UNIVERSIDADE FEDERAL DE MINAS GERAIS

A SEGURANÇA NA INTERNET E SUA RELAÇÃO COM O DESENVOLVIMENTO DE SOFTWARES LIVRES

Albert Douglas de Castro Costa
Hugo Pereira Lima Junior
Marcela Claudia Carvalho
Raphaella Carvalho Diniz

Belo Horizonte
2010

Albert Douglas de Castro Costa
Hugo Pereira Lima Junior
Marcela Claudia Carvalho
Raphaella Carvalho Diniz

A SEGURANÇA NA INTERNET E SUA RELAÇÃO COM O DESENVOLVIMENTO DE SOFTWARES LIVRES

Artigo apresentado ao UEADSL – Universidade, EAD e Software Livre 2010 e à Faculdade de Letras da UFMG.
Disciplina: Oficina de Produção de textos
Universidade Federal de Minas Gerais
Coordenadora: Prof.ª Ana Cristina Fricke

Belo Horizonte
UFMG
2010

RESUMO

Uma das maiores vantagens para os usuários de software livre é proveniente do fato de que a liberdade de acesso ao código-fonte permite um fluxo constante no processo de atualização e correção de *bugs*. Softwares livres não são presos às suas empresas desenvolvedoras como são os softwares proprietários: geralmente existe uma gigantesca comunidade por trás da manutenção dos mesmos, organizada de tal forma que o reporte de erros/falhas promove a rápida solução de problemas. Esta característica faz do software livre uma alternativa muito segura na qual um usuário não está confiando apenas no nome de uma empresa proprietária, mas na *expertise* de desenvolvedores e interessados em todo o mundo.

O Software Livre e sua filosofia podem minimizar os efeitos dos programas considerados nocivos, baseando-se na sua política de colaboração. No âmbito dos Sistemas Operacionais, por exemplo, o Windows é um dos mais visados atualmente por vírus, *spywares* e outros softwares potencialmente prejudiciais. Esses programas procuram coletar informações sobre o usuário, alterar as configurações do computador, comprometer o desempenho, excluir e danificar dados. Além disso, muitos *sites* como bancos, servidores de e-mails e redes sociais também podem ser atacados por essas aplicações.

Permitir que vários usuários espalhados geograficamente possam contribuir no desenvolvimento do produto é uma das principais vantagens do Software Livre. Essa característica faz com que as discussões sobre segurança entre os desenvolvedores sejam mais frequentes e o produto tende a crescer com isso. A todo o momento, desenvolvedores e usuários verificam novas falhas e podem reportá-las imediatamente à comunidade de software livre ou corrigi-las diretamente. Cabe a toda a comunidade estar atenta às ameaças e desenvolver um produto seguro.

Porém, até que ponto as pessoas devem se preocupar com a segurança na rede? No mundo da Internet, quebras de segurança ocorrem a todo instante e quase nunca a polícia consegue rastrear e punir os seus malfeitores. Dentre as invasões mais trágicas e assustadoras promovidas por hackers até hoje está o *worm* WANK (*Worms Agains Nuclear Killers*) que fez com que aparecesse um *banner* em todos os computadores do sistema da NASA, como um protesto contra o lançamento de uma sonda a Júpiter. Outro caso assustador foi a invasão ao CDUniverse.com, onde foram roubados 300 mil números de cartão de crédito por um hacker de codinome Maxim que exigiu 100 mil dólares como chantagem para destruir os dados.

Palavras-Chave – Segurança, Internet, Software Livre, vírus, rede

SUMÁRIO

1 INTRODUÇÃO

Software livre, segundo a definição criada pela *Free Software Foundation* é qualquer programa de computador que possa ser usado, copiado, distribuído e redistribuído sem restrições. O software livre foi criado com o intuito de se opor ao conceito de software proprietário e proporcionar aos seus usuários maior flexibilidade de adaptação e melhoria de seus sistemas, além da correção de erros mais rápida e eficiente, proporcionando ainda maior confiança na segurança do software.

O crescimento do número de aplicações de software livre indica uma mudança de comportamento e paradigma que nossa sociedade está passando. Empresas, usuários e desenvolvedores passaram a questionar a propriedade sobre o conhecimento e estão buscando alternativas sustentáveis e colaborativas. Nesse trabalho, apresentaremos os benefícios desse novo paradigma para a segurança e quais são as novas preocupações em relação a isso.

Atualmente, existem opções de software livre em diversos segmentos de aplicações, desde editores de texto até antivírus. Mas o que muitos se perguntam é sobre a questão de segurança nas opções livres. Essa discussão sobre segurança entre softwares livres eu proprietários é válida e fruto de muitas discussões entre os usuários, afinal, segurança de softwares é um assunto que vêm ganhando espaço e que afeta diretamente os usuários.

O dinâmico cenário da Internet em constante evolução faz com que as questões de segurança sempre estejam presentes nas pautas de discussões sobre o mundo virtual. Existe uma série de práticas e ferramentas que podem ser utilizadas para aumentar a proteção dos usuários da rede e seus serviços, mas nem sempre isso é o bastante. Este é um assunto que constantemente se renova à velocidade das mudanças tecnológicas e comportamentais na Internet.

2 OS BENEFÍCIOS DO SOFTWARE LIVRE

Os softwares livres são comumente distribuídos, embutindo a eles uma licença de software livre e disponibilizando o seu código fonte.

No inicio dos anos 80, Richard M. Stallman foi o primeiro a formalizar esta maneira de pensar para o software sobre a forma de quatro liberdades:

- **1ª liberdade**: A liberdade de executar o software, para qualquer uso.
- **2ª liberdade**: A liberdade de estudar o funcionamento de um programa e de adaptá-lo às suas necessidades.
- **3ª liberdade**: A liberdade de redistribuir cópias.
- **4ª liberdade**: A liberdade de melhorar o programa e de tornar as modificações públicas de modo que a comunidade inteira beneficie da melhoria.

O software que siga esses quatro princípios é chamado "Software Livre" (ou *Free Software*).

Muitos defendem que o Software Livre é mais seguro que as soluções proprietárias. De fato, o GNU/Linux possui desde sua idealização uma grande consideração com a segurança; sua definição de permissões é bem clara e nada é executado sem autorização do Administrador. Os riscos de invasões e infecções por vírus chegam a ser insignificantes se comparados a sistemas proprietários.

Por possuir uma comunidade de milhões de programadores e usuários espalhados pelo mundo, trabalhando muitas vezes por paixão e não por obrigação, os Softwares Livres são geralmente mais testados e a correção de *bugs* e atualizações é mais rápida do que nos Sistemas e Softwares Proprietários. Também não existe a necessidade de uma suíte de aplicativos para trabalhar (como a *Creative Suite* da Adobe), pois todos os softwares que possam vir a ser escolhidos trabalham com formatos de arquivos abertos, prevalecendo assim a compatibilidade e a liberdade na escolha das aplicações a serem usadas.

2.1 Cultura Livre e sua Filosofia

No atual cenário de pirataria cada vez mais frequente de softwares proprietários, surge uma nova opção: a **Filosofia do Software Livre.**

A filosofia do Software Livre encontra as suas raízes na livre troca de conhecimentos e de pensamentos que podem tradicionalmente ser encontrada no campo científico. Tal como as ideias, os programas de computador não são tangíveis e podem ser copiados sem perda. A sua distribuição é a base de um processo de evolução que alimenta o desenvolvimento do pensamento.

A filosofia ao Software Livre é acima de tudo um respeito ao uso de um aplicativo. Se pretende-se fazer um serviço e desempenhar o melhor com o que se sabe, é preciso ter um conhecimento pleno e reconhecer os desafios que podem surgir como frutos de seus próprios erros.

O Software Livre e a sua filosofia se resumem ao uso consciente do computador, no estudo das funções por trás de cada clique ou do código liberado.

Os programadores por trás do Software Livre buscam não apenas desenvolver aplicativos “grátis”, mas principalmente possibilitar que o conhecimento ali empregado esteja disponível a todos. Em uma comunidade de Software Livre, o aperfeiçoamento vem através de uma comunidade cansada dos erros encontrados em outros softwares com ideias inovadoras que são melhoradas numa verdadeira tempestade mental de sugestões e inovações.

Quando estamos falando de Software Livre, não estamos falando apenas de um produto, mas de uma abordagem ampla das possibilidades de se usar um computador. Falamos também em economia de custo e na possibilidade de muitos técnicos utilizarem seu conhecimento não só para sanar dúvidas, mas para compartilhar o conhecimento. Essa é a verdadeira filosofia da cultura livre.

2.1.1 A Liberdade de acesso ao código fonte

A liberdade de acesso ao código fonte beneficia os utilizadores em vários sentidos. Sem o acesso ao código nem ao direito de modificá-lo e distribuir uma versão como openSUSE simplesmente não seria possível obter todos os benefícios abaixo:

- **Correção / Adaptação do software**: Como o código é aberto, é possível implementar modificações livremente no software a fim de corrigir *bugs* ou falhas de segurança ou ainda adaptar o software para contextos e funcionalidades distintas.
- **Colaboração**: O software livre permite que o mesmo seja partilhado entre toda a comunidade interessada, compartilhando seus benefícios com mais usuários e permitindo que novas melhorias sejam desenvolvidas.
- **Conhecimento e controle da segurança**: Com softwares livres e o acesso aos seus códigos, é possível interpretar o que realmente o software faz “nas entrelinhas” e modificar caso encontre alguma funcionalidade ofensiva. Já com softwares proprietários, sabe-se que muitos espiam os seus usuários e varrem informações acerca do mesmo representando risco à segurança, além de quebra da privacidade, mas nada pode ser efeito para definitivamente descobrir e eliminar esses códigos espiões.
- **Evolução constante**: Como o software livre é de código aberto, as manutenções nunca terminam. O software está em constante evolução. Assim ele nunca fica defasado, está sempre atualizado segundo novos padrões e

> técnicas, além de se tornar uma grande manifestação do princípio Beta Perpétuo.

2.1.2 O Princípio da Colaboração

Software Livre é mais do que apenas disponibilizar o código a todos. O conceito de Software Livre envolve toda uma discussão acerca da colaboração e do trabalho em comunidade.

A comunidade do Software Livre propõe o compartilhamento entre os usuários. Cada nova versão ou modificação de um software livre deve ser distribuída entre toda a comunidade.

Muitos *bugs* e correções de falhas de segurança beneficiam toda a comunidade graças ao princípio da colaboração intrínseco ao conceito de Software Livre. A preocupação de cada membro em não somente divulgar problemas encontrados em distribuições de softwares, mas ainda corrigir e partilhar novas distribuições é que fez com o que o Software Livre tivesse se disseminado tão rapidamente e favoravelmente.

Até mesmo os governos têm incentivado o uso de Software Livre alegando que os mesmos são muito menos propensos a falhas e quebras de segurança, uma vez que a colaboração mútua entre os desenvolvedores e usuários age muitas vezes mais rapidamente do que os mal intencionados destinados a implantar códigos maliciosos em softwares.

O Brasil é um ótimo exemplo dessa preocupação do governo em incentivar o uso e o desenvolvimento de softwares livres. Para se conseguir patrocínio do governo brasileiro em projetos de ONG's envolvendo tecnologia da informação, é necessário que uma determinada parte utilize software livre em oposição a softwares proprietários.

2.2 Diminuição de erros e os benefícios reais para o usuário

Além do objetivo a que se propõe o Software Livre e de seus princípios como código aberto e colaboração, um dos seus benefícios mais cobiçados é a diminuição de erros, inconsistências e instabilidades para o usuário final.

Para as empresas, este benefício se resume predominantemente na segurança das transações que precisa executar no seu trabalho diário e no armazenamento de dados confidenciais e estratégicos para a organização.

Um exemplo claro que evidencia as vantagens para empresas que optam pelo uso de softwares livre, além, é claro, do custo, é a confiança de que invasões de segurança são muito mais raras para um banco, por exemplo, que precisa garantir não só a consistência como a garantia de suas transações.

Para o usuário final, por ouro lado, é muito mais visado como um benefício a garantia da segurança ao navegar pela Internet e disponibilizar informações confidenciais em cadastros na web. Para isso, o uso de softwares livres evita tanto as possíveis invasões de spywares,

quanto a ocorrência de erros inesperados em aplicações web que também utilizem softwares livres.

A redução de erros, por outro lado, é um ponto fundamental para qualquer tipo de usuário em qualquer categoria de software. E é neste ponto também que o software livre se destaca mais uma vez. Graças a sua evolução constante e à colaboração de toda a comunidade do Software Livre, eventuais erros são corrigidos assim que identificados por algum membro e as versões corrigidas são distribuídas para todos os usuários.

3 O SOFTWARE LIVRE E SUAS APLICAÇÕES

O Software Livre possui diversas aplicações e hoje pode substituir grande parte dos programas mais utilizados pelos mais diferentes tipo de usuários, desde leigos a profissionais. Além do Linux como Sistema Operacional livre, podemos encontrar diversos aplicativos desenvolvidos sob a ótica dessa filosofia, como programas para escritório (editores de textos e planilhas), navegadores de internet, correio eletrônico, Messenger, firewall, antivírus, tratadores de imagem, gerenciamento de banco de dados e softwares educativos.

Essa proliferação de aplicações se explica pelas vantagens que o software livre possui sobre o software proprietário. Por ser gratuito, já explica grande parte da migração de usuários comuns e empresas para esses softwares. Mas, além disso, a liberdade de execução, de estudo, de distribuição e de melhoria torna-se um grande benefício para aqueles que se interessam em desenvolver e aperfeiçoar suas ferramentas.

3.1 O Linux e suas vantagens em relação à segurança

Como dissemos anteriormente, são grandes as vantagens do software livre sobre o proprietário. No entanto, a questão da segurança entra como fator importante. Vamos explicitar alguns fatores que evidenciam essa diferença o que pode fazer com que o software livre agregue valor nesse sentido:

- Definição de permissões: muitos desenvolvedores têm se empenhado no sentido de fazer com que seus programas possuam formas de determinar o acesso aos seus recursos pelo tipo de usuário. Isso se mostra uma vantagem importante, uma vez que softwares proprietários carecem desses recursos por terem código fechado e execução limitada.
- Grande número de teste: a liberdade de estudo e execução garante ao software livre grande número de testes por diversos usuários e desenvolvedores do mundo inteiro. Além disso, a correção de *bugs* pode ser realizada infinitamente mais rápida.
- Risco de invasão: o risco de invasão por programas mal intencionados é bem menor que o do software proprietário. Os motivos que levam a isso discutiremos a seguir.

Assim como as aplicações de software livre, o Sistema Operacional Linux possui todas essas vantagens sobre os demais sistemas operacionais. Contudo, há uma discussão grande que envolve o fato de que invasões, ataques e falhas nesses sistemas sejam substancialmente menores que nos demais. Alguns pontos são importantes destacarmos antes de julgar os softwares proprietários como os causadores ou as fontes dos problemas de segurança:

1. **Escalabilidade**: não é novidade que sistemas como o Windows e aplicativos como Internet Explorer ainda fazem parte do cotidiano de grande parte dos usuários. Isso ajuda a explicar o ataque de programas mal intencionados a esses softwares e porque a questão da segurança nesses casos é mais preocupante.
2. **Usuários leigos**: ainda há uma grande discussão em torno de Linux vs. Windows, e grande parte disso se dá pelos problemas de usabilidade que o primeiro pode apresentar. Com isso, temos um afastamento de usuários leigos

e certa rejeição por parte dessas pessoas, fazendo com que o Windows domine grande parte dos computadores pessoais e corporativos. Porém, temos a questão: quem está mais preparado para se precaver e para evitar ataques que visem explorar a confiança das pessoas e sua possível falta de informação? Logicamente, a concentração de usuários mais experientes na utilização do Linux diminui drasticamente seu risco de contaminação.

3. **Colaboração entre desenvolvedores**: as comunidades virtuais estão empenhadas em melhorar constantemente os programas, fazendo com que as atualizações dos mesmos ocorram de forma muito mais rápida, até mesmo pela própria política das empresas privadas de desenvolvimento. Isso faz com que estes softwares estejam mais preparados para possíveis ataques e invasões.
4. **Aspecto organizacional**: a organização privada pode trazer muitos benefícios para os softwares proprietários. Muitas seguem padrões internacionais que ditam aspectos de desenho, desenvolvimento, teste e implantação desses programas. Tudo isso, apesar de trazer 'perdas' em relação às atualizações, não deve ser desconsiderado.

3.2 Programas muito visados: Software Livre como Alternativa

Até pouco tempo, a ausência de leis que abordam crimes de informática era algo preocupante para empresas e usuários. O mercado de segurança na rede cresce em torno de 20% ao ano, alimentado por esse medo constante e pelo aumento do número de transações comercias e financeiras na internet. Mesmo com várias campanhas em favor do uso da internet para diversas operações rotineiras, ainda prevalece a dúvida sobre os riscos que estamos correndo na rede.

Como já dissemos, o software livre pode ser uma alternativa para programas proprietário por vários motivos, dentre eles a segurança. O princípio da colaboração e a filosofia da liberdade garantem que os programas possam se adaptar à realidade do usuário e que sejam atualizados constantemente a partir das descobertas de desenvolvedores do mundo todo.

Os ataques podem vir de várias formas e seu sucesso depende, e muito, dos usuários. Esses softwares mal intencionados podem ser classificados de várias formas, de acordo com seu objetivo e a sua forma. Dentre eles citamos:

- Engenharia social: esse termo tornou-se popular nos últimos tempos por denominar práticas utilizadas para obter acesso a informações pessoais e sigilosas de outros usuários, explorando falhas nos programas que elas utilizam.
- *Phishing*: é uma fraude onde alguém tenta se passar por outra pessoa para tentar ganhar a confiança da vítima e, dessa forma, obter suas informações ou arquivos pessoais.
- *Cross*-site *scripting*: é uma forma de ataque que ocorre quando usuários acessam páginas da web que contenha código malicioso ou quando alguém quer burlar as políticas de segurança da página.

Por esses motivos, não podemos simplesmente afirmar que o software livre seria uma solução definitiva. O software proprietário possui muitos benefícios providos pela experiência e organização das empresas privadas. Além disso, a muito que desenvolver quanto à usabilidade e integridade desses programas, o que não significa que as comunidades de cultura livre e sua filosofia não possam ajudar nessa área também. Entender os aspectos da

Engenharia Social pode ajudar na diminuição dos riscos e na conscientização dos usuários, são leigos ou experientes.

3.3 Software Livre nas Empresas

Está cada vez mais comum encontrar empresas onde o Sistema Operacional básico é o Linux. Muitos dos usuários se vêem obrigados a lidar com esses programas, seja para desenvolver suas tarefas na empresa onde trabalha, seja nas escolas que optaram pelo software livre.

No ambiente corporativo, questões como segurança é fundamental. Mas, além disso, o crescimento do software livre pode ter diversos motivos, seja pelo aspecto técnico ou pelo aspecto ‘filosófico’. Dentre essas razões, podemos citar:

- Preço: a gratuidade dos softwares é um dos grandes atrativos para empresas que buscam diminuição de custos e não podem se arrisca a utilizar um software pirata.
- Assistência técnica: o que era um grande problema das comunidades de software livre não é mais. Pelo menos para o Linux, as empresas já podem contar com atualizações constantes e assistência técnica
- Incentivo do governo: o governo brasileiro incentiva iniciativas de promoção ao software livre, beneficiando aquelas empresas que desejam utilizar esses softwares e principalmente as estatais, que vêem seus custos reduzidos sem terem que pagar licenças

4 A VANTAGEM DO SOFTWARE LIVRE SOBRE O SOFTWARE PROPRIETÁRIO NAS QUESTÕES DE SEGURANÇA

A questão da segurança é um assunto muito discutido entre os usuários de todo o mundo. Hoje, grande parte dos usuários se preocupa com o sigilo de suas informações, principalmente de senhas e dados pessoais. Além da preocupação com seus dados, a questão da quebra de privacidade é outro foco de preocupações. A maioria dos usuários já conhece sobre falhas de segurança, invasões, vírus. O que, antigamente, era foco somente de alguns, hoje é conhecido pela grande maioria e fruto de muitas ações contra esse tipo de falha.

A segurança vem se tornando foco no desenvolvimento das aplicações. Hoje, parte do tempo de desenvolvimento contempla a análise de possíveis ataques e o modo de cercá-los. Campanhas são feitas para alertar os usuários sobre comportamentos de risco, senhas seguras, sites e aplicativos maliciosos.

Nessa discussão, a segurança de aplicações também é importante. Nos últimos tempos, surgiram várias discussões sobre a segurança de software livre e proprietários. Alguns dizem que softwares proprietários são mais seguros, pois, geralmente, possuem uma grande empresa por trás que financia todo o desenvolvimento. Porém, grande parte dos usuários vem dizendo que softwares livres trazem maior segurança. O argumento utilizado é a contribuição da comunidade de software livre, erros abertos, possibilidade de correção pelos próprios usuários, comunicação de erros diretamente à comunidade responsável pelo desenvolvimento.

De fato, não se pode dizer ao certo qual modelo de desenvolvimento provê aplicações mais seguras, mas serão levantados pontos que indicam que o desenvolvimento de software livre possui mais pontos que indiquem menor possibilidade de sofrer com graves problemas de segurança.

4.1 A contribuição das comunidades

As comunidades de software livre são grupos de usuários que interagem para contribuir para uma aplicação livre. Na maioria das vezes, esses usuários estão em localizações geográficas distintas e não se conhecem. Todos têm como objetivo contribuir para o desenvolvimento, suporte, correções e evoluções do software. Qualquer pessoa que queira colaborar ou aprender pode fazer parte desse grupo.

A comunidade é composta por regras e têm sua própria metodologia para contribuição. Geralmente, toda a comunidade desenvolve o produto e fica atenta aos problemas que pode apresentar. Essa característica faz com que os problemas e falhas sejam cercados mais rapidamente que os softwares proprietários.

Nos softwares proprietários, espera-se que uma falha seja descoberta, então a empresa responsável mobiliza sua equipe para efetuar a correção do problema. Ocorre uma série de processos até que uma nova versão ou uma atualização do sistema seja disponibilizada.

No software livre, toda a comunidade pode se empenhar para que, assim que uma falha é detectada, seus membros podem imediatamente corrigi-la.

A grande quantidade de colaboradores, a possibilidade que cada usuário tem de corrigir o problema individualmente tornam o processo mais rápido. Há também a minimização de erros devido às discussões internas da comunidade sobre segurança. Vários colaboradores com experiências e vivências diferentes podem apontar possíveis falhas, melhores técnicas de desenvolvimento para reduzir erros e problemas de segurança, formas de se corrigir um problema. A própria comunidade é um centro de conhecimento utilizado para aperfeiçoar a aplicação, corrigir seus problemas e, conseqüentemente, tornar o usuário final mais satisfeito.

4.2 Segurança vs. Software Livre

Muitas pessoas indicam que softwares proprietários são mais vulneráveis a problemas de segurança, principalmente quando se fala de sistemas operacionais e seus programas nativos. Essa afirmação, em partes, é um mito, pois se estima que a grande maioria dos usuários utilize softwares proprietários ao invés das opções livres. Por essa razão, as falhas de segurança são mais exploradas nesses programas que têm maior representação no mercado, sejam eles sistemas operacionais, navegadores de internet, softwares para edição de texto. Existem mais pessoas usando essas aplicações e, conseqüentemente, mais pessoas tentando explorar suas falhas, de forma maliciosa ou não. Outro detalhe é que, com mais pessoas utilizando, normalmente surgem mais problemas oriundos da utilização natural dessas pessoas. Dessa forma, muitos afirmam que softwares proprietários possuem mais falhas sem levar em consideração esses tópicos.

Porém, pela sua própria filosofia, softwares livres possuem um ambiente mais propício à correção de erros. Primeiramente, quando uma falha ocorre em uma aplicação livre, o próprio usuário pode corrigi-la, sem necessidade de passar por todo o processo que um software proprietário acarreta. Esse usuário pode, inclusive, comunicar imediatamente a correção na comunidade para que outros usuários de protejam e se beneficiem.

Como o software livre possui código aberto, qualquer um pode analisar esse código, alterá-lo e descobrir novas falhas. Isso também ajuda na correção de problemas, pois, ao contrário dos softwares proprietários, o código do erro é aberto. O usuário sabe em que parte e porque o problema aconteceu.

Existem hoje, aplicações de segurança, como antivírus e firewalls desenvolvidos na metodologia do software livre. A grande vantagem desses softwares é que, logo um novo vírus seja detectado, sua proteção pode ser desenvolvida dela comunidade e disponibilizada. Existem também aplicações em outras áreas que, por serem desenvolvidas por membros da comunidade que também são usuários, podem atender melhor às expectativas dos usuários quanto a usabilidade e funcionalidade. Quando se sabe a forma como o programa é utilizado, antecipa-se problemas de segurança.

Porém, uma vantagem e, ao mesmo tempo, desvantagem para a segurança de software livres é a possibilidade de o próprio usuário personalizar sua aplicação. Como o código fonte é aberto, os usuários finais podem alterá-lo e adaptá-lo às suas necessidades. Do ponto de vista funcional, essa característica favorece o usuário, pois ele poderá ter uma aplicação customizada, que atenda melhor às suas necessidades, por um preço mais acessível e o suporte da comunidade de software livre por trás. O código pode ser adaptado, melhorado, novas funcionalidades podem ser incluídas da forma que atenda melhor o usuário. Porém, alterações no código podem trazer sérios problemas de segurança.

Alterações no software podem fazer com que ocorram falhas em partes que antes estavam estáveis ou novas falhas sejam introduzidas. Se alguma falha assim ocorre, é natural que o usuário acredite que o problema é do próprio software, e não resultado das alterações que foram feitas.

Uma alternativa às alterações no código é a contratação do desenvolvimento personalizado de uma empresa de desenvolvimento de software. Essa opção nem sempre é barata e, por questões de prazo e custo, essas empresas, muitas vezes, deixa de lado a análise de segurança de seus produtos, pois essa análise demanda tempo de desenvolvimento, e, conseqüentemente, um aumento no preço do projeto. Assim, as empresas que contratam esses serviços nem sempre sabem que esses produtos podem conter falhas de segurança.

4.3 O que torna os programas proprietários mais vulneráveis?

Como dito anteriormente, softwares proprietários tentem a ser mais vulneráveis pelo simples fato de, muitas vezes, possuírem maior representação no mercado. Portanto, em representação, ocorrem muito mais erros que em softwares livres.

Uma maior representação no mercado também leva mais usuários a explorarem suas falhas. Hackers, em geral, aproveitam para explorar sistemas onde um maior número de usuários será afetado. Quanto mais usuários utilizando o sistema em questão, mais dados serão obtidos com uma falha de segurança, maior disseminado o ataque será.

Softwares proprietários têm uma desvantagem quanto ao seu ciclo de correções. Geralmente, uma falha tem que ser comunicada à empresa responsável pelo software. Essa empresa deverá mobilizar recursos – sejam eles humanos ou financeiros – para que o desenvolvimento seja feito. A correção passará, então, por uma fase de testes e somente depois uma versão de correção ou uma atualização do software será disponibilizada para os usuários. Porém, os usuários não querem que a todo o momento sejam disponibilizadas novas correções, pois essas atualizações acarretam em maior processamento na máquina do usuário, maior trafego na rede e mais tempo gasto para utilizar a aplicação.

As empresas devem medir esse número de correções para equilibrar o número de atualizações. Por isso, muitas vezes as correções são disponibilizadas para o usuário separadas por nível crítico. Assim, se o usuário desejar, ele poderá efetuar a atualização somente para a correção de problemas críticos, deixando o restante para mais tarde.

5 SEGURANÇA NA INTERNET

Em um mundo cada vez mais interconectado, a diversidade de formas de interação vem aumentando continuamente. Este cenário dinâmico é perfeito para novas ferramentas frutos de boas idéias. O problema reside no fato de que quanto mais inovações se apresentam, mais preocupações devemos ter com todas as já conhecidas questões inerentes ao mundo virtual: produtividade, veracidade, privacidade, confidencialidade e muitos outros. Como sempre em destaque, não podemos esquecer de um tema em constante discussão: a segurança. Já são de conhecimento público as boas práticas de comportamento quando falamos de segurança no mundo virtual: não abrir e-mails suspeitos mesmo vindos de remetentes conhecidos, manter atualizados antivírus e *firewall*, etc. Realmente podemos sim, com relativa facilidade, seguir estes passos na tentativa de garantir uma convivência segura nos ambientes virtuais freqüentados, mas existem certas situações que são inesperadas até mesmo para os mais experientes usuários: as falhas de segurança dos *softwares*: existe uma diversidade imensa de formas de ataques maliciosos no mundo virtual e muitos deles tiram proveito do comportamento de usuários desavisados, mas talvez os mais desastrosos sejam aqueles que aproveitam fragilidades de *softwares*.

5.1 O combate aos softwares mal-intencionados

O combate às ameaças virtuais tem se tornado um mercado muito aquecido à medida que a Internet se populariza. A descentralização do conhecimento tem formado potenciais *crackers* nas faculdades e escolas técnicas, além dos que podem ser chamados de autodidatas nas “ciências virtuais”, contribuindo assim, como efeito colateral, para o aumento dos crimes digitais.

5.1.1 Ameaças Virtuais

Podemos definir algumas categorias de ameaças virtuais, tais como:

- Engenharia Social

Este termo é utilizado para descrever um método de ataque baseado no abuso da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para acesso não autorizado a dados privados.

Exemplos deste tipo de ataque são e-mails que supostamente são de um banco solicitando atualização de dados cadastrais, solicitações forjadas de instalação de ferramentas que prometem proteger ou melhorar o desempenho do computador, um desconhecido que liga para sua residência se passando por um técnico do seu provedor de acesso e solicita informações que permitem que ele tenha acesso à sua conta e muitas outras formas.

- Códigos Maliciosos (Malware)

Código malicioso ou *malware* (*Malicious Software*) é um termo que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Estas ameaças são representadas por vírus, *worms* e *bots*, *backdoors*, cavalos de tróia, *keyloggers* e outros programas *spyware*, *rootkits*, etc.

- Negação de Serviço (Denial of Service)

Nos ataques de negação de serviço (DoS - *Denial of Service*) o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

Este tipo de ataque geralmente gera uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo ou dá origem a um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível, tirando do ar importantes serviços de um provedor e impossibilitando o acesso dos usuários.

Nesse ataque os computadores não são invadidos mas seus serviços ficam inacessíveis por um período de tempo.

- O próprio uso da Internet

O simples ato de navegar pela Internet já coloca os usuários diante de muitos perigos. Os cuidados devem ser muitos e o usuário deve sempre criticar as informações apresentadas a ele antes de tomar ações como clicar em *links*, fazer *downloads* e executar programas direto do navegador.

Os recursos necessários para se navegar pela Internet podem ser facilmente utilizados para objetivos maliciosos. A configuração dos *browsers*, os *cookies* e programas Java, JavaScript e ActiveX dos *sites* e até mesmo as simples janelas *pop-ups* apresentadas podem fazer, por exemplo, com que o usuário seja direcionado para um *site* falso que utiliza engenharia social para obter acesso a dados privados. Cabe ao usuário se precaver e se educar para evitar problemas. Um bom início para quem quer começar a aprender sobre isso é a cartilha do Cert.br, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br) disponível no site http://cartilha.cert.br/.

- Vulnerabilidades de software

Talvez o problema de segurança mais esquecido pelos usuários sejam as vulnerabilidades de software. Muitos não se preocupam se os softwares adquiridos (sejam livres ou proprietários) garantem segurança durante sua utilização. É importante lembrar que todo software está sujeito a erros e por isso pode conter falhas que permitem quebras de segurança. Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede.

Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

5.1.2 Como se proteger

Para uma variada gama de perigos, tem surgido uma grande diversidade de promessas de proteção. Podemos destacar algumas delas:

- Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus e outras ameaças no computador. Um bom antivírus deve identificar e eliminar a maior quantidade possível de vírus e outros tipos de *malware*, analisar os arquivos que estão sendo obtidos pela Internet, verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e pen drives, de forma transparente ao usuário, procurar vírus, cavalos de tróia e outros tipos de *malware* em arquivos anexados aos e-mails e atualizar as assinaturas de vírus e *malwares* conhecidos, pela rede, de preferência diariamente.

Atualmente muitas outras funcionalidades estão sendo incluídas nos antivírus e existem boas opções gratuitas para uso residencial.

É primordial, no uso destas ferramentas, mantê-las em execução durante todo o tempo de uso do computador para permitir a verificação de todo e qualquer tipo de arquivo e também sempre atualizar seu banco de dados de registros de vírus.

- *Firewalls*

Um antivírus não é capaz de bloquear acessos não autorizados a um computador. Os *firewalls* têm justamente esta finalidade: constituídos pela combinação de *software* e *hardware*, são utilizados para dividir e controlar o acesso entre redes de computadores.

Se alguém ou algum programa suspeito tentar se conectar ao seu computador, um *firewall* bem configurado entra em ação para bloquear tentativas de invasão. Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de e-mail, cavalos de tróia e outros tipos de *malware* antes mesmo que os antivírus atuem.

- Atualização de *softwares*

Vários *softwares* disponibilizam eventualmente pacotes de atualização para corrigir os mais diversos problemas. Muitos destes problemas são relacionados a segurança, principalmente quando se trata de Sistemas Operacionais. Portanto, a melhor forma de evitar incidentes de segurança é sempre manter seu Sistema Operacional e seus aplicativos atualizados.

Além disso, existem *sites* como http://www.cert.org/, http://cve.mitre.org/ e http://www.us-cert.gov/cas/alerts/ que mantêm listas atualizadas de vulnerabilidades em softwares e sistemas operacionais.

5.2 Os problemas de vulnerabilidade

A dinâmica das técnicas e tecnologias virtuais é tão grande que podemos dizer que todo *software* desatualizado é vulnerável em algum nível (salvo pouquíssimas exceções). Cabe ao administrador ou usuário dos mesmos, o zelo pela sua correta manutenção e, mesmo que este processo seja feito de forma adequada, a invulnerabilidade não pode ser garantida.

Tanto softwares livres quanto proprietários estão igualmente sujeitos aos mesmos problemas. A diferença, como já foi discutido em seções anteriores, se dá em como e quando os erros e falhas são descobertos e corrigidos.

Existem acaloradas discussões sobre os Sistemas Operacionais mais vulneráveis e como sempre, as comparações entre Windows e Linux não poderiam deixar de constarem nas pautas.

Zelando pela imparcialidade nesta discussão que se renova a cada nova versão dos Sistemas, nos limitamos a dizer que nenhum software é isento de erros que podem torná-los vulneráveis a quebras de segurança. Em se tratando de Sistemas Operacionais, tais vulnerabilidades podem ser particularmente trágicas quando permitem que o sistema seja invadido e informações sejam roubadas ou recursos inutilizados. Quando falamos de servidores, o aspecto de segurança é especialmente importante e tem grande influência na decisão de qual sistema deve ser implementado.

Não raramente são veiculadas notícias de invasões a sistemas bancários, de *e-commerce* e outros serviços que utilizam a rede ou de roubo de informações privadas como números e senhas de cartões de crédito, documentos, etc. Tais situações poderiam ser evitadas ou pelo menos amenizadas se os devidos cuidados com as vulnerabilidades fossem tomados tanto no desenvolvimento dos softwares quanto na velocidade e qualidade do processo de reporte de erros e correção dos mesmos.

5.3 Ataques históricos

É interessante ver as conseqüências de sistemas críticos com vulnerabilidades em seu projeto. Dois crimes virtuais históricos foram a invasão de sistemas da NASA, nos EUA e do LHC, acelerador de partículas próximo a Genebra, na Suíça, usado para simular as partículas existentes durante o *Big Bang* e a criação do universo.

O caso envolvendo a NASA é tido como o primeiro ataque de um *cracker* ativista: um *worm* chamado WANK (sigla para "*Worms Against Nuclear Killers*", ou seja, "vermes contra os assassinos nucleares") fez aparecer um *banner* em todos os computadores do sistema em forma de protesto com o intuito de tentar impedir o lançamento da sonda Galileo a Júpiter utilizando plutônio como combustível. Até hoje não se sabe ao certo a origem do ataque mas muitos apontam para ativistas de Melbourne, na Austrália.

Já o caso do LHC foi mais preocupante pois mostrou falhas de segurança num sistema crítico que poderia causar desastres de proporções mundiais. Um grupo autodenominado “Equipe de Segurança Grega” invadiu um sistema do LHC durante uma experiência. Segundo os invasores, o intuito era provar a vulnerabilidade dos técnicos que estavam à frente daquela que foi considerada uma das maiores experiências do mundo.

Os responsáveis pelo projeto explicaram que a invasão teria sido realmente perigosa se o grupo de invasores tivesse tomado o controle de outras redes a partir das quais conseguiriam desligar partes do sistema. Apenas uma pequena parte foi afetada mas o incidente foi assustador para toda a comunidade que enviou mensagens e telefonemas para os cientistas demonstrando suas preocupações com as conseqüências da experiência e a falta de segurança.

6 CONCLUSÃO

O fato de o Software Livre permitir as quatro liberdades (execução, estudo do funcionamento, redistribuição de cópias e modificação e publicação de melhorias) promove a elevação do conhecimento, a autonomia tecnológica e a possibilidade de produtos diferenciados, que podem atender de forma superior as necessidades, sejam elas educacionais ou mercadológicas. O impacto de todos esses benefícios é visto pelo usuário final como diminuição de erros e aumento da segurança, aliado ao princípio do compartilhamento que educa e instiga toda a comunidade do Software Livre a contribuir entre si.

O Software Livre vem como alternativa para muitos programas hoje disponíveis e consegue substituir uma ampla variedade de aplicativos disponíveis hoje. Contudo, deve-se ressaltar o que isso trará de benefícios. Vimos que a questão da segurança é um fator relevante e ressaltado nas comunidades livre, porém os aspectos organizacionais de desenvolvimento de empresas privadas não podem ser desconsiderados. Além disso, a segurança passa não somente pelo software em si, mas pelos usuários. Por esse motivo, conhecer os aspectos da Engenharia Social é importante para usuários e programadores atualmente.

Softwares livres apresentam um ambiente mais propício para a correção de problemas de funcionamento e falhas de segurança. Essas características incluem o apoio da comunidade, que está sempre atenta a falhas que podem vir a ocorrer, possibilidade de o próprio usuário corrigir os problemas que encontrar, código aberto para facilitar a correção e descoberta de novos erros e troca de experiências de vários colaboradores espalhados pelo mundo e com vários níveis de experiência e conhecimento sobre áreas diversas.

Sempre em voga, a segurança dos *softwares* e na Internet é um tema que se renova constantemente e enfrenta desafios inéditos a cada novidade tecnológica. As boas práticas de comportamento e interação no mundo virtual são muito bem vindas na tentativa de manter uma relação saudável com as facilidades que a informática e a rede mundial oferecem. Um aspecto importante, mas muito negligenciado pela maioria dos usuários é que todo *software* possui erros e vulnerabilidades e, portanto, deve ser adequadamente mantido e atualizado, seja ele *software* livre ou proprietário.

7 REFERÊNCIAS BIBLIOGRÁFICAS

SARTINI, HUMBERTO. Conisli 2004. São Paulo, 2004. *Segurança com Software Livre.* Palestra disponível em: < http://www.hss.blog.br/arquivos/mslpr-seguranca.pdf>. Acesso em: 03 nov. 2010.

GUIMARÃES, GUILHERME. *O que é Software Livre.* 2008. Disponível em: <http://www.abril.com.br/noticia/tecnologia/no_99099.shtml>. Acesso em: 04 nov. 2010.

Software Livre: Uma Filosofia. 2008. Disponível em: <http://imasters.com.br/artigo/9968/livre/software_livre_uma_filosofia/>. Acesso em: 05 nov. 2010.

Software Livre e Open Source. Disponível em: <http://pt.opensuse.org/Software_livre_e_open_source>. Acesso em: 05 nov. 2010.

Cartilha de Segurança para Internet Versão 3.1. 2007. Disponível em <http://cartilha.cert.br/>. Acesso em: 04 nov. 2010.

Mistérios dos crimes na internet. 2008. Disponível em: <http://www.fraudes.org/clipread.asp?CdClip=7250>. Acesso em: 05 nov. 2010.

Maior acelerador do mundo sofreu ataque de “hackers” durante experiência. 2008. Disponível em: <http://blog.hsn-advogados.com.br/2008/09/12/maior-acelerador-do-mundo-sofreu-ataque-de-%E2%80%9Chackers%E2%80%9D-durante-experiencia/>. Acesso em: 05 nov. 2010.