firewall* pessoal
- Actualizar de uma forma rotineira o sistema operativo e aplicações
- Instalar as correcções de segurança disponibilizadas pelos fabricantes dos programas utilizados
- Desactivar partilhas e serviços não utilizados
- Utilizar sempre softwares originais
- Desactivar as macros dos documentos em que não se tenha absoluta confiança
- Fazer sempre cópias de segurança dos documentos mais importantes

Spams, fraudes e vírus por e-mail

- Nunca clicar em programas ou ficheiros recebidos por e-mail cuja origem seja desconhecida e cujo texto seja suspeito
- Verificar com antivírus actualizado os ficheiros recebidos por e-mail antes de os executar
- Activar filtros anti-spam no cliente de e-mail (muitos fornecedores hoje fornecem estes serviços)
- A menos que solicitados, bancos nunca entram em contacto com clientes através de e-mail, muito menos operadores de cartões de crédito
- Desconfiar de TODAS as mensagens recebidas por e-mail cujo conteúdo solicite informações ou actualizações de dados pessoais
- Não clicar em URLs de bancos recebidos por e-mail
  - Normalmente direccionam os utilizadores para sites fraudulentos

Navegando de forma segura

- Acostume-se a digitar sempre manualmente no browser o endereço (URL) do seu banco
- Em acessos a páginas da Internet que peçam login e senha, verificar sempre a presença do cadeado fechado no canto inferior direito do browser
- Desactivar a execução de Java, Javascript, ActiveX, pop-ups e a recepção de *cookies* no browser
  - Activar a execução destes somente para sites confiáveis
- Não divulgar informações pessoais, como telefone ou morada, em sites de relacionamentos pessoais, blogs ou mesmo em *chats* (Icq, Msn, etc).
- Não aceder a páginas bancárias ou que necessitem de informações confidenciais em computadores que não sejam de confiança
  - Exemplo: Cyber-Cafés
- Instalar ferramentas que ajudem a verificar o grau de risco dos URLs acedidos, como o "Anti-Phishing Toolbar", da NetCraft (www.netcraft.com)

Password: cuidados a ter

- Não utilizar *passwords* baseadas em informações pessoais, sequências de números (123456) ou palavras de dicionários
- Alterá-las regularmente
- Utilizar pelo menos 6 caracteres, misturando letras, números e caracteres especiais (, . @ # % * , etc)
- Construir *passwords* baseadas em frases:
  - Frase: Segurança.*é*. importante!
  - Senha: S.*e*.1!
- Caso desconfie que a sua *password* foi violada, modifique-a e avise a instituição envolvida imediatamente

Utilização de redes sem fios

- Utilizar WEP ou WPA sempre que possível
- Esconder o SSID
- Tentar obter informações sobre o SSID da rede que pretendemos aceder antes de nos ligarmos
- Em redes Wi-Fi públicas, evitar aceder a sites de bancos ou outros que necessitem de informações pessoais
- Não criar ligações Ad-hoc (PC a PC) com computadores que não conhecemos
- Desactivar sempre o Bluetooth ou Infravermelhos dos aparelhos (portátil, telemóvel, PDA) quando esses serviços não estiverem a ser utilizados

Desconfiar e denunciar

- Caso se notem diferenças, ainda que subtis, no acesso ao banco através da Internet, entrar imediatamente em contacto com a agência
- Enviar possíveis e-mails de *Phishing Scam* (fraude) recebidos para o grupo de segurança da instituição envolvida
- Em caso de dúvidas sobre como proceder, contactar sempre o grupo de segurança da instituição envolvida