AMEAÇAS À SEGURANÇA DO CLIENTE DE COMÉRCIO ELETRÔNICO NO BRASIL

Threats to Security Electronic Commerce Client in Brazil

Cristiano Antônio Rocha Silveira Diniz[1]
David Leandro Correia[2]
Geraldo Aparecido Borges[3]

RESUMO
Este artigo tem como objetivo reunir informações sobre as principais ameaças à segurança dos clientes de comércio eletrônico no Brasil. Com a crescente difusão da internet e a criação de novas tecnologias e ferramentas o comércio eletrônico expandiu-se rapidamente originando ameaças tanto para essas ferramentas como para os seus clientes. Trata-se nesse artigo de uma pesquisa do tipo exploratória, que utilizou como técnica a pesquisa bibliográfica.
Palavras-chave: Segurança. Comércio Eletrônico. Ameaças.

Abstract: This paper aims to gather information on the major threats to the security of e-commerce customers in Brazil. With the increasing spread of the Internet and the creation of new technologies and tools e-commerce has expanded rapidly causing threats to both these tools as for their clients. It is in an exploratory research, which utilized as the technical literature article.
Keywords: Security. Electronic Commerce. Threats.

1 - Introdução

O tema deste artigo é uma análise das principais ameaças à segurança do cliente de comércio eletrônico no Brasil.

Considera-se neste estudo como ameaças à segurança do cliente de comércio eletrônico, as ameaças que podem causar danos aos dados e informações que trafegam em redes públicas ou privadas, fazendo com que esses dados sejam modificados, destruídos, expostos ou perdidos (ALBERTIN, 1998).

[1] Especialista em Gestão da Segurança da Informação e Professor do curso de Graduação em Sistemas de Informação pela Faculdade Infórium de Tecnologia. E-mail cristianodiniz@gmail.com.
[2] Graduando em Sistemas de Informação pela Faculdade Infórium de Tecnologia. E-mail dlclegal@hotmail.com.
[3] Graduando em Sistemas de Informação pela Faculdade Infórium de Tecnologia. E-mail geraldo.estudos.trabalho@gmail.com.

Com a rápida expansão da internet e a evolução tecnológica surgiram ferramentas que são utilizadas atualmente em larga escala, entre elas está o comércio eletrônico.

A segurança do comércio eletrônico é vital para a sua sobrevivência, mas ela por si só não protege contra fraudes e extravio de informações pessoais que acontecem regularmente no seu uso. É necessário também que os seus clientes tenham conhecimentos sobre as ameaças existentes para que possam se proteger, fazendo com que o seus acessos e compras pela internet sejam mais seguros e confiáveis.

Segundo uma pesquisa feita pela United Information Systems (UNISYS) com 934 pessoas entre fevereiro e março de 2012, somente 2% dos brasileiros entrevistados confiam nos sites de compras e internet banking, 82% dos entrevistados preferem ir pessoalmente a uma loja ou agência bancária ou realizar a transação por telefone, apenas 8% não se sentem seguros com transações online e apenas 2% confiam no website de seu banco e em sites de compras (CONVERGÊNCIA DIGITAL, 2012).

Delimitou-se o tema deste artigo a uma análise das principais ameaças à segurança do cliente de comércio eletrônico no Brasil.

O objetivo geral é reunir informações que esclareçam sobre as principais ameaças à segurança dos clientes de comércio eletrônico no Brasil. São objetivos específicos: descrever o que representa comércio eletrônico e caracterizar as principais ameaças à segurança dos clientes deste tipo de comércio.

A pergunta de pesquisa é no sentido de investigar quais são as principais ameaças e os riscos envolvidos para o cliente no uso de uma ferramenta de comércio eletrônico.

Este estudo justifica-se tendo-se em vista criar um instrumento detalhado das ameaças existentes oferecendo uma contribuição de consulta que sirva para orientar os clientes de comércio eletrônico assim como usuários da própria internet, porque os mesmos estão vulneráveis às ameaças e muitas vezes não possuem conhecimento acerca destas, assim como os seus métodos de prevenção.

Tendo-se em vista a quantidade de informações pessoais que são extraviadas constantemente na internet, como dados de cartão de crédito, contas de

e-mail e senhas. Esses extravios ocorrem devido a uma série de ameaças existentes como, Vírus, *Worms*, *Trojans*, *Spam*, *Phishing*, Engenharia Social entre outras.

Trata-se de uma pesquisa do tipo exploratória para a qual busca-se apresentar uma base conceitual e teórica sobre o objeto de estudo, utilizando-se como técnica a pesquisa bibliográfica.

2 - Comércio Eletrônico: Visão Teórica

Esta seção apresenta uma abordagem teórica sobre o tema deste estudo, o comércio eletrônico.

Com o avanço da tecnologia e popularização da internet surgiram ferramentas usadas tanto por empresas como por usuários, entre essas ferramentas está o comércio eletrônico que conforme Albertin (2000, p.248) pode ser definido como:

> A realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio. Os processos podem ser realizados de forma completa ou parcial, incluindo as transações negócio-a-negócio, negócio-a-consumidor e intra-organizacional, numa infra-estrutura predominantemente pública de fácil e livre acesso e baixo custo.

O comércio eletrônico está relacionado ao uso de tecnologias e processamento de informações, tal fato pode ser identificado em:

> "Qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços por meio da Internet." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.113).

Esse avanço tecnológico permitiu às empresas que atuam em diferentes setores do mercado contemplassem o comércio eletrônico como uma ferramenta para elevação de lucros, permitindo que seus produtos fossem visualizados a nível global e fazendo com que essas empresas se tornassem mais competitivas (ALBERTIN, 1998).

Outras características impulsionaram a adoção do comércio eletrônico por partes das empresas, segundo Albertin (1998, p. 58):

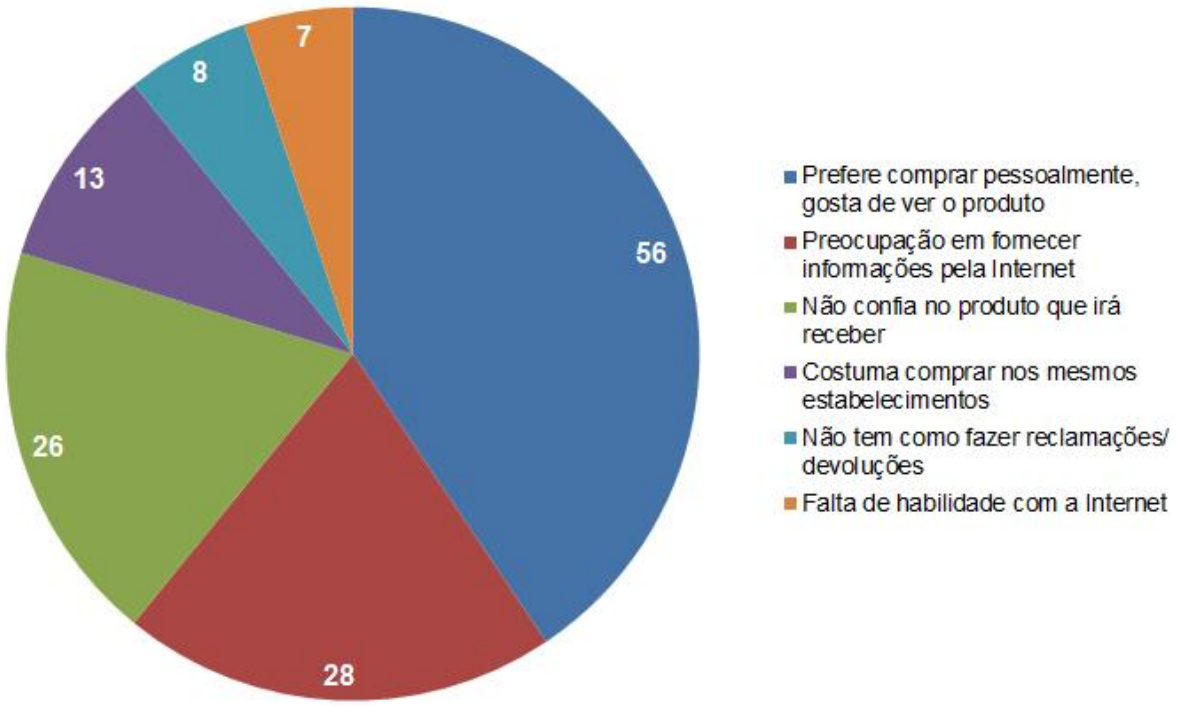
> A penetração global, o baixo custo e o acesso fácil reduzem drasticamente o custo de comunicar uma mensagem para um mercado potencial bastante grande. Em adição, os filtros eletrônicos e os sistemas de suporte a *marketing* direto prontos na Internet estão se

> tornando disponíveis para apoio adicional de recursos direcionados para um vasto mercado global de consumidores.

Já em relação à utilização do comércio eletrônico pelos clientes ainda é possível notar uma resistência no que diz respeito à realização de transações comerciais que utilizam informações pessoais de seus clientes e também da própria empresa como fornecedora do serviço (ALBERTIN, 1998). Tal resistência pode ser observada pela pesquisa realizada pela TIC[1] entre setembro e novembro de 2008, na qual entre os motivos apontados pelos entrevistados no momento de realizar uma compra pela internet, 28% destes afirmaram estar preocupados em fornecer suas informações pessoais na internet (CENTRO DE ESTUDOS SOBRE TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO, 2008).

Na figura 1 apresenta-se um conjunto de dados estatísticos sobre os principais motivos em percentual que influenciaram os brasileiros a não realizar compras pela internet.

Figura1: Relação em percentual dos principais motivos para os brasileiros não terem realizado compras pela internet em 2008.



Fonte: Adaptado de (CENTRO DE ESTUDOS SOBRE TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO, 2008). Elaborado pelo Autor.

[1] TIC DOMICÍLIOS - Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil.

É perceptível na figura 1 a influência que a preocupação do usuário sobre o fornecimento de informações pessoais na internet tem na sua preferência quando o assunto é realizar compras através de ferramentas como o comércio eletrônico.

Todas essas características devem ser levadas em conta no momento da implantação de uma ferramenta de comércio eletrônico por parte das empresas, entretanto também é necessário que as mesmas façam investimentos que suportem este tipo de comércio e também para que possam se diferenciar nesse novo tipo de mercado.

Assim as capacidades das empresas desempenham um papel fundamental na adoção do comércio eletrônico (ALBERTIN, 1998).

Quanto às capacidades de uma empresa Albertin (1998, p.58) afirma:

> [...] as capacidades que permitem a um negócio entregar consistentemente um valor superior para seus clientes, por meio de melhor coordenação e gerenciamento de fluxo de trabalho, customização de produtos e serviços, e gerenciamento de cadeia de fornecimento.

Nesse sentido conforme Diniz (1999, p.79):

> A exploração das vantagens dos sistemas de comércio eletrônico exigirá grande esforço por parte das organizações que nele se envolverem. O desenvolvimento e implementação de tais sistemas demandará investimentos em recursos humanos com visão estratégica, conhecimento dos processos de negócio, dos sistemas herdados, competência tecnológica e habilidades gráficas.

Com o objetivo de gerar valor para o negócio de uma organização, o comércio eletrônico comparado aos mecanismos de comércio tradicionais se destaca por utilizar e fazer parte das tecnologias e ferramentas disponíveis no ambiente tecnológico, englobando aspectos de segurança tanto para empresas como para clientes, permitindo a ampliação de suas transações comerciais e a obtenção de lucro sobre os investimentos realizados (DINIZ, 1999).

O comércio eletrônico permite a realização dos objetivos de negócio de diversos ramos de atividades, devido a sua acessibilidade e expansão além de requisitar um baixo investimento para a sua implantação, mas também necessita de mecanismos de segurança para proteger as informações que trafegam pelo comércio eletrônico e suas redes relacionadas (ALBERTIN, 1998).

Destaca-se do pensamento de Diniz (1999, p. 81) a respeito da informação: "é a mercadoria mais fácil de ser comercializada eletronicamente, é também a que sofre mais riscos de ser apropriada e adulterada, sem qualquer tipo de controle.".

A segurança desempenha um papel fundamental na proteção da informação porque a mesma pode ser definida como: “[...] a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.” (ABNT NBR ISO/IEC 17779, 2005, p. ix).

Portanto a segurança da informação é vital para o comércio eletrônico porque o mesmo “[...] é vulnerável a inúmeras ameaças de rede que podem resultar em atividades fraudulentas, disputas contratuais, e divulgação ou modificação de informação.” (ABNT NBR ISO/IEC 17779, 2005, p. 59). As ameaças do comércio eletrônico relacionam-se ao acesso a informações confidenciais dos seus clientes, assim existe uma grande preocupação com a segurança dessas informações que trafegam em um site de comércio eletrônico e também na própria internet. Tal preocupação com a segurança no comércio eletrônico é demonstrada conforme afirma Albertin (1998, p.50):

> Os aspectos complexos de segurança, privacidade, autenticação e anonimato têm especial importância para o comércio eletrônico. Confidencialidade, confiabilidade e proteção das informações contra ameaças de segurança são um pré-requisito crítico para a funcionalidade do comércio eletrônico.

Nesse sentido Oliveira (2013, p. 30) afirma que “[...] a segurança da Informação está relacionada com a proteção dos valiosos dados de um indivíduo ou de uma determinada empresa, defendendo a confidencialidade, integridade e disponibilidade da informação”.

Os clientes de comércio eletrônico possuem uma grande preocupação com a confidencialidade das suas informações, tal preocupação pode ser responsável pela não utilização de ferramentas e tecnologias disponibilizadas por essas empresas (ALBERTIN, 1998). Desse modo torna-se importante para empresas e clientes o conhecimento sobre determinados aspectos da segurança da informação, no quadro 1 são descritos os aspectos que envolvem a segurança da informação.

Quadro 1: Relação de aspectos e suas respectivas descrições que envolvem a segurança da informação.

ASPECTOS	DESCRIÇÃO
- Ativo	"Qualquer coisa que tenha valor para a organização." (ABNT NBR ISO/IEC 27001, 2006, p. 2).
- Disponibilidade	"Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada." (ABNT NBR ISO/IEC 27001, 2006, p. 2).
- Confidencialidade	"Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados." (ABNT NBR ISO/IEC 27001, 2006, p. 2).
- Integridade	"Propriedade de salvaguarda da exatidão e completeza de ativos." (ABNT NBR ISO/IEC 27001, 2006, p. 3).

Fonte: Adaptado de ABNT NBR ISO/IEC 27001, 2006. Elaborado pelo autor.

Tais aspectos podem ser violados pelas ameaças existentes, essas por sua vez trafegam livremente pela internet e é de responsabilidade das empresas que fornecem serviços de comércio eletrônico a implantação de mecanismos de segurança com o objetivo de evitar que essas ameaças explorem as vulnerabilidades existentes (ABNT NBR ISO/IEC 27001, 2006).

A quantidade de ameaças existentes na internet coloca em risco o principal ativo de empresas e clientes, a informação, podendo gerar perdas intangíveis. Portanto o conhecimento sobre tais ameaças é de extrema importância para o combate às mesmas. Esse conhecimento torna-se fundamental sendo reforçado em:

> [...] o número de casos de violação da segurança de acesso aos computadores tem crescido 50% ao ano desde 1988, sendo que a maioria dos casos refere-se à violação de e-mail ou entrada nos computadores através dele. (MARTINS, L., GUROVITZ, 1997 apud ALBERTIN, 1998, p.50, p.51).

3 – Comércio Eletrônico: Ameaças

Está seção aborda as principais ameaças à segurança de ferramentas de comércio eletrônico, os clientes das mesmas e usuários da internet em geral, apresentando as motivações que pessoas mal intencionadas utilizam para o manuseio

das ameaças na realização de ataques cibernéticos, além de demonstrar métodos que podem ser utilizados para a prevenção de tais ataques.

Para Albertin (1998, p. 51) “[...] a ameaça de segurança é definida como uma circunstância, condição ou evento com potencial de causar danos em dados ou recursos de rede, na forma de destruição, exposição, modificação de dados, negação de serviço, fraude, perda ou abuso.”.

No quadro 2 busca-se relacionar um conjunto de ameaças que podem afetar informações sigilosas e confidenciais tanto de clientes de comércio eletrônico como de usuários da internet, sem o conhecimento prévio dessas ameaças, informações pessoais são extraviadas e utilizadas de forma ilícita podendo gerar perdas financeiras aos seus donos.

Quadro 2: Relação de ameaças aos clientes de comércio eletrônico e usuários da internet.

(Continua)

AMEAÇAS	DESCRIÇÃO
- Engenharia Social	“Técnicas utilizadas para descobrir informações sigilosas e confidenciais, principalmente em grandes corporações, que podem ser destruídas através de um simples gesto de simpatia ou ingenuidade por parte de funcionários ou colaboradores, mas também muito utilizada para descobrir e solucionar falhas”. (OLIVEIRA, 2013, p. 29).
- Vírus	"É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.24). Para Albertin (1998, p.51) é definido como: “[...] um segmento de código que é replicado através da anexação de cópias de si mesmo nos executáveis existentes. A nova cópia do vírus é executada quando o usuário ativa o programa hospedeiro.”.
- Phishing	"É o tipo de fraude por meio da qual um golpista tenta **obter dados pessoais e financeiros de um usuário**, pela utilização combinada de meios técnicos e engenharia social." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.9).

Pharming	"É um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.11).
- *Spam*	"É o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial E-mail)." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.33).
- *Trojan*	"É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.28). É: “um programa que desempenha uma tarefa desejável mas também inclui funções inesperadas e indesejáveis.”. (ALBERTIN, 1998, p. 51).
- *Worms*	"É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. **Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo** em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.25, grifo nosso). É: “um programa auto-replicante que é autocontido e que não necessita de um programa hospedeiro. O programa cria uma cópia de si mesmo e causa sua execução, não requerendo a intervenção do usuário.”. (ALBERTIN, 1998, p. 51).
- *Bot e Botnet*	"É um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.26).
- *Spyware*	"É um programa projetado para monitorar as atividades de um sistema e enviar as

	informações coletadas para terceiros." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.27).
- *Backdoor*	"É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.28).
- *RootKit*	"É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.29).

Fonte: Adaptado de (ALBERTIN, 1998, p. 51), (CARTILHA DE SEGURANÇA PARA INTERNET, 2012). Elaborado pelo autor.

Estas ameaças constituem um grande risco para a segurança das informações que trafegam pela internet englobando empresas, clientes de comércio eletrônico e usuários da própria rede, elas exploram vulnerabilidades e afetam a integridade, confidencialidade e disponibilidade das informações (CARTILHA DE SEGURANÇA PARA INTERNET, 2012). Nesse sentido "[...] uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.18).

Para Marciano (2006, p. 49) uma vulnerabilidade é definida como: "[...] um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça.".

O quadro 3 relaciona as principais motivações que pessoas mal intencionadas utilizam como base para o manuseio das ameaças existentes e a realização de ataques. Segundo Marciano (2006, p. 51) os ataques podem ser definidos como: "[...] à concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante uma ação deliberada e por vezes meticulosamente planejada".

Quadro 3: Relação de motivações e suas respectivas descrições.

MOTIVAÇÕES	DESCRIÇÃO
- Financeira	"Coletar e utilizar informações confidenciais de usuários para aplicar golpes." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.17).
- Comercial	"Tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.18).
- Ideológica	"Tornar inacessível ou invadir sites que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.17).
- Por poder	"Mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.17).
- Por prestígio	"Vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo." (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.17).

Fonte: Adaptado de (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.17-18). Elaborado pelo autor.

Essas motivações permitem à pessoa mal intencionada direcionar o seu ataque e utilizar das ameaças para prejudicar financeiramente ou moralmente as potenciais vítimas. Tais ataques podem incluir técnicas como: varredura de redes, falsificação de *e-mails,* interceptação de tráfego, força bruta, desfiguração de página e negação de serviço. O uso da internet e de suas ferramentas permitem a realização de múltiplas tarefas de forma rápida e precisa, mas é necessário que se tenha conhecimento sobre os cuidados e preocupações quanto a sua utilização de forma

correta e segura nesse ambiente (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).

No quadro 4 são relacionados os métodos de prevenção assim como o seu ambiente de sua aplicação.

Quadro 4: Relação de métodos de prevenção para clientes de comércio eletrônico e usuários da internet em geral.

(Continua)

APLICAÇÃO	PREVENÇÃO
- Ao efetuar transações bancárias e acessar sites de Internet Banking	Não forneça suas senhas e dados pessoais, principalmente através de telefone, não realize transações bancárias em computadores de terceiros, evite acessar os sites bancários através de links de terceiros, desconfie de mensagens de instituições bancárias as quais você não pertence e revise periodicamente o seu extrato bancário a procura de lançamentos indevidos na sua conta. (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).
- Ao usar navegadores web	Atualize com freqüência o seu navegador, versões antigas do mesmo podem conter vulnerabilidades, seja cauteloso na utilização de cookies e evite a inserção de informações pessoais e não permita que elas sejam memorizadas em navegadores instalados em computadores de terceiros (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).
- Ao efetuar transações comerciais e acessar sites de comércio eletrônico	Não utilize computadores de terceiros para o pagamento de compras, desconfie de preços muito baixos, antes de comprar em site de comércio eletrônico pesquise sobre sua procedência, verifique se o site de comércio eletrônico fornece mecanismos de segurança para o trafego de suas informações e em caso de dúvidas entre em contato com a central do cliente fornecido pela ferramenta (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).
- Ao acessar Webmails	Tenha bastante atenção na estética e ao endereço do webmail que acessa para não ser vítima de *phishing*, configure opções de recuperação de senha, elabore senhas consistentes e fortes (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).
- Ao utilizar o computador	Mantenha o seu antivírus atualizado, cuidado com arquivos com formatos que você não conhece e não instale software ilegal porque

	podem conter vírus (POLÍCIA MILITAR DE MINAS GERAIS, 2014). Tenha cuidado ao instalar plug-ins, extensões e completos de terceiros em seu computador, mantenha os softwares atualizados e faça back-up regularmente de suas informações (CARTILHA DE SEGURANÇA PARA INTERNET, 2012).

Fonte: Adaptado de (CARTILHA DE SEGURANÇA PARA INTERNET, 2012), (POLÍCIA MILITAR DE MINAS GERAIS, 2014). Elaborado pelo autor.

O conhecimento sobre as ameaças e de suas respectivas formas de prevenção permitem uma mudança cultural na utilização de tecnologias e ferramentas disponíveis na internet, além de criar uma base de informações sólidas que tornam a utilização de ferramentas de comércio eletrônico e do próprio uso da internet em um ambiente mais seguro e confiável.

Dessa forma constata-se que uma correta abordagem do comércio eletrônico por parte de clientes e empresas na qual inclui um ambiente mais seguro fornecido por estas e o conhecimento das ameaças existentes e adoção correta dos métodos de prevenção do lado de seus clientes, permitem usufruir dos benefícios do comércio eletrônico com um todo (ALBERTIN, 1998).

4 – Comércio Eletrônico: Discussão

Iniciou-se este estudo contextualizando comércio eletrônico e destacando a relevância da segurança da informação para esta ferramenta, assim como às principais ameaças que envolvem também os seus clientes.

Em seguida justificou-se o interesse pelo tema por meio da relação de ameaças como: Engenharia Social, *spam*, *trojan*, *phishing* e *worms* entre outras.

Assim apresentou-se dados da pesquisa realizada pela Unisys com um conjunto de dados estatísticos sobre a preferência dos consumidores brasileiros quanto à utilização de serviços de forma eletrônica ou tradicional como: comprar diretamente em uma loja física ou utilizar um site de comércio eletrônico, utilizar internet banking ou ir diretamente a uma agência bancária.

As características do comércio eletrônico tais como alcance global, baixo custo e uma alta acessibilidade, tornam esse novo tipo de mercado muito atraente para

empresas de diferentes setores da indústria, mas a existência de barreiras internas e externas dificulta a utilização do mesmo em todo o seu potencial (ALBERTIN, 1998).

A existência de uma barreira cultural na utilização de ferramentas como o comércio eletrônico conforme afirma Albertin (1998), está relacionada com a segurança da informação fornecida por empresas nesse ambiente. Diniz (1999) acrescenta nesse mesmo sentido que há fragilidade na informação deste ambiente. A adoção do comércio eletrônico requer modificações na estrutura de uma empresa através de investimentos em áreas como: Recursos Humanos, Tecnologia da Informação e *Marketing,* estes tipos de investimentos foram ressaltados por Albertin (1998) e Diniz (1998).

A segurança da informação possui aspectos relevantes que devem ser preservados como: confidencialidade, integridade e disponibilidade, tais aspectos e suas descrições podem ser observados no quadro 1. Estes aspectos estão vulneráveis a um conjunto de ameaças existentes no ambiente eletrônico como informado pela norma (ABNT NBR ISO/IEC 27001, 2006). As ameaças por sua vez possuem características comuns entre elas, e podem ser usadas separadas ou em combinação com outros tipos, tais características podem ser contempladas no quadro 2. Como exemplo: o *worms* possui a capacidade de se multiplicar de forma automática ou através da exploração de vulnerabilidades existentes em determinado programa de computador. Tal vulnerabilidade foi definida por Marciano (2006) na seção 3, no caso do *spam* determinado grupo de vítimas poderiam receber *e-mails* contendo arquivos no qual estariam armazenadas outras ameaças como o *worms*, vírus e *trojans.*

Com relação à motivação que sustenta a realização de ataques contra empresas, clientes de comércio eletrônico e usuários da internet em geral, utilizando das ameaças citadas nesse estudo, a mesma nem sempre é explícita e pode partir de diferentes motivações como contemplado no quadro 3 na seção 3. Essas motivações podem estar relacionadas a cunho financeiro no qual, informações pessoais das vítimas como: dados de cartão de crédito e senhas bancárias constituem o alvo principal nos ataques realizados por esses tipos de criminosos. Na motivação comercial geralmente as vítimas são empresas do mesmo ramo de atividade, na qual, tornar inacessível determinado site ou ferramenta do concorrente é um dos objetivos principais.

Na motivação por poder, serviços e ferramentas das empresas alvo podem ser atacados com o objetivo de demostrar que esses por sua vez são falhos e estão vulneráveis a ataques e ameaças, podem ser seguidos de suborno visando corrigir as falhas encontradas. Todos esses ataques e ameaças tanto para empresas assim como para o seus clientes e usuários da própria internet possuem métodos de prevenção e que quando adotados corretamente permitem criar um ambiente seguro para ambos os casos. Tais métodos de prevenção podem ser observados no quadro 4 na seção 3.

Os métodos de prevenção citados neste estudo abordam tanto clientes de ferramentas de comércio eletrônico como usuários da internet em geral, tais métodos vão desde a proteção do computador pessoal até a realização de transações online, sejam elas bancárias ou comerciais.

Destaca-se do comércio eletrônico a importância deste para a elevação dos lucros e alcance global para as empresas, essas por sua vez necessitam fazer investimentos e alterações na sua estrutura organizacional para uma melhor e mais completa adoção do comércio eletrônico, a segurança da informação é um requisito indispensável na sua utilização dessa forma parte dos investimentos devem ser atribuídos a ela.

Com o comércio eletrônico os clientes ganham em agilidade nas compras, variedades em produtos e em preços mais acessíveis em relação às lojas físicas, porém é necessário ter conhecimento das ameaças às quais estão expostos, assim como os seus respectivos métodos de prevenção, para que a utilização não só do comércio eletrônico, mas também de outros serviços e ferramentas disponíveis na internet possa ser feita de forma segura e confiável.

5 – Considerações Finais

Em virtude da evolução tecnológica e consequentemente do surgimento de novas ferramentas como o comércio eletrônico, a sua adoção por parte das empresas trouxe substanciais benefícios para as mesmas, ao mesmo tempo em que requisitou investimentos significativos para que o comércio eletrônico fosse suportado, além de

uma profunda alteração na estrutura organizacional destas empresas para o usufruto de todo o seu potencial.

Entretanto tais benefícios e investimentos foram confrontados pelo surgimento de ameaças presentes tanto no comércio eletrônico como em outras ferramentas e serviços disponíveis na internet. Dessa forma buscou-se reunir informações sobre as principais ameaças à segurança de clientes de comércio eletrônico e usuários da internet em geral, apresentando também um conjunto de métodos de prevenção que auxiliam na proteção de suas informações pessoais que frequentemente estão vulneráveis.

Como sugestão para trabalhos futuros é necessário realizar novas buscas e pesquisas sobre o surgimento de novas ameaças e os seus meios de prevenção para formação de uma base sólida de informações que contribua para a segurança de empresas, clientes e usuários da internet e que sirva como consulta e aprendizado para os mesmos, devido a constante evolução tecnológica.

Referências

ALBERTIN, Alberto Luiz. **Comércio Eletrônico: Benefícios e Aspectos de sua Aplicação.** São Paulo, RAE, v.38, n. 1, p.52-58 Jan./Mar. 1998.

ALBERTIN, Alberto Luiz. **Comércio Eletrônico: Modelo, Aspectos e Contribuições de sua Aplicação.** São Paulo, Atlas, v.40, n. 2, p. 108 Abr./Jun. 2000.

ALBERTIN, Alberto Luiz; MOURA, Rosa Maria. **Comércio Eletrônico: Seus Aspectos de Segurança e Privacidade**. São Paulo, RAE, v. 38, n. 2, p. 49-61 Abr./Jun. 1998.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17779:** Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. [s.l], ABNT, 2.ed, 2005. 120p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. [s.l], ABNT, 1.ed , 2006. 34p.

CARTILHA DE SEGURANÇA PARA INTERNET. São Paulo, 2012, Disponível em: <http://cartilha.cert.br/livro/>. Acesso em: 18 maio. 2014.

CENTRO DE ESTUDOS SOBRE TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO. **TIC DOMICÍLIOS E USUÁRIOS 2008 – TOTAL BRASIL.** Set./Nov. 2008. Disponível em: <http://www.cetic.br/usuarios/tic/2008-total-brasil/rel-ecom-07.htm/>. Acesso em: 20 maio 2014.

CONVERGÊNCIA DIGITAL. **Brasileiro mantém 'pé atrás' com vendas pela Internet,** [s.l.], Maio. 2012. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=30407&sid=4#.UpN_T8Tktu4> Acesso em: 23 nov. 2013.

DINIZ, Eduardo Henrique. **Comércio Eletrônico: Fazendo Negócios por meio da Internet.** [s.l.], RAC, v.3, n. 1, p.72-81 Jan./Abr. 1999.

MARCIANO, João Luiz Pereira. **Segurança da Informação – uma abordagem social.** 2006. Tese (Doutorado) – Universidade de Brasília, Brasília, 2006. Disponível em: <http://repositorio.unb.br/handle/10482/1943>. Acesso em: 19 set. 2013.

OLIVEIRA, Carla Danielle Dias. **Engenharia Social. Segurança Digital,** [s.l.]**,** 10.ed, p. 29-32, abr/2013. Disponível em: <http://www.segurancadigital.info/>. Acesso em: 20 nov. 2013.

POLÍCIA MILITAR DE MINAS GERAIS. **Dicas PM.** Minas Gerais, [entre 1998 e 2014], Disponível em: <https://www.policiamilitar.mg.gov.br/portal-pm/dicas.action/>. Acesso em: 18 maio. 2014.