XIV INIC Encontro Latino Americano de Iniciação Científica
X EPG Encontro Latino Americano de Pós Graduação
IV INIC Jr Encontro Latino Americano de Iniciação Científica Júnior

SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: um estudo comparativo sobre os programas de antivírus e sistemas de *firewall*

Mônica Gonçalves de Mendonça, Edson Aparecida de Araújo Querido Oliveira, Vilma da Silva Santos, Paulo Cesar Ribeiro Quintairos

Universidade de Taubaté – UNITAU, Programa de Pós-graduação em Gestão e Desenvolvimento Regional– Rua Visconde do Rio Branco, 210. Centro – 12020-040 – Taubaté – SP – Brasil. monica@ita.br; edson@unitau.br; vilma70@gmail.com; quintairos@gmail.com.

Resumo- A popularização do acesso à internet e aos computadores pessoais acarretou rápido crescimento das ameaças à segurança de sistemas de computadores. O crescimento em número e diversidade dos vírus se tornou, nos últimos anos, uma grande preocupação para os administradores de sistemas de informação. Essas crescentes ameaças fomentam o mercado de produtos de segurança, especialmente os de firewall e dos programas de antivírus. Atualmente há uma ampla variedade desses produtos disponíveis no mercado, com grande variedade de preços, funções e qualidade. Neste trabalho serão apresentados os resultados de uma pesquisa exploratória e descritiva, realizada a partir de um levantamento bibliográfico e documental, sobre os produtos disponíveis no mercado varejista brasileiro de segurança de informação. O objetivo desta pesquisa é construir um quadro comparativo dos produtos analisados, a partir de documentos de acesso público. Os resultados apresentados indicam que a variedade de produtos é devida às diferentes necessidades dos clientes potenciais, sendo esses fatores desconsiderados por significativo número de usuários desses sistemas de segurança.

Palavras-chave: Segurança em Sistemas de Informação. Antivírus. *Firewall*.
Área do Conhecimento: Ciências Sociais Aplicadas.

Introdução

Os computadores estão cada vez mais presentes na vida das pessoas, facilitando a execução de tarefas e permitindo armazenamento e tratamento de informações, as quais devem estar disponíveis, íntegras e confidenciais sempre que o usuário delas necessitar (SÊMOLA, 2003).

Entretanto, em virtude da interligação dos computadores em redes como a *Internet*, a integridade e o sigilo das informações armazenadas localmente nos computadores são cada vez mais vulneráveis a ameaças virtuais. Atualmente os chamados vírus de computador podem comprometer a integridade e a privacidade das informações armazenadas em computadores. Uma solução para se evitar ou amenizar o comprometimento dos dados armazenados é a utilização dos Softwares Antivírus.

Neste artigo serão apresentados os resultados de uma pesquisa comparativa entre os principais antivírus disponíveis no mercado brasileiro, visando possibilitar a escolha do produto mais adequado, as diferentes condições de utilização e orçamento disponíveis**.**

Metodologia

O presente trabalho de pesquisa tem caráter descritivo-exploratório. Trata-se de uma pesquisa bibliográfica e documental, tendo sido desenvolvido a partir da análise qualitativa de dados obtidos em documentos de acesso público.

Resultados

Segundo Cidale (1990), os vírus de computador são pequenos segmentos de códigos, desenvolvidos por programadores, com o objetivo de provocar comportamentos indesejáveis nos computadores infectados.

Ainda segundo o autor supracitado, o código do vírus funciona como uma função de programa que se apodera de áreas importantes de comando do sistema. A partir disso, o vírus pode transferir réplicas de seus códigos a outros arquivos já presentes na memória ativa e a arquivos que estejam armazenados nos discos rígidos e disquetes, além de áreas de controle destes meios contaminando-os.

Com a capacidade de multiplicação pela contaminação através de arquivos transmitidos por disquetes, CDs entre usuários e também pela facilidade de quebrar fronteiras através dos e-mails, tem a similaridade e comparação com os vírus biológicos que infectam por auto-reprodução, diversos órgãos do corpo humano.

Segundo *Fred Cohen (1995 apud Santos e Barros 2005)* descrevendo sobre a evolução histórica dos vírus de computador, relata que os primeiros vírus que estão registrados desde meados de 1983 são: *Brain, Lehigh, Jerusalem, MacMag, Den Zuk* e muitas de suas variantes.

Os vírus podem ser categorizados em:

- Multipartite, quando infectam programas e arquivos;
- Polimóficos, quando tem alto poder de reprodução em diferentes cópias;
- Criptografados, quando utilizam chaves criptográficas para disfarce;
- Macros são aqueles que infectam documentos que contém macros como Word e Excel;
- Furtivos podem ser de arquivos ou de boot e são de difícil detecção;
- Auto spam são vírus de macro que enviam e-mails com arquivos infectados.

Para Symantec (2006) um computador para ser infectado por um vírus, é preciso que um programa previamente infectado seja executado, podendo ocorrer de diversas maneiras, tais como:

- Abrir arquivos anexados aos e-mails;
- Abrir arquivos do Word, Excel;
- Abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- Instalar programas de procedência duvidosa ou desconhecida, obtidos pela *Internet*, de disquetes, pen drivers, CDs, DVDs etc;
- Ter alguma mídia removível que esteja infectada conectada ou inserida no computador, quando ligado.

Segundo a empresa Symantec Vulnerabilidades são falhas no software de computador que criam deficiências na segurança geral do computador ou da rede. As vulnerabilidades também podem ser criadas por configurações incorretas do computador ou de segurança. As ameaças exploram as vulnerabilidades, o que resulta em possíveis danos para o computador ou dados pessoais (SYMANTEC, 2006).

De acordo com a empresa Microsoft (2009), Mesmo para uma pessoa experiente, remover um vírus corretamente de um computador é, muitas vezes, uma tarefa intimidante quando não há ajuda das ferramentas específicas desenvolvidas para isso. Alguns vírus e outros softwares indesejados foram desenvolvidos para se reinstalarem depois de serem detectados e removidos! Felizmente existem ferramentas que podem remover permanentemente estes softwares indesejados, são os antivírus.

Os programas do tipo antivírus **s**ão programas que procuram detectar e, então, anular ou remover os vírus de computador (CERT, 2007). Os antivírus possuem uma base de dados contendo as assinaturas dos vírus de que podem eliminar. Desta forma, somente após a atualização de seu banco de dados, os vírus recém-descobertos podem ser detectados.

Ainda de acordo com Symantec (2006), novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover diversos tipos de código malicioso, barrando programas hostis e verificando e-mails.

Um bom antivírus deve: analisar e eliminar todos os vírus conhecidos além de outros tipos de *malware*, analisar em tempo real os arquivos que estão sendo obtidos pela *Internet*, verificação agendada de discos rígidos, ou *Hard Drives (HDs)*, e contínua de disquetes e unidades removíveis, como CDs, DVDs e *pen drives*, de forma transparente ao usuário, verificação de e-mails e anexos, atualizar as assinaturas de vírus e malwares conhecidos, pela rede, diariamente.

Quanto ao funcionamento, Cidale (1990) relata que os programas de antivírus agem, principalmente de 4 formas diferentes, para conseguir detectar o máximo de vírus possível.

- Escaneamento de vírus conhecidos - Quando um novo vírus é descoberto seu código é desmontado e é separado um grupo de caracteres (uma string) que não é encontrada em outros softwares não maliciosos. Tal string passa a identificar esse vírus, e o antivírus a utiliza para ler cada arquivo do sistema (da mesma forma que o sistema operacional), de forma que quando encontrá-la em algum arquivo, emite uma mensagem ao usuário ou deleta o arquivo automaticamente.
- Sensoreamento heurístico - O segundo passo é a análise do código de cada programa em execução quando usuário solicita um escaneamento. Cada programa é varrido em busca de instruções que não são executadas por programas usuais, como a modificação de arquivos executáveis. É método complexo e sujeito a erros, pois algumas vezes um executável precisa gravar sobre ele mesmo, ou sobre outro arquivo, dentro de um processo de reconfiguração, ou atualização, por exemplo. Portanto, nem sempre o aviso de detecção é confiável.
- Busca Algorítmica - Expressamente, a busca algorítmica é aquela que utiliza algoritmos para selecionar os resultados. Essa classificação em "Busca Algorítmica", do Inglês "*algorithmic search*", é de caráter

publicitário ou vulgo já que qualquer mecanismo de busca utiliza um algoritmo. Esta denominação foi criada para se diferenciar das "Buscas Patrocinadas" em que o pagamento (patrocínio) dos mecanismos de busca faz com que os resultados patrocinados tenham prioridade. Por exemplo: para buscar strings (cadeias de texto) que detectariam um vírus de computador

- Checagem de Integridade - Checagem de integridade cria um banco de dados, com o registro dos dígitos verificadores de cada arquivo existente no disco, para comparações posteriores. Quando for novamente feita esta checagem, o banco-de-dados é usado para certificar que nenhuma alteração seja encontrada nesses dígitos verificadores. Caso seja encontrado algum desses dígitos diferentes dos gravados anteriormente, é dado o alarme da possível existência de um arquivo contaminado.

Os programas do tipo antivírus podem ser divididos em três grandes categorias: pagos, gratuitos e *online.*

* Pagos: É preciso comprar a licença para utilizar o software;

* Gratuitos: Pode ser instalado e utilizado sem restrição;

* Online: Pode ser pago ou gratuito. Ele não precisa ser instalado, mas é necessário estar conectado a internet. É uma nova tendência, aproveitando a computação nas nuvens.

Comparando os antivírus pagos e gratuitos, eles são equivalentes em alguns testes de detecção de vírus. Já o Online está sendo utilizado cada vez mais, mas não deve ser o substituto dos anteriores, pode ser utilizado como uma segurança adicional.

Segundo fonte da revista INFO (2010) os principais antivírus grátis do mercado ganharam, nos últimos meses, importantes atualizações. Elas resultaram em várias mudanças nos sistemas de varredura contra vírus e no recurso de proteção em tempo real desses programas.

Testes feitos pelo INFOLAB demonstraram que o *Avast* 5 *Free* leva o primeiro lugar, não em razão do desempenho, mas sim pelos recursos oferecidos, o AVG 9 *Free* antivírus divide o primeiro lugar com o *AVAST* pelo bom desempenho, O *BitDefender Free* Antivirus 2010 oferece proteção básica contra vírus tendo ainda varredura programada e customização de interface. Também tem um eficiente sistema de quarentena.

Já o *Avira AntiVir Free* 2010, apesar de intuitiva e simples de usar, a interface do *Avira* precisa evoluir, este é principal ponto negativo da atual versão, porém em contrapartida é um dos poucos softwares de segurança do mercado preparado especificamente para rodar em *notebooks*. Dentre os principais fabricantes podemos destacar a *Mcafee* e *Symantec*.

No mercado brasileiro, as soluções de segurança no ambiente corporativo são as que mais crescem atualmente dentro do segmento de software, alcançando um crescimento em torno de 13% no Brasil durante o primeiro semestre, segundo estudo da IDC. O resultado revela que os efeitos da instabilidade econômica mundial não afetaram o mercado nesse período e só devem se tornar evidentes no último trimestre do ano.

Apesar do cenário positivo, a proporção de investimentos em segurança no Brasil, no entanto, ainda é pequena em relação à média mundial.

Um dos motivos é a falta de consciência quanto aos riscos existentes, especialmente por parte das pequenas e médias empresas (TI Inside 2008).

Atualmente, as soluções para *security content and threat management*, ou seja, proteção contra vírus, spyware, spam, hackers, invasões representaram 70% do mercado brasileiro de software no primeiro semestre. (Modulo 2008).

Segundo pesquisa da *ComputerWorld* (2009) 30% das pequenas e médias empresas (PMEs) brasileiras não usam antivírus; 47% delas não contam com ferramentas de segurança na máquina dos seus usuários, isto se deve a falta de produtos adequados ás suas necessidades, pequena capacidade de investimento e desinformação.

FABRICANTE / NOME PRODUTO	CARACTERÍSTICAS		
AVIRA AVIRA ANTIVIR	Avira antivir personal free	Avira Antivir Premium R$46,00	Avira Antivir Professional R$84,00
ALWIL SOFTWARE AVAST	Avast Free	Avast Pro Antivírus R$69,00	Avast Internet Security R$89,00
GRISOFT AVG	AVG Free	AVG Antivírus 9 Comercial R$72,00	AVG Internet Security R$108,00
MCAFEE MCAFEE	Mcafee Antivírus Plus R$89,00	Mcafee Total Protection R$108,00	Mcafee Internet Security R$95,00
SYMANTEC NORTON	Norton Antivírus Premier R$79,00	Norton Antivírus Corporate Edition R$169,00	Norton Antivírus Internet Secutiry R$249,00

Quadro 1 – Produtos disponíveis no mercado brasileiro. Fonte: Empresas desenvolvedoras

Considerações Finais

Atualmente os vírus se alastram rapidamente, especialmente devido à popularização do acesso aos computadores e à Internet. Os programas nocivos à segurança e ao bom funcionamento dos sistemas se aproveitam das falhas de segurança dos programas e das vulnerabilidades existentes nos sistemas para conseguirem se propagar. O uso de metodologias como teste de softwares, pesquisas em empresas desenvolvedoras e um levantamento das necessidades, é fundamental para organizar informações esclarecendo o usuário a importância dos softwares antivírus e as tecnologias aplicadas a eles. Estas medidas forçam as empresas desenvolvedoras de antivírus a criarem novos mecanismos com o objetivo de barrar provenientes ataques.

Os resultados apresentados neste trabalho apontam que de fato não existe um único método de detecção para todos os casos. Os programas do tipo antivírus necessitam estar sempre atualizando de forma dinâmica seus métodos de varredura, bem como sua base de dados, de modo que possam assim identificar os novos vírus que surgem a cada dia.

A escolha de um bom software de antivírus é essencial, entretanto, não devemos confiar plenamente em um único produto podendo-se encontrar no mercado soluções antivírus que utilizam os mecanismos de varredura e bases de dados de mais de um fornecedor. Entretanto, a maneira mais eficaz de evitar a infecção por vírus é a conscientização do usuário.

Referências

- AVAST. Pesquisa no sítio da Alwill. Disponível em: <http://avast.com/pt-br/free-antivirus/>. Acesso em Agosto 2010.

- AVG – GRISOFT. Pesquisa no sítio da Grisoft. Disponível em: <http://avgbrasil.com.br.>. Acesso em Agosto 2010.

- AVIRA. Pesquisa no sítio da Avira. Disponível em <http://avira.com.br.>. Acesso em Agosto 2010.

- CIDALE, R. A. Vírus digital. Uma abordagem para prevenção e manutenção de seus sistemas de informação. São Paulo. Makron McGraw-Hill, 1990.

- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para Internet. Disponível em <http://cartilha.cert.br/download/cartilha-02-prevenção.pdf.> Acesso em: Agosto, 2010.

- INFOExame – Revista Infoexame. Disponível em <http://info.abril.com.br/aberto/infonews/.>. Acesso em Agosto 2010.

- MCAFEE – Mcafee. Disponível em <http://br.mcafee.com/>. Acesso em: Agosto, 2010.

- NORTON ANTIVIRUS – Symantec. Disponível em <http://symantec.com.br>.Acesso em Agosto 2010.

- TIINSIDE. Disponível em: <http://tiinside.com.br.> Acesso em Agosto 2010.

-MICROSOFT. Pesquisa no sítio da Microsoft. Disponível em: <www.microsoft.com/brasil/security/virus>. Acesso em Agosto 2010.

-SANTOS A. P. G.; BARROS, O. H. B. O Funcionamento Interno dos Softwares Antivírus. Instituto de Estudos Superiores da Amazônia, 2005. Disponível em <http://www3.iesam-pa.edu.br/ojs/index.php/computacao/article/viewArticle/>. Acesso em Agosto 2010.

- SÊMOLA, M. Gestão da Segurança da Informação - Uma visão executiva. Rio de Janeiro: Elsevier, 2003.