ESTUDO DOS POSSÍVEIS MOTIVOS DO AUMENTO DE INCIDENTES DE *MALWARES* NAS EMPRESAS

STUDY OF POSSIBLE REASONS FOR INCREASES IN INCIDENTS WITH *MALWARE* ON BUSINESS

ESTUDIO DE POSIBLES MOTIVOS DEL AUMENTO DE INCIDENTES DE *MALWARES* EN LAS EMPRESAS

FELIPE CÉSAR DAMATTO[1]
RICARDO RALL[2]

Recebido em novembro de 2010. Aceito em março de 2011.

[1] Graduando em Tecnologia em Informática para Gestão de Negócios pela Faculdade de Tecnologia de Botucatu.
[2] Professor Doutor da Faculdade de Tecnologia de Botucatu.

ESTUDO DOS POSSÍVEIS MOTIVOS DO AUMENTO DE INCIDENTES DE *MALWARES* NAS EMPRESAS

RESUMO

A informação tem um papel fundamental dentro das empresas, pois, baseadas nessas informações, decisões importantes são tomadas. Para se ter um controle sobre as informações, as empresas recorrem a sistemas de informação. A tecnologia da informação auxilia os sistemas facilitando, por exemplo, o armazenamento, acesso e envio das informações. Porém, existem problemas como os *malwares*, que são programas mal intencionados e que podem causar perdas e alterações nas informações, além da queda de desempenho do sistema. Atualmente, vem aumentando o número de problemas devido à incidência de *malwares*. Neste trabalho, foi realizada uma pesquisa em livros, artigos, reportagens sobre as empresas que utilizam tecnologia da informação. Também foram levantadas informações sobre *malwares* que estão em evidência atualmente e os possíveis motivos para o aumento no número dessas ocorrências, mostrando a importância da segurança da informação nas empresas e da sua prevenção.

PALAVRAS-CHAVE: Incidentes. *Malware.* Segurança da informação.

STUDY OF POSSIBLE REASONS FOR INCREASES IN INCIDENTS WITH *MALWARE* ON BUSINESS

ABSTRACT

Information has a role crucial in business because based on this information important decisions are taken. Companies are using information systems to have control over the information. Information technology helps systems facilitating, for example, storage, access and transmission of information. However there is a problem in information technology, the *malware*, which are malicious programs that can cause losses and alterations on information and also decrease the system performance. Currently it has increased the number of problems due to the incidence of *malware*. In this work it was conducted a survey based on books, articles and reports of companies that use information technology. It was also raised information about *malware* that are in evidence nowadays and the possible reasons for the increases in the number of these occurrences showing the importance of information security in companies and their prevention.

KEYWORDS: Incident. Information security. Malware.

ESTUDIO DE POSIBLES MOTIVOS DEL AUMENTO DE INCIDENTES DE *MALWARES* EN LAS EMPRESAS

RESUMEN

La información tiene un papel fundamental dentro de las empresas, pues basadas en esas informaciones, decisiones importantes son tomadas. Para tenerse un control sobre las informaciones, las empresas recurren a sistemas de información. La tecnología de la información auxilia los sistemas facilitando, por ejemplo, el almacenamiento, acceso y envío de las informaciones. Sin embargo, existen problemas como los *malwares*, que son programas mal intencionados y que pueden causar pérdidas y alteraciones en las informaciones, además de la queda de desempeño del sistema. Actualmente, viene aumentando el número de problemas debido a la incidencia de *malwares*. En este trabajo, fue realizada una pesquisa en libros, artículos, reportajes sobre las empresas que utilizan tecnología de la información. También fueron levantadas informaciones sobre *malwares* que están en evidencia actualmente y los posibles motivos para el aumento en el número de esas ocurrencias, mostrando la importancia de la seguridad de la información en las empresas y de su prevención.

PALABRAS-CLAVE: Incidentes. *Malware.* Seguridad de la información.

1 INTRODUÇÃO

Com o desenvolvimento e implantação dos sistemas de informação, as ferramentas da tecnologia da informação passaram a auxiliar as organizações, os profissionais, os usuários e a sociedade na aquisição, manipulação e comunicação das informações. Com isso, os sistemas de informação se tornam importantes estruturas organizacionais, auxiliando no gerenciamento e classificação das informações, úteis nas tomadas de decisão do negócio. Entretanto, atualmente, é fácil se atacar sistemas informatizados, pois estes estão conectados por meio das redes (BURGO; TAMAE, 2006).

As informações têm um papel muito importante no cenário empresarial, pois são com base nessas informações que são tomadas muitas decisões. Pelo seu valor, as informações devem ser armazenadas de forma que se tenha acesso fácil, mas organizado e seguro. A tecnologia da informação auxilia o sistema de informação quanto à comunicação, armazenamento e segurança das informações.

A tecnologia da informação é muito usada devido às facilidades e benefícios que ela proporciona às empresas. Porém, há pontos negativos, como a existência de *malwares*, que são softwares maliciosos que causam vários tipos de danos ao computador.

No cenário atual, empresas, organizações, governos e até mesmo usuários em suas próprias casas vêm tendo problemas com *malwares*. Esses vírus virtuais causam muitos problemas e transtornos em empresas, como perda ou alterações das informações, queda de desempenho das máquinas ou sistemas, roubo de senhas e acesso de pessoas não autorizadas. Esses problemas podem proporcionar prejuízos financeiros, perda de tempo e, dependendo do ramo da empresa, esta pode até perder credibilidade.

Para que um computador seja infectado, é preciso que um programa infectado seja executado através de outro computador contaminado na rede, por meio de *pendrive*, disquete, etc.

Foi estudado o cenário atual sobre o uso de tecnologia da informação nas empresas e também as ameaças que o *malware* representa. Com os resultados obtidos, as empresas podem se prevenir e agir para combater essas ameaças, evitando problemas.

2 REVISÃO DE LITERATURA

2.1 Definição

Malware é um programa cuja intenção é sua instalação no computador de outro usuário sem o seu conhecimento ou sua permissão e destina-se a causar algum tipo de dano (MANSON, 1999).

Os vírus são grandes preocupações para empresas, organizações governamentais, militares, corporações e pessoas físicas que estão ao alcance dessas ameaças. Mesmo com os avanços tecnológicos, os sistemas e os dados armazenados ainda não estão seguros. As tecnologias criadas pelos *malwares* geralmente são altamente eficientes, podendo provocar uma epidemia global em poucas horas (KARISNTON; MAZZOLA, 2002).

Segundo Gaspar (2007), softwares maliciosos, também conhecidos como *malwares*, são programados especificamente para executar ações danosas no computador.

Para Fuentes (2008), *malware* é um termo geral designado a qualquer software malicioso que prejudique o computador. Dependendo da eficiência, o *malware* pode danificar uma infraestrutura de rede interna, nacional e até mesmo redes corporativas.

2.2 Tipos

Os *malwares* podem ser divididos em várias categorias, como a ocultação (cavalo de tróia), *malware* infectante (vírus e *worms*) e *malware* para tirar proveito (*Spyware* e *adware*).

Também é importante ressaltar a definição de carga, que é uma ação que é executada quando o *malware* alcança a máquina hospedeira. A carga pode ocasionar várias ações, como criar porta dos fundos (*back door*), alteração e exclusão de dados e negação de serviços.

- Vírus: é um código desenvolvido com a intenção de replicação. O vírus tenta se espalhar de um computador para outro, por meio de um programa hospedeiro. O vírus pode causar danos no *hardware*, nos *softwares* ou nos dados. Quando o *software* do hospedeiro é executado, o vírus também entra em execução, fazendo com que infecte outros hospedeiros e, às vezes, entregando carga adicional.

- Verme (*Worms*): é um código mal intencionado autopropagável de um computador para outro, por meio da rede. A ação nociva pode ocorrer pelo consumo de recursos da rede ou do sistema local, podendo causar um ataque de negação de serviço. Alguns vermes podem ser executados, espalhando-se sem que o usuário perceba, enquanto outros precisam que o usuário execute o verme, para que este se espalhe. Além de se replicar, o verme pode entregar uma carga.

- Cavalo de Tróia: É um programa que parece ser útil ou inofensivo, porém tem códigos ocultos criados para explorar ou

danificar o sistema no qual foi executado. Geralmente os cavalos de tróia chegam através de mensagens de *e-mail*. Um cavalo de tróia pode interromper o trabalho do usuário, operações normais do sistema, podem abrir uma porta dos fundos no sistema para que um hacker invada o sistema, roube dados ou altere configurações.

- *Spyware*: também conhecido como *spybot* ou *software* de rastreamento. O *spyware* executa algumas atividades no computador sem obter a autorização do usuário, como a obtenção de informações pessoais, modificação das definições do navegador de internet, degradação do desempenho do computador e invasão de privacidade.
- *Adware*: é um tipo de programa que exibe anúncios e o seu objetivo é fornecer anúncios em massa de uma maneira ou em um contexto que possa ser inesperado ou indesejado por parte dos usuários. Muitos aplicativos *adware* também têm a função de rastreamento. Alguns clientes podem querer remover o *adware* por desaprovarem o rastreamento ou pelos efeitos causados no desempenho do sistema (MICROSOFT TECHNET, 2006).

2.3 Empresas informatizadas

Segundo o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), na pesquisa Tecnologia de Informação e Comunicação (TIC) Empresas, realizada no ano 2007, mais de 95% das empresas pequenas, médias e grandes do Brasil estão informatizadas e, dentre elas, 97% tem acesso à internet.

A pesquisa foi realizada entre outubro e novembro de 2007, com 2,3 mil empresas com mais 10 funcionários ou mais listadas na fonte Relação Anual de Informações Sociais (RAIS) e no cadastro Central de Empresas do Instituto Brasileiro de Geografia e Estatística (IBGE).

A divulgação relatou que as atividades mais usadas na rede são o envio e recebimento e-mail, seguido por buscas de informações sobre produtos e serviços (NIC.br, 2008).

Em outra pesquisa, também realizada pelo site NIC.br, a TIC Empresas 2008, 94% das empresas do Brasil utilizavam computadores, numa porcentagem semelhante ao do ano anterior.

Tal pesquisa mostrou que a utilização da tecnologia está relacionada ao porte da empresa, pois em empresas com 50 ou mais funcionários, 100% utilizavam essa tecnologia. Em relação ao número de computadores ligados na internet, se manteve em 97% (NIC.br, 2009).

Em estudo realizado pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas do estado de São Paulo

(SEBRAE-SP), foi realizada uma pesquisa para identificar a utilização de Tecnologias da Informação e Comunicação (TIC) nas Micro e Pequenas Empresas (MPEs). A TIC a que esse estudou se referiu foram os microcomputadores, internet e celular. O celular foi utilizado em 91% das MPEs, 75% utilizavam microcomputadores e 71% tiveram acesso à internet.

O SEBRAE-SP (2008) relatou que o sistema operacional mais usado pelas MPEs foi o Windows (96%), seguido com o Linux (2%), MS-DOS (1%) e outros (Macintosh, Novell, Unix, etc.) também com 1%. As empresas que utilizaram software integrado (software que interligue vários setores, como compras, vendas, contas a pagar, estoque, entre outros setores) totalizaram 34%.

Na 10ª edição da pesquisa nacional de segurança da informação realizada pelo Módulo Risk Management (2006), foi relatado que 15% das empresas investiram menos de 1% do valor destinado à tecnologia da informação.

2.3 Problemas e ocorrências com *Malwares*

Ano após ano, vem crescendo o número de *malwares* existentes. Para se ter uma noção do crescimento de *malwares* existentes, foi pesquisado no site da McAfee (2010), uma empresa que trabalha com programas para segurança de informação, a quantidade de ameaças que se consegue detectar.

Tabela 1 – Número de ameaças detectadas pelo software da McAfee no período de agosto de 2008 a agosto de 2010.

Versão DAT	DAT Data de Lançamento	Ameaças Detectadas
5310	4/6/2008	397574
5635	3/6/2009	532235
6002	3/6/2010	622531

Fonte: DAT Readme. McAfee Theat Center

Nota-se na Tabela 1 que, no período de 2 anos, de junho de 2008 a junho de 2010, houve um crescimento de quase 225 mil novas ameaças.

Informações sobre as ocorrências de incidentes no Brasil e os tipos de ataques foram retiradas do site Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Os incidentes reportados ao CERT.br vêm crescendo ano após ano.

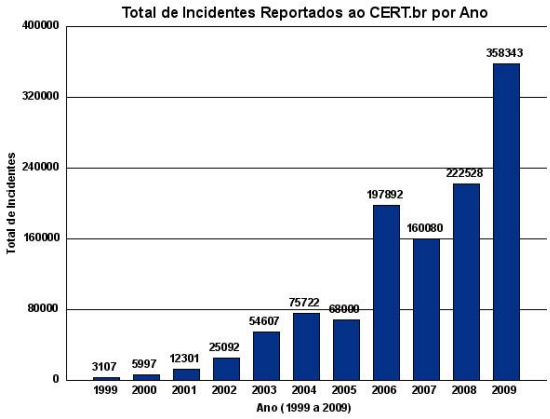

Figura 1 – Incidentes reportados ao CERT.br do ano de 1999 até 2009

Fonte: CERT (2009).

As últimas 3 edições do TIC Empresas, realizadas nos anos de 2007, 2008 e 2009, mostram os tipos de problema com a segurança em relação ao número de funcionários. Comparando-se os 3 anos, nota-se que houve um aumento de problemas devido à segurança. Os crescimentos maiores de problemas são com relação a vírus, cavalos de tróia e *worm*.

Na 10ª edição da pesquisa nacional de segurança da informação, realizada pelo Módulo Risk Management (2006), os investimentos na área de segurança da informação ajudaram empresas a ficarem mais preparadas para enfrentar falhas de segurança. No entanto, 33% das empresas não souberam quantificar as perdas e 21% sequer conseguiram identificar os responsáveis pelos problemas.

Um dos motivos dessas falhas é a falta de planejamento na área de segurança. Quando conseguiram identificar os responsáveis pelos problemas, chegou-se à conclusão de que 24% deles ocorreram pelos próprios funcionários, 20% por causa de *hackers*, 15% por vírus, 10% por de *spam* e 8% por fraudes.

Atualmente, existem várias metodologias usadas para difundir os *malwares* entre os usuários. Nos próximos parágrafos estão expostos alguns relatos sobre métodos usados pelos criadores desses softwares maliciosos para disseminarem essas pragas virtuais, métodos como vírus em celular, por meio de redes sociais, comunicador instantâneo e sites infectados.

Em 2004, foi descoberto o primeiro vírus para celular e até o começo do ano de 2008, foram contabilizados 362 tipos de vírus para celular que afetam principalmente aparelhos que utilizam o sistema operacional para celular *Symbian.*

Esses vírus de celular podem causar vários tipos de problemas, como desconfigurar os aparelhos, descarregar a bateria, enviar mensagens, obter informações privilegiadas como agenda telefônica, gravar chamadas feitas e recebidas ou mensagens. Para se espalharem para outros celulares, os vírus são enviados por *bluetooth*, mensagens multimídias (MMS), por *download* e instalação de arquivos infectados (BAIO; FERREIRA, 2008).

Vírus e *spams* estão se propagando facilmente por meio de redes sociais, como a *Facebook* e *Twitter*, pois os usuários têm certa relação de confiança com esses sites e navegam despreocupados. O usuário não acredita que um colega possa tentar seu computador através de uma mensagem aparentemente inofensiva ou um link para a visualização de uma suposta foto que, na realidade, é um software malicioso e nocivo. Por mais inocente que possa parecer essa técnica de espalhar o *malware*, muitos usuários são surpreendidos. Geralmente esses vírus roubam a senha da conta do usuário e, com isso, a vítima pode sofrer um roubo de identidade *on-line* (GIL, 2009).

O comunicador instantâneo MSN Messenger também pode causar um problema semelhante. O usuário recebe uma mensagem de outro usuário que esteja em sua lista de contatos, e essa mensagem contém um link. Quando, inocentemente, a vítima abre esse link, o computador é infectado por algum tipo de *malware*. Quando infectado, o computador começa enviar mensagens através do MSN para a lista de contatos, sem que usuário saiba. Essas mensagens também contêm um link onde há códigos maliciosos e quando a próxima vítima acessar esse endereço eletrônico, ele será infectado. Assim, um computador vai infectando outros computadores. (HONORATO, 2008).

Existem vírus para MSN capazes de checar o sistema e mudar o idioma da mensagem que tenta induzir o usuário a acessar o endereço eletrônico. O vírus pode enviar as mensagens em espanhol, inglês, holandês, francês, alemão, italiano, português, sueco, turco e grego, com conteúdo da mensagem sendo do tipo "haha, eu encontrei sua foto" seguido pelo endereço eletrônico (FOLHA ONLINE, 2005).

Foram identificados centenas de milhares de sites infectados por *softwares* maliciosos. Os responsáveis pela disseminação dos *malwares* em sites utilizam geralmente scripts automatizados ou anúncios maliciosos (MESSMER, 2009). Após a contaminação dos sites pelo código malicioso, esses então passam a infectar os computadores dos visitantes. Essa tática passa ser interessante para os criminosos para espalhar os vírus, pois o usuário deposita confiança em sites que já conhece e, com isso, navega pelo site sem preocupação (ROHR, 2010).

Outro problema é a infecção causada por falsos antivírus. O principal objetivo é de lucrar com a venda desses programas. Esses programas funcionam de maneira semelhante aos antivírus normais, em que o falso antivírus avisa os usuários que estão infectados e são mostrados vários *pop-ups* e *screensavers* (proteção de tela) de forma contínua, praticamente impossibilitando que o usuário possa

utilizar o computador. A finalidade dessas mensagens é de assustar o usuário fazendo com que eles paguem por um serviço melhor de antivírus (PANDA SECURITY, 2008). Hautsch (2009) explicou que esses falsos antivírus são programas que se disfarçam de ferramentas de proteção e remoção de *malwares*, mas que, na realidade, expõem o computador das vítimas a diversos tipos de ameaças.

Alguns *malwares* se destacam em relação a outros, pois alguns têm um grande poder de contágio, como o Conficker.

Conficker, kido ou DownadUp foi descoberto no final do ano de 2008 e novos tipos foram detectados no começo de 2009. Esse *malware* é um *worm* (verme) que explora uma vulnerabilidade do sistema operacional Windows. Ele se espalha por meio de rede e dispositivos de armazenamentos removíveis, como por exemplo, *pendrives*, usando a função de execução automática do Windows. O objetivo desses *worms* é gerar nos computadores infectados, uma grande rede de *bots* para que seus criadores possam enviar *spams*, roubar informações e encaminhar o usuário a sites maliciosos (TREND MICRO, 2010).

No começo de 2009, a empresa Panda Security (2009) realizou um estudo que envolvia cerca de 2 milhões de computadores, e mostrava que a infecção se originou na China e se espalhava para 83 países, entre eles o Brasil. Segundo diretor técnico da PandaLab, Luis Corrons, dos 2 milhões de computadores analisados, cerca de 115.000 estavam infectados com este *malware*, um fenômeno que não se verificava desde os tempos das grandes epidemias do Kournikova ou do Blaster. (PANDA SECURITY, 2009).

O Conficker teve grande repercussão no dia 1º de abril de 2009, quando o último variante desse *worm* iria modificar o modo de comunicação com outros infectados da rede de *bots*, visando infectar mais máquinas e aumentando as tentativas de conexão (TREnD MICRO, 2010).

3 MATERIAL E MÉTODOS

3.1 Material utilizado

Para a realização do trabalho foi necessária a utilização de um computador provido dos seguintes componentes: sistema Microsoft Windows XP com a atualização do *Service Pack* 3, editor de texto Microsoft Office Word para a redação do artigo e anotações, Microsoft Office Excel para a elaboração de gráficos e tabela, navegador de internet Windows Internet Explorer 8 e navegador Mozilla Firefox e acesso à internet.

3.2 Metodologia

O passo inicial foi verificar se realmente houve um aumento de incidentes com relação a *malwares*.

Foi acessado o site do CERT.br, criado com a função de responder sobre incidentes de segurança na internet do Brasil. O CERT.br recebe as informações, analisa-as e dá uma resposta sobre o ocorridos. Seu objetivo é de ajudar administradores de redes em relação a problemas na área de segurança das tecnologias da informação, auxiliando numa maior capacidade de detecção de incidentes, correlação de eventos e determinação de tendência de ataques no espaço da internet do Brasil.

Observando-se que realmente vem ocorrendo aumento do número de incidentes, foram feitas buscas para se saber quais os tipos que mais ocorreram. No site do Núcleo de Informação e Coordenação do Ponto BR, o NIC.br, foi encontrada essa informação. Confirmado que houve um aumento de incidentes, teve-se início do levantamento de literatura para se analisar a causa.

A realização do levantamento de literatura foi feita em três etapas, sendo que a primeira consistiu no levantamento de definições essenciais para o entendimento do assunto. Na segunda etapa, foi realizada uma busca de informações sobre a utilização de tecnologia da informação nas empresas e, na terceira, foi realizado um levantamento de informações sobre o cenário de ameaças atuais e ocorrências relatadas.

3.2.1 Levantamento de definições

Foi o primeiro passo para a realização do trabalho. Sabe-se que o *malware* prejudica no desempenho da Tecnologia da Informação, causando um dano no sistema de informação usado pelas empresas. Com isso, é importante saber o que são dados, informação, sistema de informação e tecnologia da informação. Essas definições foram retiradas de livros de segurança da informação, livros de gerenciamento de sistema de informação e artigos científicos relacionados a esses assuntos.

3.2.2 Estudo de uso da Tecnologiada Informação pelas empresas

No site do Núcleo de Informação e Coordenação do Ponto BR, o NIC.br, que foi responsável por coordenar e integrar as iniciativas de serviços da internet do país, foram levantadas as pesquisas sobre a Tecnologia de Informação e Comunicação (TIC) das empresas nos anos de 2007, 2009. Estas pesquisas contêm informações sobre a porcentagem de empresas que

fazem uso da tecnologia da informação, estabelecendo uma relação de tamanho da empresa quanto à utilização de tecnologia da informação. Também informou o número de empresas que tem acesso à internet.

O Serviço Brasileiro de Apoio às Micro e Pequenas Empresas do estado de São Paulo (SEBRAE-SP) também realizou uma pesquisa TIC no ano de 2008 enfocando Micro e Pequenas Empresas (MPEs). Nesse site foi levantada a porcentagem de MPEs que fizeram uso de microcomputadores, internet e celular. Também foi analisado o crescimento do uso de computador e internet do ano de 1992 até 2008. Outro ponto estudado, utilizado para a redação deste trabalho, foi a informação de que 96% dos computadores das MPEs utilizam sistema operacional Microsoft Windows.

Em pesquisa realizada pela Módulo Risk Management em 2006, a 10ª edição da pesquisa nacional de segurança da informação, foi estudado o grau de investimento que as empresas realizaram com a segurança da informação (Figura 4). Notou-se que depois de problemas com *hackers* e com os próprios funcionários, os maiores problemas são os *malwares*.

3.2.3 Estudo de ocorrências e relatos que envolvam *malware*

Esta etapa consistiu em procurar, em matérias jornalísticas, reportagens com relatos de *malwares*.

Foi feita uma busca da quantidade de *malwares* existentes até o presente momento, porém não foi encontrado um valor consensual. Por essa razão, foi feita uma busca nos sites dos antivírus dos softwares antivírus para a pesquisa de número mais real.

No site McAfee, pesquisou-se a última versão de atualização de seu programa, lançado no dia 3 de junho de 2010 (foi acessado no dia 3 de junho de 2010, ou seja, a versão que foi lançada no próprio dia). Também foram levantados as atualizações de 1 e 2 anos atrás (3 de junho de 2009 e 4 de junho de 2008), a fim de se comparar o aumento de ameaças. Com essas informações, obteve-se o número aproximado de 600 mil *malwares*. Também pode ser observado que houve um grande aumento do número de ameaças.

Após a comparação das versões do antivírus McAffe, foi pesquisado se o antivírus conseguia detectar a maioria dos vírus existentes. Como resultado, observou-se que o antivírus da McAffe detectou 98,9% dos *malwares*.

A 10ª edição da pesquisa nacional de segurança da informação realizada pelo Módulo Risk Management indicou alguns problemas que causaram falhas no sistema de segurança, como falta de planejamento

na área de segurança, os funcionários, *hackers*, vírus, *spam*, fraude, entre outros. Outro ponto importante é o relato de que 33% das empresas não sabem quantificar o valor dos prejuízos e 21% não sabe identificar o causador do problema.

Após ter essas informações levantadas, foram procurados artigos e reportagens recentes sobre *malwares*, em sites de notícias e de segurança da informação. Alguns fatos interessantes foram explanados na revisão de literatura.

4 RESULTADOS E DISCUSSÃO

Após o levantamento das informações necessárias e análise dessas informações, com a confirmação de que realmente houve um aumento de incidentes, os possíveis motivos do aumento de incidentes estão relacionados aos itens abaixo:

4.1 Surgimento de novas ameaças

O aumento no número de ameaças é real, porém difícil de ser quantificado, mas estima-se aproximadamente de 600 mil novos *malware*, no período de dois anos. Por essa razão, para se ter uma estimativa de crescimento, foi calculada a quantidade de *malware* que o antivírus da McAfee detectava entre os anos de 2008 e 2010, quando se obteve o resultado de, aproximadamente, 225 mil novas ameaças.

4.2 Surgimento de novas técnicas de disseminação de *malwares*

Além das formas mais comuns de se contaminar o computador, por meio da execução de programas infectados, de computador da rede com vírus, por meio de *pendrives* e disquetes contaminados, há novos meios.

Os novos vírus estão contaminando sites normais, com o objetivo de o usuário acessar esses sites de forma despreocupada, pois são sites conhecidos e confiáveis. Também estão sendo utilizados meios como redes sociais e programas de mensagens. Computadores infectados repassam a mensagem que contém um link para a lista de contato. A vítima realmente acredita que a mensagem foi enviada por um conhecido, abre o link e o computador é contaminado, formando uma reação em cadeia.

Celulares estão disseminando *malwares* via *bluetooth* e mensagens multimídias, também conhecidas como mensagem MMS.

4.3 Falta de uma regra de segurança definida nas empresas

Segundo pesquisa realizada pelo Módulo *Risk Management* em 2006, que aborda análises de riscos nas organizações, a capacitação de equipes e a conscientização de funcionários ajudam a minimizar os incidentes. Apontaram a falta de planejamento na área de segurança como um dos principais fatores para o aumento do número de incidentes de segurança. Os funcionários devem se submeter às regras de segurança para que não haja problemas nos sistemas de informação. Nas empresas sem regras de segurança, o usuário pode fazer uso de computadores para fins pessoais e não empresariais.

4.4 Pouco investimento por parte das empresas

A mesma pesquisa realizada pelo Módulo Risk Management relatou que, aproximadamente, 15% das empresas gastaram menos de 1% com segurança da informação do valor que é destinado ao investimento na área de tecnologia da informação. É um valor muito baixo para se investir.

As empresas não dão o devido valor ao investimento com segurança da informação, como por exemplo, em treinamento de funcionários, aquisição de *softwares* antivírus e de *firewall*, facilitando a contaminação de computadores das redes empresariais.

4.5 Desinformação do usuário

Após ter analisado as pesquisas relacionadas a incidentes que envolviam *malwares*, modo de disseminação e funcionamento de alguns *malwares*, conclui-se que a principal vulnerabilidade de um sistema de informação é o descuido e desinformação por parte do usuário.

O usuário navega despreocupado pela internet, não atualiza os *softwares*, faz uso de *software*s piratas, não verifica arquivos com antivírus, utiliza *pendrives* de forma descuidada, é descuidado ao ver e-mails, é vítima de golpes para roubo de dados pessoais (*phishing*), entre outros descuidos.

A boa conduta do usuário de computador é um grande passo para que os sistemas de informações empresariais sejam mais seguros. É de extrema importância a realização de investimentos em treinamentos de usuários para que adquiram bons costumes com computadores empresariais

4.6 Medidas de segurança

Algumas medidas devem ser tomadas para evitar os *malwares*. Essas

medidas não são efetivas, mas podem minimizar o número de incidentes que envolvam *malwares*. São algumas delas:

- Utilização de um bom antivírus, mantendo-o sempre atualizado. É importante verificar o seu histórico e a empresa que desenvolve o software antivírus, pois existem falsos antivírus no mercado.
- Verificação, com o antivírus das unidades removíveis (como CDs, disquetes e pen drives) ao serem introduzir no computador.
- Realização, sempre que possível, de varredura no sistema com software antivírus.
- Utilização de firewall.
- Utilização de software *antispyware*.
- Não utilização de softwares piratas.
- Manutenção do sistema operacional sempre atualizado, pois os malwares exploram as vulnerabilidades dos sistemas operacionais. As atualizações contem correções para eliminar as vulnerabilidades.

Atualização continua dos *softwares*, pois os *malwares* exploram as vulnerabilidades desses *softwares*. Além dessas, as atualizações das ferramentas também auxiliam problemas de vulnerabilidade.

- Atenção com os e-mails. Caso receba um e-mail suspeito, não se deve abrir e se for de pessoa conhecida, verificar se a pessoa realmente enviou.
- Aplicação de uma política de segurança bem definida.

E, principalmente, as empresas devem:

- Educar o usuário a ter práticas de segurança, através de conhecimentos sobre o que são malwares, o que podem causar e como evitá-los e combatê-los.

5 CONCLUSÃO

Vem ocorrendo um aumento continuo do número de *malwares*, com novos meios e técnicas de disseminação. Pelos dados obtidos, detectou-se que a principal vulnerabilidade de um sistema de informação de uma empresa são os próprios funcionários, agindo de maneira inapropriada e mesmo assim, algumas empresas não apresentam uma política de segurança adequada.

Essas empresas deveriam investir em cursos de esclarecimento e treinamento aos seus funcionários, a fim de preservar a suas informações.

REFERÊNCIAS

BURGO R.N.S.; TAMAE P.Y. Administração de sistemas de informação: os desafios éticos da

tecnologia da informação x segurança. **Revista Cientifica Eletrônica de Administração,** Garça, n. 11, dez, 2006

BAIO, C. ; FERREIRA, L. Seu celular anda meio louco? Cuidado, ele pode estar com vírus. **UOL tecnologia**. Jan, 2008. Disponível em: <http://tecnologia.uol.com.br/proteja/ultnot/2008/01/23/ult2882u34.jhtm> Acesso em: 3 jun. 2010.

FOLHA ONLINE **Vírus que se espalha via MSN Messenger "fala" diversas línguas**. Out. 2005. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u18861.shtml>. Acesso: 4 jun. 2010.

FUENTES L.F. *Malware, una amenaza de* Internet. **Revista Digital Universitária,** México D. F., v. 9, n. 4, abril, 2009**.** Disponível em: <http://www.revista.unam.mx/vol.9/num4/art22/int22.htm>. Acesso em: 13, set. 2009.

G1. **Apesar de 'silêncio' em 1º de abril, ameaça do vírus Conficker continua.** Abr. 2009 <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1070107-6174,00-APESAR+DE+SILENCIO+EM+DE+ABRIL+AMEACA+DO+VIRUS+CONFICKER+CONTINUA.html> Acesso em: 4 jun. 2010.

GIL P., Vírus e spams circulam impunemente nas redes sociais. **Folha Online.** Dez. 2009. Disponível em <http://www1.folha.uol.com.br/folha/informatica/ult124u669487.shtml>. Acesso em: 5 jun. 2010.

HONORATO L. **Cuidado! Não seja vítima de vírus via MSN messenger**. Nov. 2008. Disponivel em: <http://www.artigonal.com/seguranca-artigos/cuidado-nao-seja-vitima-de-virus-via-msn-messenger-661474.html>. Acesso em: 5 jun. 2010.

KARISTON, P.; MAZZOLA, V.B. Modelo das Tríades Conjugadas. In: IV Simpósio Segurança em Informática - SSI'2002, 2002, São José dos Campos - SP. **Anais do IV Simpósio Segurança em Informática SSI'2002**. CTA/ITA: S. José dos Campos, 2002. p. 45-54.

MANSON, M, **Estudio sobre vírus informáticos**, 1999. Disponível em: <http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml?monosearch. Acesso em: 12 set. 2009.

McAfee. *Dat Readme.* ***McDfee Theat Center*****.** 2010. Disponível em: <HTTP://VIL.NAI.COM/VIL/DATREADME.ASPX> Acesso em: 3 jun. 2010

MESSMER, E. ***Malwares*** **atingem mais de mais de meio milhão de sites no mundo**. Out, 2009. Disponível em: <http://computerworld.uol.com.br/seguranca/2009/10/28/malwares-atingem-mais-de-meio-milhao-de-sites-no-mundo/ > Acesso em: 10 mai. 2010.

MÓDULO RISK MANAGEMENT. 10ª **Pesquisa nacional de segurança da informação**. 2006. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf > Acesso em: 5 maio . 2010.

NIC.br. **Mais de 95% das empresas brasileiras estão informatizadas e têm acesso *Web*.** Maio, 2008. Disponível em: <http://www.nic.br/imprensa/clipping/2008/midia223.htm >. Acesso em 22 abr. 2010.

NIC.br. **CGI.br divulga os resultados da pesquisa TIC Empresas 2008.** abr, 2009. Disponível em: < http://www.nic.br/imprensa/releases/2009/rl-2009-09.pdf >. Acesso em 22 abr. 2010.

PANDA SECUTITY. **Seis porcento dos computadores analisados pela Panda Security infectados pelo *worm* Conficker**. Jan. 2009. Disponível em: <http://www.pandasecurity.com/portugal/h omeusers/media/press-releases/viewnews?noticia=9527>. Acesso: 5 jun. 2010.

SEBRAE-SP. **As Tecnologias de Informação e Comunicação (TICs) nas MPEs brasileiras**. 2008. <http://www.sebraesp.com.br/sites/default/files/informatizacao_br_2008.pdf> Acesso em 26 abr. 2010.

TRED MICRO. **O *Worm DOWNAD*/Conficker** <http://br.trendmicro.com/br/threats/conficker-worm/>. Acesso em: 5 jun. 2010.