SEGURANÇA DA INFORMAÇÃO EM TI

Marcelo Bispo Almeida[1]

RESUMO

A tecnologia da informação é um assunto bastante discutido na atualidade, devido ao seu favorecimento junto à competitividade e crescimento empresarial. No entanto, é imprescindível que toda essa tecnologia e informação sejam seguros. Por esse contexto às questões de segurança que envolve a tecnologia da informação dentro do aspecto dos sistemas e programas que compõem as redes corporativas e integradas, que são utilizadas por inúmeras pessoas ao mesmo tempo ficando cada vez mais suscetíveis a problemas e ameaças de segurança, especialmente no que se refere ao bem mais precioso das empresas: a informação. Esse estudo tem como objetivo geral demonstrar como as redes corporativas, seus sistemas e programas, especialmente integrados, são suscetíveis a problemas e ameaças de segurança, considerando os vírus como principal ameaça, destacando os principias meios de proteção e prevenção dos problemas ocasionados pelos vírus, bem como comparando os tipos mais severos e predominantes nos dias atuais. Para realização desse estudo, além do conhecimento pessoal serão utilizados resultados de pesquisas existentes sobre o assunto, destacando autores e pesquisadores especializados no assunto, de modo a demonstrar que as hipóteses selecionadas nesse estudo sejam atendidas satisfatoriamente e os resultados e objetivos sejam alcançados com sucesso.

Palavras-Chave: Segurança; Tecnologia; Informação.

[1]Especializando em Gestão de Redes e Segurança da Informação – Faculdade de Administração e Negócios de Sergipe, Licenciado em Informática – Universidade Tiradentes. E-mail: marcelo20006abm@hotmail.com

ABSTRACT

Information technology is a much discussed topic today, due to his favor with the competitiveness and business growth. However, it is essential that all this technology and information are safe. For this context to security issues involving information technology in the aspect of systems and programs that make up the corporate and integrated networks, which are used by many people at the same time becoming more susceptible to security issues and threats, especially as regards the much precious firms: information. This study has the general objective to demonstrate as corporate networks, systems and programs, especially integrated, are susceptible to security problems and threats, considering the virus as the main threat, stressing the main means of protection and prevention of problems caused by viruses, as well as comparing the most severe and prevalent types today. To conduct this study, in addition to personal knowledge will used the results of existing research on the subject, highlighting authors and specialized researchers on the subject, in order to demonstrate that the assumptions selected in this study are met satisfactorily and the results and objectives.

Keywords: Security; Technology; Information.

INTRODUÇÃO

Atualmente as empresas precisam se conscientizar e principalmente se adaptar a uma nova era, denominada era da informação digital, que possibilita as organizações estão estratégica mais eficiente, tomadas de decisões mais precisas e consequentemente maiores competitividade através do uso de recursos inteligentes que são oferecidos pela tecnologia da informação especialmente pelos sistemas de informação.

A tecnologia da informação tem disponibilizado as empresas ao longo dos anos, recursos tecnológicos e computacionais voltados à geração e gerenciamento de informação. Os sistemas de informação estão cada vez mais sofisticados, produzindo mudanças significativas e positivas nas organizações, visto que possibilita que estas tenham melhores condições de enfrentar o mercado em que estão atuando, através do uso das informações.

Atualmente pode-se dizer que não existe possibilidade de as empresas serem competitivas sem que se utilizem dessas ferramentas, visto que elas possibilitam novas visões, sejam do presente ou do futuro da empresa.

Os sistemas de informações da atualidade favorecem a empresa mediante a disseminação de informações que são consideradas essenciais para a organização, muitas vezes sendo transformadas em conhecimentos e experiências que facilitam as decisões da empresa.

No entanto, é necessário que esses sistemas sejam envoltos de uma segurança ampla e eficiente. Nesse contexto, esse estudo foi motivado pelo fato de que dá ênfase às questões de segurança que envolve a tecnologia da informação em seu contexto dos sistemas e programas que compõem as redes corporativas e integradas, que são utilizadas por inúmeras pessoas ao mesmo tempo ficando cada vez mais suscetíveis a problemas e ameaças de segurança, especialmente no que se refere ao bem mais precioso das empresas: a informação.

Esse estudo tem como objetivo geral demonstrar como as redes corporativas, seus sistemas e programas, especialmente integrados, são suscetíveis a problemas e ameaças de segurança, considerando os vírus como principal ameaça, destacando os principias meios de proteção e prevenção dos problemas ocasionados pelos vírus, bem como comparando os tipos mais severos e predominantes nos dias atuais.

Para realização desse estudo, além do conhecimento pessoal serão utilizados resultados de pesquisas existentes sobre o assunto, destacando autores e pesquisadores

especializados no assunto, de modo a demonstrar que as hipóteses selecionadas nesse estudo sejam atendidas satisfatoriamente e os resultados e objetivos sejam alcançados com sucesso.

2 SEGURANÇA DA INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Aplicando-se a definição de sistema, pode-se afirmar que Sistema de Informação como um conjunto de elementos inter-relacionados, processos, dados e tecnologia, cuja finalidade é alimentar os centros de decisões, com as informações de ação que permitam a consecução dos objetivos da organização.

A finalidade de um sistema de informação é trabalhar dados e transformá-los em informações para auxiliar os administradores na direção e controle das operações. E, para isso torna-se necessário um conjunto de dispositivos físicos, procedimentos de processamento de informação e canais de comunicações. A informação é o resultado final da transformação dos dados existentes acerca de alguém ou de alguma coisa.

Um sistema de informação visa a tornar disponível para a administração da entidade informação de natureza gerencial ou operacional, para uso em todos nos níveis de decisões sejam eles estratégicos, operacionais ou táticos.

Segundo O´Brien (2002, p. 6) “Sistema de informação é um conjunto organizado de pessoas, hardware, software, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização”.

Para Stair (1998, p. 11) “É uma série de elementos ou componentes inter-relacionados que coletam (entrada), manipulam e armazenam (processo), disseminam (saída) os dados e informações e fornecem um mecanismo de feedback”.

Laudon e Laudon (1999) expõem que:

> Um sistema de sistema de informação pode ser definido como um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informações com a finalidade de facilitar o planejamento, o controle, a coordenação, a analise e o processo decisório em empresas e outras organizações. Laudon e Laudon (1999, P. 04)

De acordo com essas definições, podemos dizer que um sistema de informação trabalha dados e transforma-os em informações que serão utilizadas no processo decisório das organizações. É produzir informações úteis e confiáveis são realizados os procedimentos de

entradas, processamento dos dados, e por fim, as saídas de informações. Stair (1998, p. 12) enuncia os componentes de sistema como:

> A entrada é a atividade de juntar os dados primários. O processamento envolve a conversão ou transformação dos dados em saídas úteis. A saída envolve a produção de informações úteis, geralmente na forma de documentos, relatórios e dados de transações. Feedaback é uma saída usada para fazer ajustes e modificações nas atividades de entrada ou processamento.

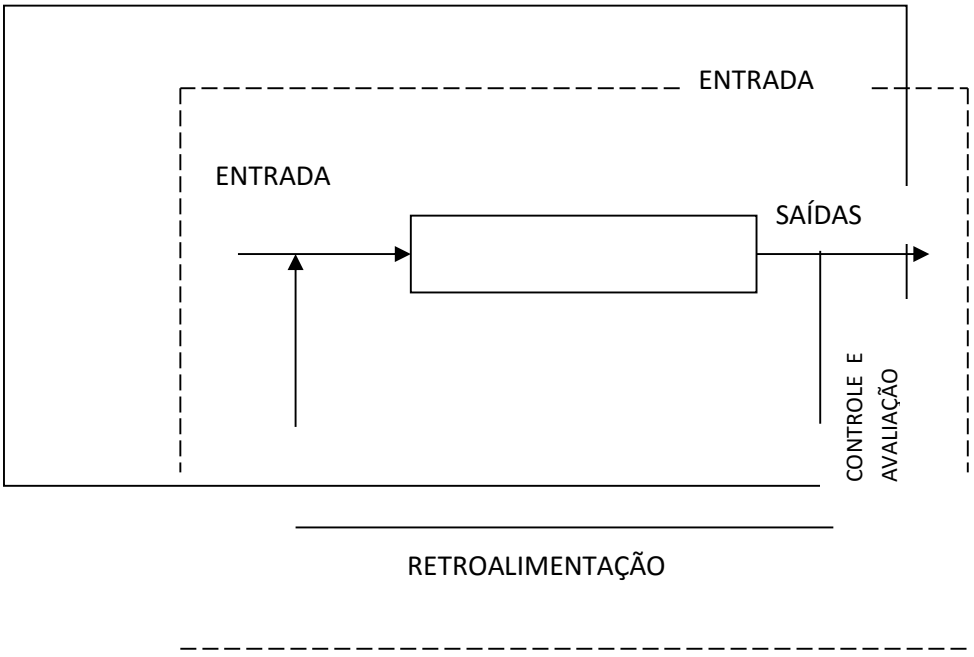


Figura 1 - Componentes de um sistema
Fonte: OLIVEIRA, 2001.

Assim, sistema de informação é um, conjunto de procedimentos que visam captar dados e transformá-los em informações úteis e transmiti-las á gerentes e administradores para dar subsídios ao processo decisório.

Para controle e fiscalização das rotinas da empresa, o sistema de informações é implantado nas empresas. Este sistema de informação "é o controle obtido mediante a prestação de informações aos níveis adequados da administração". (CREPALDI, 2002: p. 65). Segundo Cruz (2000: p. 82):

> “Sistemas de informações gerenciais são desenvolvidos para garantir a administração eficiente a qualquer tipo de empresa.” E mais adiante diz, “são o conjunto de tecnologias que disponibiliza os meios necessários à operação do processo decisório em qualquer organização por meio do processamento dos dados disponíveis.” (CRUZ, 2000, p. 54)

Conforme OLIVEIRA (1996: p. 39) esses sistemas é: “o processo de transformação de dados em informações que são utilizadas na estrutura decisória da empresa, bem como proporcionam a sustentação administrativa para otimizar os resultados esperados. Segundo Bio (1996, p. 34) os sistemas podem ser classificados em: Sistemas de apoio às operações; Sistema de apoio a gestão.

Para Bio (1996, p. 34) “Os sistemas de apoio às operações são tipicamente processadores de transações, ou seja, são redes de procedimentos rotineiros que servem para o processamento de transações recorrentes”.

Conforme Daft (1999, p. 221) sistemas de as operações são “Sistemas de processamento de transações que automatizam a rotina das da organização e as transações comerciais cotidianas. As tarefas podem ser executadas com mais eficiência pela utilização da tecnologia computacional”.

Desse modo o sistema de apoio às transações serve como suporte das operações que fazem parte da rotina diária de uma organização. Desse modo, podem dar suporte as operações mais simples como compras, faturamento, contas a pagar, contas a receber, entre outras; e as operações mais complexas como, controle de produção, contabilidade, e outras.

Bio (1996, p. 35) comenta que: “Os sistemas de apoio à gestão não são orientados para o processamento de transações rotineiras, mas existem especificamente para auxiliar processos decisórios”.

Segundo Padoveze (1997, p. 36) “[...] os sistemas de apoio a gestão preocupam-se basicamente com as informações necessárias a gestão econômico-financeira da empresa”.

Diante do exposto, os sistemas de apoio à gestão são fundamentais para auxiliar a tomada de decisão de gerentes e administradores proporcionando uma visão mais ampla das atividades da empresa, servindo de apoio para correção de problemas que possam existir.

Dessa forma, os sistemas de operações devem proporcionar eficiência nos processos para execução das operações rotineiras e os sistemas de gestão devem auxiliar a tomada de decisão segura, uma vez estas irão delinear o bom andamento da organização.

A administração revela-se nos dias de hoje como uma das áreas do conhecimento humano mais impregnadas de complexidades e de desafios. O profissional que utiliza a administração como meio de vida pode trabalhar nos mais variados níveis da organização.

Não há duas organizações iguais, assim como não existem duas pessoas idênticas. Cada organização tem os seus objetivos, o seu ramo de atividade, os seus dirigentes e o seu pessoal, os seus problemas internos e externos, o seu mercado, a sua situação financeira, a sua tecnologia, os seus recursos básicos, a sua ideologia e política de negócios.

O ponto fundamental do sistema de informação é o uso da informação contábil como ferramenta para a administração.

Para que essa informação seja usada no processo de administração, é necessário que seja desejável e útil para as pessoas responsáveis pela administração da empresa. Para os administradores que buscam a excelência empresarial, uma informação, mesmo que útil, só é desejável se conseguida a um custo adequado e interessante para a empresa. A informação não pode custar mais do que ela pode valer para a administração.

Para se fazer, então, contabilidade gerencial, é mister a construção de um Sistema de Informação Contábil Gerencial. Em síntese, é possível fazer e é possível ter contabilidade gerencial dentro de uma organização, desde que se construa um Sistema de Informação Contábil.

Os sistemas de informações gerenciais que têm como objetivo fundamental a consolidação e aglutinação de todas as informações necessárias para a gestão do sistema empresa. O sistema de informação contábil deverá estar completamente integrado ao sistema de gestão Empresarial.

Conforme, Iudícibus (1998, p. 15) a contabilidade gerencial caracteriza-se, de maneira geral dando enfoque especial conferido a várias técnicas e procedimentos contábeis já conhecidos na contabilidade financeira, na contabilidade de custos, na análise financeira e de balanços, etc., colocados numa perspectiva diferente, num grau de detalhe mais analítico ou numa forma de apresentação e classificação diferenciada, de maneira a auxiliar os gerentes das entidades em seu processo decisório.

Com base, nesse pressuposto, entende-se que a Contabilidade Gerencial, volta-se especificamente para a administração da empresa, procurando subsidiar os gestores com informações que se "encaixem "de maneira efetiva no modelo decisório do administrador.

Neste particular, explica Iudícibus (1998):

> (...) considere-se que o modelo decisório do administrador leva em conta cursos de ação futuros; informes sobre situações passadas ou presentes somente serão insumos de valor para o modelo decisório à medida que o passado e o presente sejam estimadores válidos daquilo que poderá acontecer no futuro, em situações comparáveis às já ocorridas. Iudícibus (1998, p. 17)

É importante relatar que estudar a Contabilidade Gerencial é de grande importância para as empresas, de um modo geral. Haja vista que sua importância origina-se, principalmente, nas relações existentes entre a tomada decisão pelos administradores e as informações, que sustentam essas decisões. "O entrelaçamento dos estudos contábeis e administrativos não deixa dúvidas, na atualidade. Valer-se do conhecimento da contabilidade para a tomada de decisões dos fatos administrativos é hoje a mais exuberante parte de estudos que se conhece no setor". (SÁ, 1971, p. 19)

A experimentação, a vivência, o bom senso e a origem das doutrinas são fatores determinantes para que os dados e interpretações oferecidos pela contabilidade não sejam abandonados pela Administração.

> "Quanto mais complexa se torna a vida econômica dos povos, quanto mais inquieto o seu sistema político-social, quanto mais agitada a legislação, tanto mais subsídios devem ser colhidos pela administração através da ciência contábil." (SÁ, 1971, p. 19)

Com o surgimento das grandes sociedades comerciais, industriais e em especial das sociedades anônimas de capital aberto, as empresas vêm distanciando o conceito de propriedade do conceito de dirigentes, uma vez que estes não são necessariamente seus proprietários. Na medida em que este processo sobressai-se aumenta a necessidade de informações precisas, basicamente contábeis, que possibilitem um maior rigor administrativo.

O abandono do empirismo tem levado a administração a buscar mais elementos na contabilidade e esta a adaptar seus sistemas para melhor servir aquela. "Fatos administrativos e fatos contábeis, oriundos de um mesmo campo não podem viver dissociados; muito pelo contrário, cada vez mais se evidencia a profundíssima ligação entre eles." (SÁ, 1971, p. 19).

2.2.1 Redes de Computadores

Segundo Oliveira (2001 p. 37), atualmente a informação é considerada a matéria-prima das organizações. Através da obtenção de informações confiáveis, relevantes, objetivas, geradas em tempo hábil é que se viabiliza a tomada de decisão segura, baseadas na real situação.

Uma empresa não pode ser considerada ou vista como parte isolada perante o todo. Para sobrevivência da mesma é necessário levar em consideração tanto as informações internas como as externas, pois ambas irão influenciar na tomada de decisão.

As empresas de hoje, independente do tamanho, necessitam de informação para reagir frente aos problemas e oportunidades do ambiente de negócio, pois assim conseguirão atingir níveis mais altos de produtividade e eficácia nas organizações, nas fábricas e na prestação de serviços.

Vários autores definiram a expressão "Sociedade da Informação". Segundo Nazareno (2006). O conceito de Sociedade da Informação está ligado à "sociedade que recorre predominantemente às tecnologias da informação e comunicação para a troca de informação em formato digital, suportando a interação entre indivíduos e entre estes e instituições, recorrendo às práticas e métodos em construção permanente". Por sua vez, Nazareno (2006) a definiu como uma nova forma de organização e de produção da sociedade em escala mundial baseada no conhecimento, na educação e no desenvolvimento científico e tecnológico. Para Castells (1999, p. 57):

> (...) uma nova economia surgiu em escala global no final do século XX, chama-se de informacional porque a produtividade e a competitividade de unidades ou agentes nessa economia, em nosso caso de organizações, dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É global porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes estão organizadas em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É rede porque as novas condições históricas a produtividade é gerada e a concorrência é feita em uma rede global de interação entre redes empresariais. É a conexão entre a base de informações/conhecimentos da economia, seu alcance global, sua forma de organização em rede e a revolução da tecnologia da informação que cria um novo sistema econômico distinto.

Neste contexto, a inclusão digital tem sido discutida tanto no cenário nacional quanto internacional, e servido de motivação em vários programas organizacionais no Brasil e em diversos países do mundo. Assim, concebe-se que no geral existe uma exclusão digital causada pela distribuição desigual do acesso às redes de comunicação interativa mediada por computadores conectados à internet e prescrevem-se como soluções democráticas a universalização do acesso a tais redes, principalmente em pequenas empresas, assim como a democratização da informação. Desta forma, a gestão da informação evoluiu rapidamente e passou a ser uma atividade estratégica utilizada por várias organizações.

Tarapanoff (2001, p. 10) diz que "o objetivo primordial da gestão de informação é identificar e potencializar os recursos tecnológicos informacionais de uma organização e sua capacidade de informação, ensiná-la a aprender e adaptar-se às mudanças ambientais". Assim,

o ambiente competitivo exige a redução do intervalo do tempo entre o registro de informações e a disponibilização de informações voltadas para processos de tomada de decisão. A competitividade é explicada por Correa (2000, p. 10) como:

> (...) como uma característica empresarial de organizações que mantêm uma cadeia produtiva ou um setor industrial que mudam com o passar do tempo. Portanto, não se pode dizer que a competitividade global faz parte de tal país. Quando há referências de algum país importa-se em dizer que o fato destas organizações estarem localizadas num determinado mercado, visto que alguns países oferecem melhores condições às empresas que nele se localizam.

Ainda de acordo com o autor, a competitividade implica em duas dimensões, uma ligada à empresa ou à cadeia produtiva, trabalhando com toda tecnologia possível e outra com suas operações desenvolvidas no país que oferecem melhores condições para a execução das operações com maior produtividade. É necessário que se identifiquem as reais necessidades dos consumidores e também verificar como a empresa pode atender estas necessidades. A importância que a empresa dá a estas questões indissociáveis define sua capacidade competitiva, ou seja, sua competitividade.

Essa capacidade que as organizações possuem de competir varia ao longo dos anos e não são raros os exemplos de empresas que perdem tal capacidade e são excluídas do mercado. Assim, pode-se dizer que à medida que elevam-se as vantagens competitivas de uma empresa, cresce também sua participação no mercado. Então se escreve que em uma situação normal de mercado oligopolista, uma empresa só sobrevive enquanto mantém alguma vantagem competitiva sobre seus concorrentes.

Gonçalves (2000, p. 30) aborda que:

> (...) uma organização pode se destacar mais e ser competitiva em um mercado e não o ser em outro, uma das formas de caracterizar uma empresa dita de classe mundial é dizer que ela é capaz de ser competitiva em mercados globais. Para que a organização torne-se competitiva ela deve estabelecer uma estratégia de ação para atuar em mercados locais, regionais ou globais. Quanto maior for o raio de sua atuação, maior será sua capacidade competitiva.

Nonnenberg (1998, p. 20) enfatiza que “a competitividade de uma organização não se define apenas por enfoques estáticos como desempenho de mercado ou eficiência produtiva”. Hoje em dia, pode-se entender por competitividade como uma capacidade da

empresa formular e implementar estratégias concorrenciais, que lhe permitam ampliar ou conservar, de forma duradoura, uma posição sustentável no mercado .

Diante desses fatos é importante salientar que as competências existentes internamente como gestão, produção, recursos humanos e inovação, sobre os quais a empresa possui poder de decisão, são determinantes na competitividade. Porém, é importante também lembrar que:

> (...) “os fatores estruturais como mercado, regime de incentivos e regulação da concorrência, sobre os quais a capacidade de intervenção é limitada, e os fatores sistêmicos, como os macroeconômicos, político-institucionais, legal-regulatórios, infra-estruturais, sociais e internacionais, sobre os quais a capacidade de intervenção é quase nula” (NONNENBERG 1998, p. 21).

Apesar de muita preocupação com a tecnologia da informação, o gerenciamento destas informações tem sido negligenciado por várias empresas, em especial nas pequenas e médias empresas. Este problema é resultante muitas vezes da falta de recursos financeiros, falta de pessoal capacitado, ou até mesmo por desconhecimento das fontes de informações acessíveis, aliando a estes fatores a preocupação com a atividade final.

Os sistemas de bancos de dados são projetados para administrar grandes volumes de informações sobre uma determinada aplicação, provendo um ambiente que seja adequado e eficiente para o armazenamento e a recuperação das mesmas (SILBERSCHATZ et al, 2006).

O termo rede é aplicado quando dois ou mais computadores são conectados. Dois computadores estão interconectados quando podem trocar informações através de algum meio como fio de cobre, fibras ópticas, microondas e satélite (TANENBAUM, 2003). Existem redes de diferentes topologias, a Internet é equivocadamente chamada de a maior rede de computadores que existe, porém, na verdade ela é uma rede de redes (TANENBAUM, 2003).

2.2 SEGURANÇA DA INFORMAÇÃO

Segundo Ramiro (2008 p. 8), é através da implantação de diretrizes, normas, procedimentos e controles adequados que se obtém a segurança da informação, garantindo a operação da instituição, enfrentando as ameaças às quais ela está propensa e preservando a princípios básicos de segurança como confidencialidade, integridade, disponibilidade, irretratabilidade e legalidade, conforme se pode observar através da tabela a seguir:

Tabela 1 – Princípios básicos de segurança

Confidencialidade	É a garantia de que somente pessoas autorizadas previamente possam ter acesso à informação;
Integridade	É a garantia de que alterações indevidas da informação não passem desapercebidas;
Disponibilidade	É a garantia de que a informação estará sempre disponível quando for necessário o seu acesso;
Irretratabilidade	É a garantia que o autor da ação não poderá negar a sua autoria
Legalidade	É a garantia de que todas as operações serão realizadas de acordo com os procedimentos, normas, diretrizes e legislação vigentes.

Fonte: Adaptado de Ramiro (2008)

Com base nesses princípios é possível detectar quais os problemas de segurança a rede corporativa vem enfrentando, sendo mais fácil observar uma ferramenta adequada para prevenção dos riscos e ameaças, impedindo invasões ou perdas de informação nas referidas redes.

2.2.1 Ameaça

É uma possível causa de um acidente indesejado, que caso se materialize pode ocasionar prejuízo à instituição. A meação podem ser classificadas como:

Naturais – decorrem de fenômenos da natureza, tais como: terremotos, enchentes, queda de raios etc.;

Involuntárias – ocorrem devido a acidentes;

Voluntárias – ocorrem de forma proposital.

As ameaças demonstram ao usuário que algo de errado poderá acontecer com a informação que contém dentro da rede corporativa, alertando que alguma providencia deve ser tomada para que as informações sejam corrigidas.

Mediante esse aspecto, Menezes (2006) apresenta em seu estudo uma tabela (Tabela 1) produzida pela Modulo Security Solutions (2003) demonstrando que algumas ameaças como “Funcionários insatisfeitos”, “Vazamento de informações”, “Divulgação de senhas” e “Acessos indevidos” estão entre as principais ameaças para informações dos sistemas corporativos:

Tabela 2 – Ameaças a segurança das informações

Vírus	**66%**
Funcionários insatisfeitos	53%
Divulgação de senhas	51%
Acessos indevidos	49%
Vazamento de informações	47%
Fraudes, erros e acidentes	41%
Hackers	39%
Falhas na segurança física	37%
Uso de notebooks	31%
Fraudes em e-mail	29%

Fonte: o autor baseado em Menezes (2006)

2.2.2 Ativo

É tudo aquilo que tem valor para uma instituição ou pessoa, tal como: computadores, softwares, capacidade de fabricar algum produto ou serviço, imagem, marca, patente etc.

2.2.3 Vulnerabilidade

De acordo com Peixoto (2006) é a fraqueza ou restrição de um ativo que pode ser atacada por uma ou mais ameaças. Vulnerabilidades podem ser classificadas em:

(a) Físicas - tais como estrutura de segurança fora dos padrões exigidos;

(b) Naturais - relativas a com variações da natureza tais como umidade e temperatura;

(c) Hardware - relativas a falhas em equipamentos, tais com fadiga do material;

(d) Software - quando mal instalado, por exemplo;

(e) Mídias - suscetíveis a falhas devido a diversos motivos, dentre eles a radiação eletromagnética;

(f) Comunicação - devido a acessos não autorizados ou perda de comunicação;

(g) Humanas - tais como o não seguimento das políticas de segurança.

2.2.4 Risco

Para Peixoto (2006), risco é a combinação de possibilidade da consolidação de uma ameaça e os resultados do impacto causado por este episódio.

Os riscos são ameaças e vulnerabilidades, que dependendo de sua atuação junto ao sistema ou processo de informação, podem ser considerados altos ou baixos, conforme poderá ser visto com mais ênfase no tópico a seguir, sobre diferentes tipos de vírus, ataques e problemas.

2.2.5 Ferramentas de Segurança da Informação

Um dos problemas mais comuns encontrados nas redes corporativas, está no requisito segurança, pois segundo Soares (1995 p. 448):

> "Segurança são procedimentos para minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos, onde vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém".

São muitas as preocupações relacionadas à segurança, em especial da informação, no que se refere às redes corporativas. Comumente, programas que são lançados com o objetivo de garantir a segurança e impedir ataques e invasões, são os mesmos utilizados como ferramenta para destruir o sistema de segurança dessas redes. Isto constantemente vem limitando a segurança das redes corporativas nos dias atuais e preocupando profissionais que trabalham na área da tecnologia com o objetivo de proteger informações e processos.

Por essa razão é importante observar os programas existentes no mercado, de modo a verificar que os mesmos realmente atendam essas condições e possam de fato garantir a

segurança das redes. No entanto, para que isso seja possível é preciso conhecer os vírus que afetam rotineiramente e drasticamente as redes corporativas.

3 VÍRUS E CODIGO MALICIOSO

3.1 PRINCIPAIS TIPOS DE VÍRUS, ATAQUES E PROBLEMAS

Código Malicioso é um software criado com finalidade de destruir dados sem a intenção do usuário. Podemos mencionar como sendo códigos maliciosos (WANDERLEY, 2005, p. 9):

> Vírus: é um programa capaz de infectar programas e arquivos em um computador. Diversos problemas podem ocorrer, desde travamentos na máquina à perda total dos dados do usuário. Existem vários tipos de vírus como por exemplo: vírus de boot, vírus de arquivo, vírus de macro, vírus de e-mail.
>
> Vermes (worm): é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente dos vírus, os worms não necessitam ser executados para se propagarem. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas existentes na configuração de software instalados em computadores.
>
> Cavalo de Tróia (Trojan Horse): é um programa que além de executar funções para as quais foi projetado, também executam outras funções normalmente maliciosas e sem conhecimento do usuário. Algumas de suas funções são: alteração ou destruição de arquivos, furtos de senhas e outras informações como números de cartões de crédito e inclusão de backdoors para permitir que o atacante tenha controle sobre o computador.

Geralmente os códigos maliciosos é que causam maiores danos as informações em redes corporativas, motivo pelo qual devem ser os que mais devem ser observados quando da PSI.

Borges (2008) destaca que um vírus maligno pode provocar:

- Erros na hora de execução de um programa;
- Baixa de memória;
- Lentidão para entrar em programas;
- Danificação de dados;
- Danificação de drives;

- Formatação indesejada do HD;
- Alocação desnecessária da memória do computador

Em alguns casos, o vírus acaba rompendo todas as possíveis proteções e faz com que haja perca total das informações contidas no computador. Motivo pelo qual conhecer o vírus, identificá-lo e descartá-lo é imprescindível.

3.1.1 Principais Vírus

De acordo com o que já se viu nesse estudo e em conformidade com o que diz Bezerra et al (2009) os ataques a computadores são tipos de crimes virtuais que visam, entre outras coisas, prejudicar computadores alheios. Crimes dos quais todos os internautas correm o risco de sofrer, mas que nem sempre sabem exatamente o que são, como agem e quais danos podem vir a causar aos computadores.

Dentre as [diferentes formas de ataques, o vírus é um dos principais, cujos s]ao pequenos programas de computador criados para causar danos na máquina infectada, apagando dados, capturando informações ou alterando o funcionamento da máquina.

Conforme Serrano (2001) os vírus podem ser classificados em:

Vírus de Boot – tem como característica principal a infecção de códigos executáveis localizados no setor de inicialização das unidades de armazenamento, tanto disquetes, quanto discos rígidos (SERRANO, 2001).

Vírus de Arquivo - têm como principal missão a infecção de arquivos executáveis, geralmente os arquivos de extensão EXE e COM. Podem também infectar arquivos importantes como os de extensão: SYS; OVL; OVY; PRG; MNU; BIN; DRV; DLL, etc (SERRANO, 2001).

Vírus de Macro – atinge o arquivo NORMAL.DOT, que é responsável pela configuração do Word e então a partir de sua contaminação, se torna ultra rápida a infecção de outros documentos, pois a cada vez que se abre ou se cria um novo documento, o NORMAL.DOT é executado (SERRANO, 2001).

3.1.2 Backdoors

Os backdoors são programas que permitem ao invasor retornar a um computador comprometido sem ser notado e sem ter que recorrer às técnicas de invasão. A forma usual de inclusão de um backdoor consiste na adição de um novo serviço ou substituição de um

determinado serviço por uma versão alterada, normalmente incluindo recursos que permitam acesso remoto (através da Internet). (WANDERLEY, 2005, p. 9).

3.1.3 Cavalo de Tróia

Conforme Soares (1995) esse é um tipo de praga digital que, basicamente, permitem acesso remoto ao computador após a infecção. Os cavalos-de-tróia podem ter outras funcionalidades, como captura de dados do usuário e execução de instruções presentes em scripts. Entre tais instruções, pode haver ordens para apagar arquivos, destruir aplicativos, entre outros.

4 FERRAMENTAS DE PREVENÇÃO

4.1 CRITÉRIOS DE AVALIAÇÃO DE ANTI-VIRUS

Dificilmente os usuários conhecem os critérios de avaliação dos antivírus, e são conduzidos por aquilo que eles ouvem ou até mesmo pela campanha publicitária que trata do assunto. Essa dúvida entre os usuários segundo Borges (2008) é bastante comum, pois escolher um bom antivírus requer conhecimento das quais características o usuário está procurando, o que nem sempre se encontra entre ao antivírus mais usados, mais baixados ou mais indicados.

Segundo Borges (2008) a escolha do antivírus deve seguir critérios claros, que mais se adéquam as necessidades do usuário., dentre eles, alguns critérios são fundamentais e estão de acordo com qualquer necessidade, como a frequência de atualizações, devendo ser de uma empresa sólida que permanece já a alguns anos no mercado, realizar suas atividades de combate de maneira rápida e clara sem comprometer o usuário naquilo que ele precisa fazer naquele momento. E, além disso, deve agregar serviços e não retirar ou transferir de versão deve ainda, exigir o mínimo do hardware, podendo então ser rodado nos computadores mais antigos. A AV-Comparatives tem realizado a observação e análise de alguns critérios, onde todos os anos os antivírus são avaliados e o resultado é publicado pela AV-Comparatives. No ano de 2015, a comparação foi a seguinte:

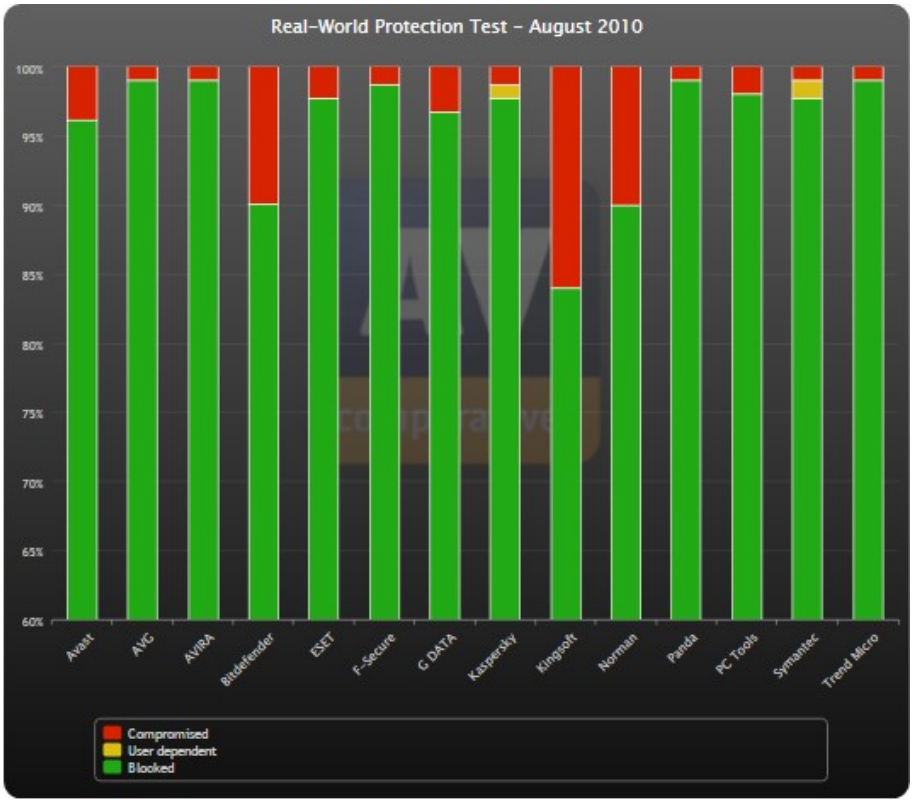


Tabela 1 – Comparativo do antivírus 2010
Fonte: Av-Compartive (2016)

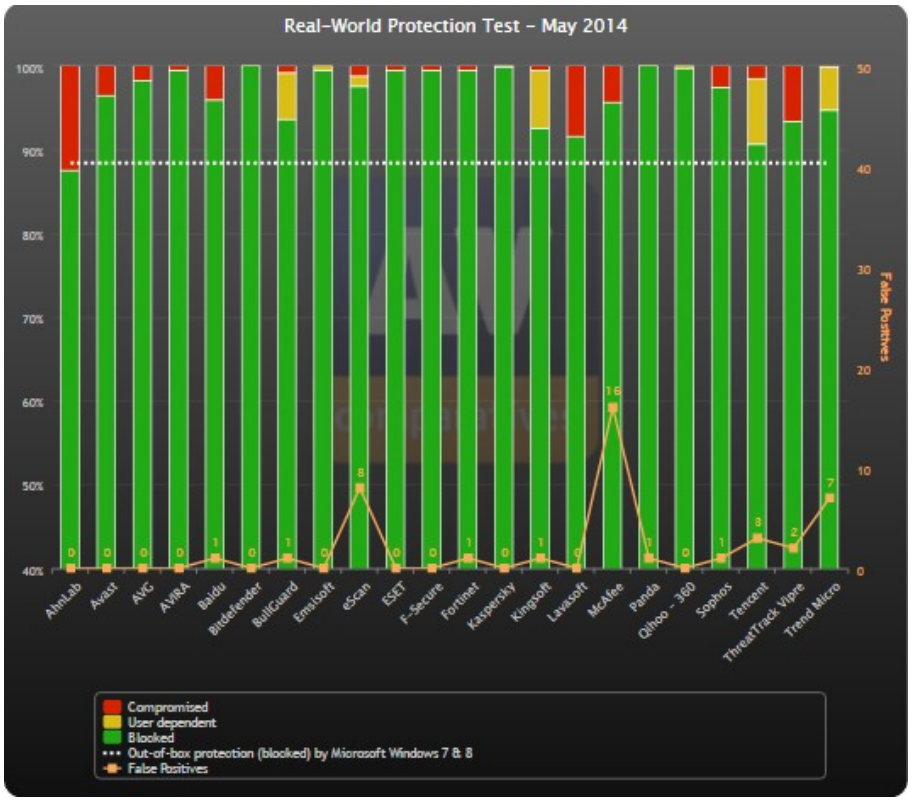


Tabela 3 – Comparativo de antivírus 2014
Fonte: AV-Compartives (2016)

Já no ano passado, a comparação publicada foi:

Tabela 4 – Comparativo do antivírus 2015
Fonte: Av-Compartive (2016)

Percebe-se que em comparação ao ano de 2014 e 2015, o numero de critérios de avaliação de antivírus aumentou e o resultado da análise também foi diferenciado. Em 2010 o AVIRA foi considerado o antivírus que mais se adequava aos critérios recomendados, já no ano de 2015, o Kaspersky e F-Secure passaram a serem os mais indicados. Percebe-se ainda que Avast, eScan e AVG tem melhorado ao longo dos anos e que também são bastante utilizados no momento, apesar de não atenderem a todos os critérios de avaliação.

4.2 **COMPARATIVOS ENTRE OUTRAS FERRAMENTAS**

Conforme alerta Borges (2008) os vírus provocam alterações na performance do sistema e principalmente, costumam alterar o tamanho dos arquivos que infectam. Desta forma, quando da redução na quantidade de memória disponível pode também ser um importante indicador de virose. Para Borges (2008) as atividades demoradas no disco rígido e outros comportamentos suspeitos do seu hardware podem ser causados por vírus, porém, também podem ser causadas por softwares genuínos, por programas inofensivos destinados à brincadeiras ou por falhas e panes do próprio hardware.

Conforme Borges (2008) os antivírus são programas utilizados para detectar vírus num computador, cujo funciona como uma vacina dotada de um banco de dados que cataloga milhares de vírus conhecidos. De acordo com Borges (2008) alguns antivírus são dotados de alguns recursos especiais, tais como:

- Tecnologia Push : cujo atualiza a lista de vírus e ao conectar-se à internet, o micro aciona o software Backweb, que busca automaticamente novas versões da lista de vírus no site da McAfee sem a necessidade do usuário fazer dowloads manuais;

- ScreenScan: varre o disco rígido enquanto o micro está ocioso e funciona da seguinte maneira: toda vez que o screen saver é acionado, o VirusScan entra em ação. Além de não atrapalhar a rotina do usuário, evita a queda de desempenho do PC.

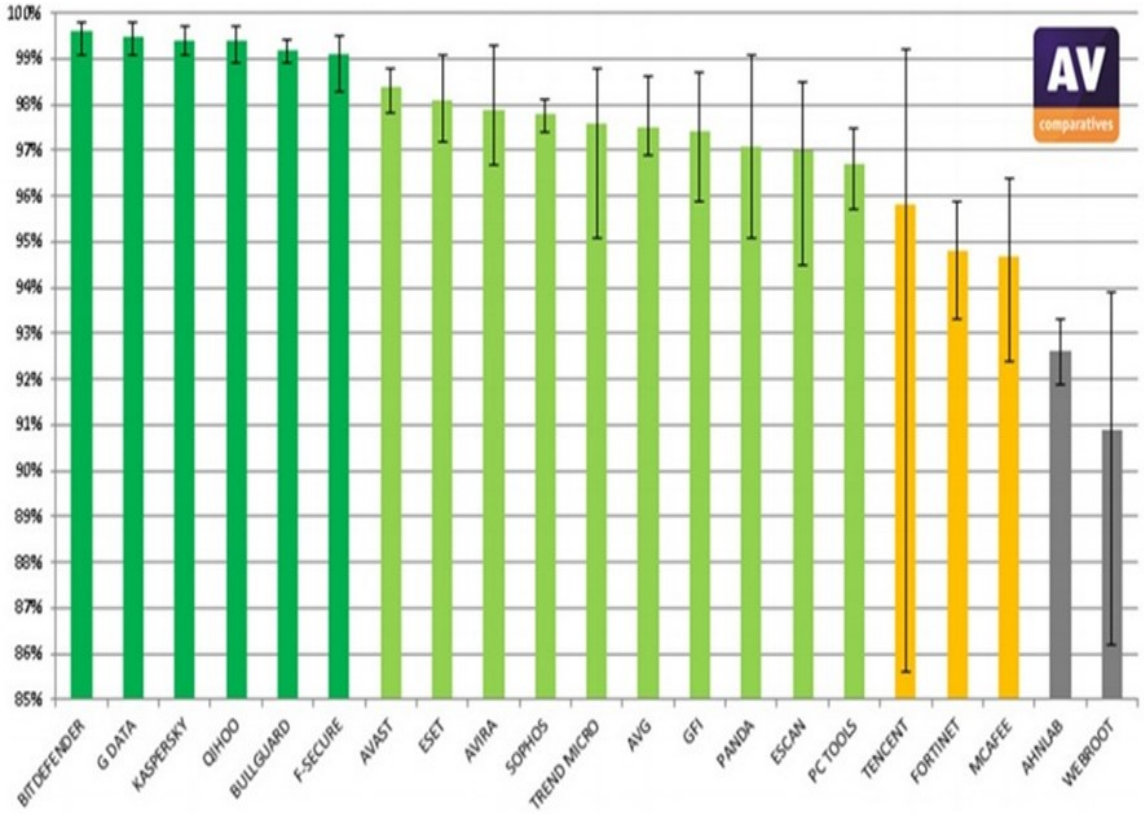
Atualmente existem muitos antivírus no mercado, no entanto, alguns destes não fazem o que prometem ou então acabam diminuindo as chances de contaminação, mas não livram por completo o computador da perca de informações ou outros danos.

Segundo o blog de Paulo Macedo alguns itens que podem ser evitados com a implantação de uma solução corporativa de antivírus são:

- Perda de produtividade;
- Lentidão na execução das atividades;
- Custos com suporte de T.I para desinfecção e reconfiguração do ambiente;
- Perda de competitividade;
- Perda ou roubo de informações;

A Pesquisa abaixo efetuada pela organização não governamental austríaca AV-Comparatives, mostra os principais antivírus existentes no mercado mundial, focando na sua eficiência quanto à proteção.

Todos os comparativos são com as versões pagas. Este gráfico mostra a média de proteção de cada solução, contemplando a mínima e a máxima proteção obtida por cada solução. Conforme o gráfico as soluções da BitDefender, G-Data e Kaspersky contemplam no mínimo 99% de proteção sendo as líderes de mercado.



Fonte: Av-Compartive (2013)

CONCLUSÃO

Esse estudo demonstra que as empresas atualmente utilizam-se das redes corporativas e juntamente com elas sistemas integrados e de informação, sem se preocuparem com a segurança das informações.

Algumas se utilizam de sistemas de segurança internos na empresa, que não envolvem as redes corporativas ou então, utilizam-se de sistemas que envolvem apenas os ataques de hacker e vírus, esquecendo-se da proteção dos usuários.

Porém, notou-se ainda, que existem sistemas de segurança destrutivos e construtivos que podem afetar de maneira negativa ou positiva o funcionamento e a proteção das redes, devendo o usuário optar por aquelas que mais atendam as suas necessidades de segurança.

Os processos, sistemas ou programas de segurança que mais são eficientes para as redes corporativas, especialmente com acesso através da internet, são aqueles que possuem sistema de criptografia perfeita ou IP seguro, que dificultam as invasões e fortalecem assim a segurança das redes e das informações.

Observaram-se ainda que os vírus são o principal motivo de ataques existentes na atualidade e que são em muitos, no entanto, existe uma série de antivírus que podem combater ou reduzir quase que completamente os riscos e ataques através de vírus.

Esse estudo cooperou ainda, para que a prática do gerenciamento de riscos dentro das redes corporativas fosse mais bem interpretada, contribuindo para que os projetos e objetivos da empresa em se tratando de redes corporativas sejam alcançados com eficiência e eficácia.

Através do gerenciamento de riscos, a empresa evita desperdícios tecnológicos, diminui os custos com usuários e programas de segurança remota e os retrabalhos. Além de contribuir para um aumento significativo na produtividade, na eficiência de execução das atividades e no desempenho das redes corporativas, consequentemente, tudo isso, vem a elevar o nível de qualidade dos serviços, da satisfação dos clientes e principalmente da competitividade e da lucratividade da empresa.

Conclui-se, portanto, que a gestão de riscos, através da utilização de programas e sistemas adequados, pode ser tratada em todos os departamentos ou setores empresariais, considerando assim essa estratégia de segurança em redes corporativas como um processo, ligado a todos os setores tecnológicos da organização, especialmente, sendo planejado, executado e controlado, juntamente com os programas de qualidade e eficiência.

Os sistemas específicos para redes corporativas precisam proteger as informações, o acesso e o uso, tanto de fatores internos, como de fatores externos, garantindo assim que a

empresa não seja prejudicada pela falta de segurança e cuidados com a informação, que atualmente, é um dos bens mais preciosos das organizações.

REFERÊNCIAS

BEZERRA et al. Ataques a computadores. Disponível em: http://www.ic.uff.br/~otton/graduacao/informaticaI/Ataques.pdf

CASTELLS, Manuel (ed.). A sociedade em rede, Lisboa, Fundação Calouste Gulbenkian. Vol.III, 1999

KUROSE, J. F., ROSS, K. W. *Redes de Computadores e a Internet: Uma abordagem topdown*. São Paulo: Pearson Addison Wesley, 2006.

GONÇALVES, R. O Brasil e o Comércio Internacional. Transformações e Perspectivas, São Paulo, Ed. Contexto, 2000

LAUDON, Kenneth C.; LAUDON, Jane Price. Sistemas de informação. 4. ed. LTC: Rio de Janeiro,1999. LAUDON, Kenneth C.;

LAUDON, Jane Price. Gerenciamento de sistemas de informação. 3. ed. LTC: Rio de Janeiro,2001

NONNENBERG, M. (1998), Competitividade e crescimento das exportações brasileiras, Rio de Janeiro, IPEA, Texto para Discussão No. 578, agosto.

O´BRIEN, James A. Sistemas de informação e as decisões gerenciais na era da internet. Tradução de Cid Knipel Moreira. São Paulo: Saraiva, 2002.

OLIVEIRA, Djalma de Pinho Rebouças de. Sistemas de informações gerenciais: estratégias, táticas, operacionais. 7 ed. São Paulo: Atlas, 2001.

PADOVEZE, Clóvis Luis. Sistemas de informações contábeis: fundamentos e análise. São Paulo: Atlas, 1997.

PEIXOTO, Mário César. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006

RAMIRO, M. L. Gestão da Segurança da Informação: Certificação Digital. (Tese de Mestrado) Fundação Getulio Vargas, Rio de Janeiro, 2008

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. Sistemas de Bancos de Dados . 5. ed. Tradução de Daniel Vieira. Rio de Janeiro: Editora Elsevier, 2006

SOARES, Fabio. Redes e segurança. São Paulo: Atlas, 1995

STEVENS, W. R. TCP/IP Ilustrated: The Protocols, vol. 1 Massachusetts: Addison Wesley, 2000

STAIR, Ralph M. Princípios de sistemas de informação.Rio de Janeiro: LTC, 1998.

TARAPANOFF, Kira. Inteligência organizacional e competitiva. Brasília: UnB, 2001.

WANDERLEY, Danilo Lustosa. Políticas de segurança. Tese de mestrado. Universidade Federal de Lavras, Lavras/MG, 2005