LINUX: O SISTEMA OPERACIONAL DE CÓDIGO ABERTO E O SEU CONCEITO DE SEGURANÇA*

Lucas Borcard Cancela - UEMG/Unidade Carangola

Adriano Simioni Alvim – UEMG/Unidade Carangola

Flávio Aparecido de Almeida - UEMG/Unidade Carangola

Luciano Dias de Sousa - UEMG/Unidade Carangola

Patrícia Aparecida Romeiro Campos Cancela - UEMG/Unidade Carangola

RESUMO: O Software Livre (SL) tem crescido de forma acentuada nos últimos anos e são vários os motivos para que isto esteja acontecendo. Diversos dispositivos que utilizamos no cotidiano utilizam o SL sem mesmo que nós saibamos disto. É bem provável que, quando se fala em Software Livre, vem logo à mente a figura de um pinguim, representando o sistema operacional (SO) Linux. Desenvolvido pelo programador Linus Torvalds, o Departamento de Ciência da Computação da Universidade de Helsinki, na Finlândia, o sistema operacional Linux possui inúmeras vantagens, entre elas, a vantagem de ser de código aberto, possibilitando ao usuário o direito de estudar, modificar e distribuir o software para qualquer finalidade, de acordo com os termos da licença. Cada vez mais utilizado quando se pensa em segurança, o Linux conta com grande número de entusiastas, programadores voluntários e empresas colaboradoras. Destaca-se também sua utilização por usuários avançados, *hackers* e a aplicação deste SO em servidores. Neste artigo, com o apoio de uma metodologia de revisão bibliográfica, objetiva-se apresentar as características peculiares do sistema operacional Linux, seu histórico de criação e os aspectos de segurança existentes neste sistema.

PALAVRAS-CHAVE: Software Livre; Linux; Código aberto; Segurança.

1. Introdução

Por diversas vezes ouvimos críticas relacionadas ao Linux, rotulando este sistema operacional como “complexo” e “não funcional”. Por outro lado, também escutamos que o Linux é “gratuito” e que ele “não pega vírus”. No entanto, para tirarmos nossas próprias conclusões, é necessário estudar para conhecer as possibilidades que este sistema oferece aos seus usuários.

A idealização dos sistemas baseados no núcleo Linux vai além de um simples *kernel* de sistema operacional. Apesar de cada distribuição do Linux possuir características únicas contendo utilitários e ferramentas para inúmeros propósitos, é a ideologia de liberdade que chama atenção e atrai cada vez mais desenvolvedores, empresas e usuários finais.

O movimento do Software Livre nasceu em meio a turbulências causadas pelos abusos das organizações de softwares com políticas restritivas. Importante destacar que Livre reporta-se ao conceito de liberdade para estudar, executar, modificar e distribuir o software, não referindo-se diretamente ao preço. De acordo com Guedes e Silva (2005), o conceito de Software livre é oriundo de FreeSoftware, do Inglês, o que pode gerar muitas dúvidas, pois a palavra free

*XVI Encontro Virtual de Documentação em Software Livre e XIII Congresso Internacional de Linguagem e Tecnologia Online.

tanto pode ter o sentido de liberdade quanto de gratuidade. Porém, analisando o contexto histórico desde sua criação e seus objetivos, entende-se Software Livre relacionado à liberdade ou permissão dos utilizadores em alguns princípios como os apontados anteriormente de executar, copiar, distribuir, estudar, modificar e até mesmo melhorar o software.

De acordo com Torvalds e Diamond (2001):

> No caso de um sistema operacional, o código-fonte - as instruções de programação implícitas no sistema - é livre. Qualquer pessoa pode melhorá-lo, transformá-lo, explorá-lo. Porém, essas melhorias, transformações e explorações precisam ser disponibilizadas livremente. Pense Zen. O projeto não pertence a ninguém e pertence a todos. Ao abri-lo a todos, há um aperfeiçoamento rápido e contínuo. Com equipes de colaboradores trabalhando em paralelo, os resultados podem acontecer muito mais depressa e com muito mais sucesso do que se estivessem sendo conduzidos a portas fechadas. (Torvalds; Diamond, 2001, p. 261).

Tratando-se da distribuição dos softwares, destaca-se a existência da GPL – GNU Public License, documento que regula as maneiras a qual os softwares poderão ser distribuídos, estabelecendo que o programa poderá ser utilizado e alterado por qualquer usuário, contanto que as modificações realizadas resultem também na disponibilização dos códigos-fonte atrelado a referência do autor original.

No momento da escolha de um sistema operacional para ser implantado em uma empresa ou para fins pessoais, é indispensável que se leve em conta a segurança das informações que serão armazenadas nele. Ataques de invasores estão se tornando frequentes e causando prejuízos incomensuráveis para grandes organizações, pequenas empresas ou para o usuário comum. O objetivo central, neste artigo, será abordar as características de segurança presentes no sistema operacional GNU/Linux. Serão apresentados, a seguir, o histórico de desenvolvimento do sistema e a segurança que ele oferece.

2. Histórico de desenvolvimento

O Linux é um sistema operacional, programa responsável pelo funcionamento do computador, que faz a comunicação entre hardware (impressora, monitor, mouse, teclado) e software (aplicativos em geral), teve sua origem no Unix, um sistema operacional multitarefa e multiusuário que possui a vantagem de rodar em uma grande variedade de computadores.

O nome Linux foi batizado assim, pois é a união do nome de seu desenvolvedor, Linus Torvalds, com Unix, que também é um sistema operacional, porém, desenvolvido para servidores de grande porte.

Segundo Kernighan and Ritchie (1988):

> “a origem do Unix tem ligação com o sistema operacional Multics, projetado na década de 1960. Esse projeto era realizado pelo Massachusets Institute of Technology (MIT), pela General Eletric (GE) e pelos laboratórios Bell (Bell Labs) e American Telephone na Telegraph (AT&T). A intenção era de que o Multics tivesse características de tempo compartilhado (vários usuários

> compartilhando os recursos de um único computador), sendo assim, o sistema mais arrojado da época" (Kernighan; Ritchie, 2008 p 67).

Existe ainda o Minix, uma versão gratuita e com o código fonte disponível que permite que um programador com conhecimentos técnicos adequados possa fazer alterações em seu código. Criado inicialmente para uso educacional, como programa introdutório do sistema Unix. De acordo com o site Brasil Escola, essa versão do sistema foi escrita do "zero" e, por não ser uma versão do Unix, não possui nenhum código da AT&T, não podendo ser distribuído de forma gratuita.

O projeto de desenvolvimento do Linux iniciou-se em 1991, a partir da ideia do aluno finlandês do curso de Ciência da Computação da Universidade de Helsinki -Finlândia. Linus tinha o objetivo de criar um sistema operacional de código livre mais poderoso que o Minix.

Para tanto, ele remeteu uma mensagem a uma comunidade pela Usenet (uma espécie de precursor da Internet). Ainda em 1991, foi disponibilizada a versão do kernel (núcleo dos sistemas operacionais) 0.02. O pesquisador continuou trabalhando até que em 1994 apresentou a versão 1.0. Quando desenvolveu o Linux, seu propósito era fazer um sistema sem fins lucrativos para seu uso pessoal, que atendesse suas necessidades. No desenvolvimento do projeto, Linus coordena um grupo de pesquisadores que implantou melhorias no sistema criado. Esse empreendimento coletivo teve como finalidade contribuir gratuitamente para a construção de um sistema operacional melhor.

O Linux é um sistema de código livre que está sob a licença GPL, a qual permite que qualquer usuário possa utilizar os programas disponibilizados, com o compromisso de não os tornar fechados e comercializados. Qualquer parte pode ser alterada, e até comercializada, mas não se pode fechá-la, isto é, proibir que outros usuários a modifiquem ou a vendam.

Para a melhor compreensão do sistema Linux é necessário saber o que é GNU. GNU é um projeto iniciado em 1984 com a finalidade de produzir um SO compatível com os sistemas de padrão Unix. O Linux por si só é núcleo do sistema operacional chamado kernel. Linus para desenvolver seu sistema utilizou de ferramentas da GNU, deixando seu kernel dentro da mesma licença.

Embora, o kernel seja a parte mais importante, pois é o núcleo e serve de comunicador entre o usuário e o computador, o kernel por si só, não é aplicável. Esse é o fato de Linus ter optado pelo uso de variantes dos sistemas GNU junto com o kernel e desta fusão o Linux se tornou um sistema operacional.

Em se tratando ainda do conceito de Linux, salienta-se que este é tão somente o Kernel ou núcleo do SO, capaz de oferecer diferentes serviços (apesar de os usuários tratarem o Linux como um sistema operacional completo).

Desde o seu surgimento, surgiram várias distribuições do Linux, segundo Guedes e Silva (2005):

> [...] algumas empresas e organizações decidiram juntar o kernel a vários programas escritos para o Linux em pacotes chamados distribuições. Como o Linux e suas aplicações são desenvolvidos em diversos locais, algumas empresas focaram suas atividades na compilação, teste, desenvolvimento de softwares e suporte, assim como milhares de aplicativos que implementassem melhorias. Dessa forma surgiram distribuições ao redor do mundo, cada uma mantendo um segmento de atuação e um mercado específico. Dentre as principais podemos citar: Slackware, Debian, Fedora, S.U.S.E.,

> Mandriva etc. (Guedes; Silva, 2005, p 8).

3. Segurança do Sistema operacional Linux

> Os sistemas Linux são mais estáveis, pois conseguem gerenciar de maneira mais eficiente os recursos de hardware. Isso permite que até máquinas mais antigas possam rodar versões mais novas das distribuições. Além disso, são mais seguros, pois o número de pragas virtuais para sistemas Linux ainda é muito reduzido, além de que códigos que modifiquem qualquer parte do sistema sempre são interceptados com a autenticação obrigatória o superusuário (root). Esse recurso inclusive começou a ser incorporado de maneira similar a partir do Windows Vista na família Windows, através do Controle de Conta de Usuário. (Sanchez, Campomori, Rocca e Lemes, 2011).

Ocorre que muitos usuários não entendem que o sistema Linux também possui vulnerabilidades e que alguém pode aproveitar dessas brechas para ataca-lo.

> "Um engano de muitos usuários do Linux é o de considerar que sua máquina não é suficiente importante para ser alvo de hackers. Eles pensam 'Não tenho nada importante em minha máquina; quem poderia querer violá-la'" (Lee, Hatche e Kurtz, p. 4, 2001).

No entanto, em se tratando de segurança de sistemas operacionais, o Linux é sempre apontado como um dos sistemas mais seguros disponíveis, um bom exemplo é a versão SELinux (Security-Enhanced Linux), considerado o melhor e mais eficiente sistema de controle de acesso obrigatório usado nos sistemas operacionais GNU/Linux, projetado e desenvolvido pela Agência de Segurança Nacional dos EUA com uma importante contribuição da NSA. O SELinux se baseia em vários anos de desenvolvimento científico na área de segurança de sistemas de TI. O sistema possui uma base teórica profunda e provou ser altamente efetivo, na prática, aplicado em sistemas militares especializados.

Devida a sua complexidade, é considerado impenetrável pelo ponto de vista da segurança de TI. Porém, a utilização de um sistema desse porte não é adequado para empresas ou redes domésticas, só se justifica a implementação de um sistema operacional dessa magnitude se a natureza dos dados armazenados e processados requererem confiabilidade e proteção excepcionais.

3.1 Características de Segurança do Sistema Linux

Ao se tratar das versões mais populares do Linux, podemos citar algumas características do sistema que o tornam menos vulnerável a ameaças. Segundo Renan Cavalieri (2016), por padrão, os usuários de GNU/Linux não possuem direitos de administrador e não podem modificar os arquivos do sistema, tornando os ataques de vírus menos frequentes. Por ser um Software Livre, permite que diversos peritos em segurança possam examinar o código fonte, detectar as vulnerabilidades ou falhas com maior facilidade e depois disponibilizar atualizações para saná-las com sucesso.

O sistema, ainda, obriga o usuário a declarar se o arquivo é executável ou não. Outro fator determinante é a variedade de distribuições existentes e totalmente diferentes do sistema Linux. Tornando-o mais seguro contra ataques de vírus que

possam explorar as fragilidades da plataforma. Caso um usuário seja infectado, seu diretório será corrompido, exceto que o utilizador tenha executado em modo Administrador (Root), o que requer autenticação, mudança de login, e outras formas diversas de bloqueios.

Ainda que o sistema Linux seja menos vulnerável a ataques se comparado a outros sistemas operacionais, é importante lembrar que nenhum sistema é livre de ameaças e falhas. Dessa forma, não seria o Linux exceção dessa regra: ameaças externas ao sistema sempre irão existir. Entretanto, os riscos que um usuário Linux sofre são diferentes comparados a outros sistemas não Unix.

Apesar de grande esforço para detectar ameaças, a maior parte dos vírus para Linux é desconhecida e, geralmente, são softwares desenvolvidos com uma única finalidade. Segue abaixo algumas ameaças já detectadas no sistema:

- O vírus Staog, o qual se aproveitava das vulnerabilidades do sistema;
- Ramen worm que atacava os sistemas Red Hat Linux;
- OSF.8759 que ataca os binários ELF do sistema;
- Backdoor o qual sonda a porta 3049 através do protocolo UDP e envia comandos internos para executar arquivos no sistema.
- L10n worm e Bliss também fizeram parte do histórico de vírus populares para Linux.

É essencial que o usuário Linux esteja sempre informado e atento às notícias sobre falhas ou vulnerabilidades presentes no Kernel e elementos do sistema, pois as frequentes atualizações, descobertas ou correções de falhas disponibilizadas não serão eficazes caso o usuário não dê a devida atenção, mantendo no mínimo seu sistema atualizado. É imprescindível utilizar um sistema considerado seguro, porém os cuidados com a proteção não podem ser ignorados.

4. Considerações Finais

Esta abordagem voltada para segurança do sistema Linux possibilita a abertura de oportunidade para se refletir sobre a importância de o usuário ser familiarizado com o sistema operacional escolhido: Linux. Nesse sentido, é de notória relevância salientar as características do sistema e como serão desenvolvidas estratégias para que com competência se possa prevenir de possíveis ataques.

Através deste trabalho observa-se que, muito mais do que por questões financeiras, organizações tem utilizado código aberto também por questões relacionadas à flexibilidade, estabilidade e segurança. Por meio da revisão bibliográfica entende-se que, por intermédio da ótica de entusiastas e estudiosos, o Software Livre condiz com a filosofia orientada ao desenvolvimento tecnológico através de um trabalho de desenvolvimento científico colaborativo.

Referências:

ATCH, B.; LEE, J.; KURTZ, G. **Hackers Expostos - Linux**, São Paulo, Makron Books, 2002.

GUEDES, R. M.; SILVA, E. M. **Introdução ao uso do Linux.** (2005) Disponível em: http://www.lee.eng.uerj.br/. Acesso em: 28 de Set. de 2019.

KERNIGHAN, B. W. and RITCHIE, D. M. **C Programming Language**. Prentice Hall, Englewood Cliffs, USA, 1988.

KROPIWIEC, D. D; GEUS, P. L. **Paradigmas de Segurança em Sistemas Operacionais**. UNICAMP, 2015.

SANCHEZ, Á; CAMPOMORI, C; ROCCa, J. M; LEMES, P. A. **Sistema Operacional Linux**, Guaratinguetá, 2011.

SANTOS, A. L. dos. **Construção de conhecimento em rede: a inteligência coletiva na comunidade Linux do Brasil**, 2016.

TORVALDS, L.; DIAMOND, D. **S*ó por prazer*: Linux, os bastidores da sua criação.** Rio de Janeiro: Campus, 2001.