

Etec – Escola Técnica Estadual de Avaré
Técnico em Informática

Segurança Digital

Palestra ministrada na Semana Nacional da Ciência e Tecnologia

Avaré-SP

2010

Etec – Escola Técnica Estadual de Avaré
Técnico em Informática

Segurança Digital
Marcelo de Almeida Borges

Avaré-SP

2010

INTRODUÇÃO

Atualmente o computador chegou a todos os níveis da sociedade, não apenas isso, ele é usado em praticamente todas as profissões, seja estudante ou profissionais que lidam com orçamentos, planilhas, transações financeiras, etc. E falando de computador nos dias atuais fica difícil deixar a internet de fora, e junto dela podemos citar também o grande crescimento de ataques a computadores, invasões e ataques de vírus, que podem acarretar algum prejuízo ou no mínimo transtornos a quem dela utiliza. E se a internet é algo tão importante para todos, precisamos manter nossos dados seguros, e para que isso seja possível precisamos de alguns cuidados especiais, que estaremos abordando nesse trabalho a respeito de nossa segurança de dados na rede.

Requisitos

Segundo a Cartilha de Segurança para Internet criada em 2006 pelo Comitê Gestor de Internet no Brasil, a segurança digital consiste na não violação da confidencialidade, integridade e disponibilidade de autenticidade de documentos e dados pessoais.

Alguns exemplos de violações a cada um desses requisitos são:

Confidencialidade: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda, contas de bancos, senhas, etc.

Integridade: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal;

Disponibilidade: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

Riscos

Os riscos de segurança digital resumem-se a estes aspectos: furto, falsificação ou perda de identidade. Pode acontecer com que alguém obtenha ilicitamente os dados da identidade digital de outrem e os use de forma fraudulenta.

Quem está por traz de uma invasão de computador ?

Obs: Primeiramente devemos nos lembrar que a palavra hacker não está literalmente ligada a algo negativo, na verdade ela é usada para designar um profundo conhecedor do universo da informática.

Hackers: É uma pessoa que tem muita facilidade em lidar com sistemas, tem uma ótima assimilação, compreensão e análise em sistemas computacionais, praticamente pode fazer o que quiser com um computador, e sabe que nenhum sistema está livre de falhas e sabe bem onde encontrá-las. É uma pessoa que busca cada vez mais conhecimento, não tenta derrubar outras pessoas ou prejudicá-las mais sim age em busca de informações que o beneficiarão.

Coders: É realmente um criminoso, sua principal atividade é roubar senhas, seus principais alvos são os usuários de *Internet Banking*. Outras senha como orkut, MSN, *e-mail*, são geralmente roubados por coders amadores com a intenção de causar transtornos a terceiros.

Crackers: Possuem tanto conhecimento quanto os hackers, mas com uma diferença, para eles não basta entrar em um sistema, quebrar senhas e descobrir falhas. Geralmente eles entram e acabam com seus documentos, arquivos e aplicativos existentes em sua maquina, e também gostam de deixar suas marcas, geralmente recados informando que esteve lá, são como os pixadores de muros.

Viruses: São autores de vírus de computador, especializados em programas maliciosos.

Backdoors: São programas utilizados para se retornar a um computador já invadido, sem que haja a necessidade de recorrer a métodos usados na primeira invasão. É a forma de um invasor visitar o micro.

Antivírus.

A segurança que não pode faltar em seu computador, ele pode ser sua salvação.

O que são: como o próprio nome já diz, são ferramentas/aplicativos que detectam, anulam ou removem vírus de um computador.

Principais funcionalidades do antivírus.

1. Identificar e eliminar o maior número de vírus possível.
2. Análise de arquivos baixados via *web*.
3. Verificação dos documentos, arquivos e aplicativos existentes no computador, verificação de *pen drives*, *CDs* e *DVDs* inseridos no computador.
4. Checam arquivos anexados aos e-mails.
5. Atualizam listas de vírus, geralmente disponibilizada pelo fabricante do antivírus, este serviço geralmente é oferecido *on-line* e automaticamente.

Algumas recomendações para o uso do antivírus:

1. Atualizá-los constantemente.
2. Configurá-lo para verificação automática de arquivos anexados aos e-mails e baixados da *web*.
3. Configurá-lo para checar mídias removíveis.
4. Configurá-lo para verificação de todo e qualquer tipo de extensão de arquivo.

Firewall

Uma segurança a mais em seu computador.

O *firewall* é um utilizado contra acesso não autorizado vindo pela *web*, é um programa que visa evitar invasões fechando portas de entrada em seu computador.

Como ele funciona: ele tenta bloquear alguém ou algum programa suspeito que tenta se conectar ao seu computador, um *firewall* bem configurado entra em ação para bloquear suas tentativas de invasão. Existem versões que filtram vírus antes mesmo do antivírus tais como cavalo de tróia e vírus de *e-mail*, e outros que trabalham juntamente com os antivírus para oferecerem maior segurança ao sistema.

Por que instalar um *firewall*?

É muito comum ouvir usuários que acreditam ter computadores seguros por utilizarem somente o antivírus, na verdade o fato é que nos dias atuais um computador não pode utilizar somente um mecanismo de defesa. Um antivírus sozinho não é capaz de impedir o acesso a um *backdoor* instalado em sua máquina, enquanto um firewall, quando bem configurado pode bloquear o acesso ao *backdoor*.

Dicas de Segurança de dados

Para alcançar um nível aceitável de segurança digital é fundamental conhecer e por em prática no próprio computador e ambiente (de trabalho ou familiar) as seguintes "use algumas dicas fundamentais de segurança digital".

Use o filtro de *SPAM* fornecido por seu provedor, ou se não for disponível adquira um para utilizar junto ao seu cliente de email. Ter um sistema capaz de filtrar as mensagens de *SPAM* de forma eficaz é importante, pois grande parte dos e-mails com arquivos maliciosos anexados são normalmente identificados como *SPAM*.

Configure seu navegador (**Internet Explorer, FireFox, Netscape...**) para que peça SEMPRE autorização e confirmação antes de baixar ou executar qualquer coisa na *internet*. Depois não o autorize a baixar nada a não ser que saiba muito bem do que se trata. Como regra nunca execute/abra códigos diretamente da internet, se necessário os baixe/salve e rode depois.

Antes de utilizar um novo site de compras e fornecer dados dos seus cartões de credito ou banco, procure informações sobre sua credibilidade, confiabilidade, solidez, segurança e eficiência. Também verifique que o site utilize, para a troca de dados e informações, uma área segura baseada em criptografia (**SSL**). Para isso confirme que no seu navegador apareça um pequeno cadeado fechado ou uma chave no canto inferior da tela.

Desconfie e rejeite comunicados, propostas e ofertas milagrosas de qualquer tipo que possam chegar por qualquer meio (*e-mail*, **MSN**, salas de bate-papo, *chats* em geral etc...).

Nunca anote senhas e outras informações confidenciais em lugares de fácil acesso (inclusive arquivos não criptografados dentro do seu computador) ou visíveis.

Criminosos podem criar sites que parecem os de bancos ou outras entidades, com o intuito de enganar as vítimas desavisadas e de capturar suas senhas e dados sigilosos. Neste caso o primeiro cuidado é verificar se o endereço que aparece no browser é mesmo o do banco e se este permanece inalterado na hora que

aparecer o *site*. O segundo cuidado é o chamado teste da senha errada ou do "falso positivo". É só tentar acessar utilizando uma senha propositalmente errada e ver se o site aceita esta senha. Sites falsos aceitam qualquer coisa, já os verdadeiros sabem reconhecer a senha válida de uma errada. Se lembre que a enorme maioria dos casos de fraudes envolvendo internet banking acontece por descuidos do usuário e não por falhas de segurança dos bancos. Portanto tome sempre os devidos cuidados quando acessar sua conta e, de forma geral, usar o seu computador.

Sempre e só utilize um computador confiável para acessar sua conta e/ou dados sigilosos. NUNCA use computadores públicos ou de terceiros ou ainda computadores que não tenham sistemas de proteção eficientes para acessar sua conta ou qualquer outra informação sigilosa ou que necessite de uma sua senha (por exemplo, uma caixa de *e-mail*).

Evite navegar em *sites* arriscados e NUNCA baixe qualquer coisa de site que não conheça bem e que não sejam totalmente confiáveis. Como regra geral, sites com material pornográfico e sites que promovem pirataria de software e outros crimes, é perigosa, pois freqüentemente contém vírus, *trojans* ou outros programas maliciosos.

Nunca execute ou abra qualquer arquivo anexado a mensagens de origem desconhecida ou não solicitado. Sobretudo NÃO abra arquivos dos tipos: EXE, COM, BAT, CMD. Também lembre-se de configurar o seu programa cliente de email (**Outlook, Eudora, Thunderbird...**) para que não abra automaticamente os anexos. Na maioria dos casos estes programas são vírus ou *trojans* ou *worms*.

Não se assuste quando receber *e-mails* ameaçadores tipo cobranças, cancelamento de documentos ou benefícios, ações na justiça etc... Também desconfie de mensagens que aparentem ter sido enviada por bancos, repartições públicas, lojas famosas e programas televisivos. Não acredite e não leve a sério este tipo de mensagens, os respectivos órgãos e empresas NUNCA enviam mensagens por email com este intuito. Sobretudo NÃO abra nenhum arquivo anexado a este tipo de e-mails nem acesse nenhum link sugerido.

Não acredite em promessas milagrosas, ofertas mirabolantes, propostas fabulosas e também não acredite em vendas simplificadas de produtos ou serviços que deveriam estar sujeitos a controle (tipo medicamentos ou coisas parecidas). Na maioria dos casos se trata de golpes ou produtos falsificados e até perigosos ou prejudiciais.

Não forneça seu endereço de email para publicação em fóruns, salas de bate papo e grupos de discussão. A mesma regra vale para qualquer outra informação pessoal como nome completo, endereço, telefone, números de documentos (RG, CPF, CNH...), lugar de trabalho etc...

Evite sempre participar de qualquer tipo de corrente na rede, sejam pirâmides financeiras sejam supostas ou reais campanhas de solidariedade seja o que for. Também desconfie muito de qualquer oferta que lhe chegue pela rede e onde exista a solicitação de um pagamento adiantado.

10 sinais de que o PC pode estar em má companhia

1. O *cooler* funciona em alta velocidade mesmo quando o computador está ocioso.
2. O PC leva muito tempo para desligar, ou não desliga corretamente
3. Conteúdo no mural de redes social não enviado pelo usuário.
4. Os programas estão muito lentos.
5. Não é possível baixar atualizações do sistema operacional.
6. Não é possível baixar as atualizações do antivírus.
7. Internet muito lenta.
8. Seus amigos e familiares têm recebido emails seus que você não enviou.
9. *Pop-ups* e anúncios se abrem, mesmo quando não se está usando um browser.
10. O **MS-Windows** exibe no Gerenciador de Tarefas programas com nomes e descrições suspeitas.

É bom lembrar que alguns destes sintomas podem estar presentes por outras razões - atualizações do sistema, sujeira nos componentes, *bugs* no sistema ou programas. Vale verificar com as ferramentas de segurança se algo suspeito está na máquina. No caso do gerenciador de tarefas, os usuários mais avançados podem até dar uma olhada no registro do sistema, e visualizar quais programas estão sendo carregados.

Dicas para elaboração de senhas

A primeira coisa que devemos lembrar é que a senha deve ser pessoal e intransferível, ela serve para identificar o usuário e por isso deve ser preservada. Se uma pessoa tiver acesso a sua senha ela poderá se passar por você, enviar mensagens em seu nome ou até mesmo obter informações importantes a seu respeito.

Uma senha pode ser denominada como uma chave que lhe irá abrir portas de acesso.

É comum algumas pessoas usarem o número da casa, conta bancária, data de aniversário ou do telefone, esta prática não é recomendável e aconselhável, pois são os primeiros itens que uma pessoa tentará buscar o seu respeito e tentarão usá-las.

Se você tem varias atividades em vários lugares, jamais deverá utilizar a mesma senha, pois se alguém a descobrir você estará literalmente acabado, principalmente se trabalha em setores como o financeiro então se lembre lugares diferentes senhas diferentes.

O ideal é que se troque as senhas com regularidade, pois períodos muito longos podem facilitar para que alguém as descubra, utilize senhas especiais utilizando letras, números e caracteres especiais tais como @, %, \$, &, etc...

CONSIDERAÇÕES FINAIS.

Como vimos anteriormente existem várias maneiras para se proteger contra invasões, ataque de vírus existentes na rede, como manter seus dados seguros, porém a melhor maneira de mantê-los seguros e protegidos não está ligados a combater vírus ou invasões, e sim fazer uma cópia de segurança de seus arquivos e dados importantes - o famoso *backup* -, não só contra vírus e ataques, mais também contra possíveis falhas no sistema ou em seu *hardware*.