OFICINA DE LÍNGUA PORTUGUESA – LEITURA E PRODUÇÃO DE TEXTOS (UNI 003)

UFMG – ICEX – CIÊNCIA DA COMPUTAÇÃO

2º SEMESTRE 2010

Superioridade do Linux sobre Windows no quesito segurança

Thiago de Freitas Faria

Lucas Moreira Carneiro de Miranda

Belo Horizonte, 8 de novembro de 2010

RESUMO

Atualmente, há uma grande diferença de segurança entre Linux e Windows. Apesar de ter código fechado, o que alguns diriam ser de grande auxílio no quesito segurança, o Windows é, certamente, mais inseguro que o Linux, uma vez que permite, mais facilmente, o acesso a regiões importantes do sistema. Além disso, o Windows é mais visado por ataques maliciosos, uma vez que abrange um grupo maior de possíveis alvos, e tem uma equipe de segurança, para correção de erros, muito inferior ao Linux.

Palavras-chaves:
SEGURANÇA, LINUX, WINDOWS

1 INTRODUÇÃO

Existem atualmente diversos sistemas operacionais, tais como Windows, Linux, Mac, cuja função é manter seus programas funcionando da maneira correta, coordenar a interação entre hardware e software, dentre outras coisas. Para que isso seja feito da maneira correta, é indispensável que esses programas estejam seguros, protegidos de qualquer software malicioso que possam danificá-los, modificando-os para que exerçam funções diferentes daquelas que deveriam fazer e, com isso prejudiquem o funcionamento correto do seu sistema.

Analisando esse ponto de vista, será tratado aqui, as diferenças de como dois desses sistemas operacionais, o Windows e o Linux, lidam com esse problema, sabendo-se que nenhum deles é completamente seguro e livre de qualquer ameaça. E que, apesar de muitos crerem no contrário, o Linux é mais seguro do que o Windows.

2 DESENVOLVIMENTO

2.1 Popularidade: Maior o uso, maior o alvo

Já faz muito tempo que o sistema operacional Windows é o mais popular no mundo dos computadores pessoais. Ele apresenta uma série de funcionalidades que atraem os seus usuários: interface gráfica bem elaborada, drivers para diversos periféricos, jogos compatíveis e uma série de programas úteis e simples de utilizar. Apesar de sua hegemonia, alguns aspectos deixam a desejar neste sistema. Com isso, o Linux, um software livre, vem crescendo e se tornando um forte concorrente, superando os pontos fracos do líder do mercado, principalmente em relação à segurança.

Por ser o mais utilizado, o Windows acaba se tornando um alvo muito visado por vírus, malwares, trojans e outros algoritmos maliciosos. Para buscarem sua segurança, seus usuários precisam instalar um bom antivírus, programas para detectar ameaças e firewalls, o que torna o sistema mais lento e não o livra completamente do risco de infecção. Do outro lado, a maioria dos arquivos que circulam pela internet contendo esses códigos maliciosos são inofensivos para uma distribuição do Linux, por funcionar de forma diferente e não ter as mesmas vulnerabilidades. Estes programas maliciosos aproveitam algum defeito (bug) do sistema para conseguirem acesso a programas e informações importantes daquele computador, afetando seu funcionamento correto.

Sendo o Windows uma distribuição praticamente única, com poucas mudanças de uma versão para outra, um determinado vírus consegue afetar a todos sem grandes dificuldades. Já no Linux existem diferentes ambientes, tais como Ubuntu, Fedora, Kubuntu, com isso um determinado vírus tem um acesso limitado àquele ambiente, atingindo um número muito inferior de pessoas.

2.2 Bugs: Equipes de detecção e correção

Estes bugs não são raros devido à dificuldade de desenvolver softwares. Os programas por si só, são uma abstração de zeros e uns, realizando operações complexas dentro de um ou vários processadores. Com isso a chance de erros e bugs é bastante alta, tanto que a frase: “Se o programa não tem bugs, você não procurou direito” é bastante comum na computação. Sabendo-se que em um programa simples já ocorrem muitos desses problemas, em um sistema complexo que coordena diversos outros programas, a possibilidade é muito maior.

Existem muitas pessoas procurando esses bugs que possam causar falhas de seguranças no Windows. Quando encontram, normalmente, ou reportam à Microsoft, para que haja alguma correção, ou propagam a informação para comunidades de hackers com o objetivo de aproveitar a falha, utilizando algoritmos maliciosos que atacam aquele ponto. Nesse segundo caso, o defeito demora para chegar até a equipe de segurança da Microsoft, reduzida a um grupo pequeno de funcionários e com isso demora a ser corrigido, podendo ocasionar diversos problemas para os usuários desse sistema.

Já no caso do Linux, apesar de haver uma quantidade grande de bugs, como ocorre no Windows, existe uma equipe muito maior corrigindo-os. Uma vez que o código fonte é disponível, qualquer pessoa do mundo pode abri-lo, lê-lo, entendê-lo, modificá-lo e distribuí-lo, tem-se, então, um grupo de pessoas muito maior para reportar e corrigir o erro. Por isso, quando um bug é encontrado e informado para a comunidade Linux, várias pessoas espalhadas por todo o mundo se empenham em desenvolver uma correção. Assim, com um número maior de pessoas com o acesso ao código fonte, apesar de também ter várias falhas, essas são rapidamente descobertas e corrigidas, muitas vezes antes mesmo que todos tenham conhecimento delas. Já o Windows tem seu código fonte fechado, somente os funcionários da empresa que o produz possuem acesso a este. É nítida a desvantagem em relação ao software livre.

2.3 Permissões de acesso

Uma das vantagens do Linux está na forma como são definidas as permissões de usuários. No Linux o acesso a áreas importantes não é dado a todos. Por padrão, um usuário tem uma conta de baixa prioridade e apenas o usuário "root" tem permissões de acessar e modificar determinadas pastas e arquivos. Mesmo que um sistema Linux seja infectado, o vírus não terá o acesso “root” necessário para atacar todo o sistema. Ele só poderá comprometer arquivos e programas locais daquele usuário afetado, causando apenas problemas pequenos e locais.

Já no Windows todos os usuários têm acesso de administrador como padrão, podendo acessar todas as pastas e arquivos, inclusive locais de risco que controlam partes importantes do computador. Dessa forma um vírus ao infectar um usuário também terá acesso a tais áreas, podendo ocasionar grandes estragos ao sistema.

2.4 Dados Importantes

Em locais em que é necessário ter uma segurança maior dos dados o uso de programas com código aberto é importante. É possível pesquisar por falhas em todo o código e corrigi-las. Quando se usa um software com o código indisponível ou proprietário, não é possível ter esse nível de acesso. Uma vulnerabilidade poderia ser acessada por aquele que conhece o código, um funcionário da empresa que o desenvolveu, por exemplo, sem que este sequer saiba que ela existe, deixando assim o sistema desprotegido. Sendo mais seguro, então, utilizar uma tecnologia que não seja controlada por um determinado grupo, como acontece com alguns bancos, a chave da segurança não fica na mão do fabricante e sim do próprio banco, logo o usuário daquele recurso tem acesso aos meios de segurança para sua proteção.

3 CONCLUSÃO

Não existe um sistema operacional sem falhas, todos possuem brechas que comprometem sua segurança. Os usuários devem ter em mente essa questão, tomando medidas para reduzir o risco de uma invasão. Evitar a instalação de arquivos de procedência desconhecida e utilizar um bom firewall são algumas destas medidas. Com o que foi analisado, pode-se afirmar que os usuários de Linux estão menos sujeitos a esses problemas de segurança, tendo assim um sistema operacional mais seguro para utilizar.

4 REFERÊNCIAS BIBLIOGRÁFICAS

Novo no Software Livre. Disponível em : <http://www.ibm.com/developerworks/br/opensource/newto/#1 > Acessado em: 6 de novembro de 2010

Qual sistema é mais seguro, Linux ou Windows? Disponível em: <http://softwarelivre.org/asl-pr/qual-sistema-e-mais-seguro-linux-ou-windows> Acessado em: 6 de novembro de 2010

Segurança no Linux. Disponível em <http://linux-sem-misterio.blogspot.com/2006/02/segurana-no-linux_27.html> Acessado em: 8 de novembro de 2010