Segurança da Informação no E-commerce B2C

Information Security in B2C E-commerce

Bryan Batista Cartem

Lucas de Paula Julião

Carlos Henrique Rodrigues Sarro

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana) "Ministro Ralph Biasi"
Americana – SP - Brasil

bryan.cartem@fatec.sp.gov.br, lucas.juliao@fatec.sp.gov.br, carlos.sarro@fatec.sp.gov.br

Resumo.

Este estudo tem como objetivo compreender todo processo que revolucionou a tecnologia, nos fazendo entender toda sua história de forma simples, desde a origem, até a internet que conhecemos hoje. É possível também, a partir das análises e leituras realizadas em fontes acadêmicas, compreender sobre a Segurança da Informação, e o papel importante que ela desenvolve em todos os meios em que se armazena, trata ou transmite dados. Principalmente no período de maior conectividade em nível global, com a pandemia da Covid-19 de 2020. Ademais, é abordado nesse estudo o que é a Segurança da Informação, seus pilares e suas influências, como também, a respeito do E-Commerce, além da sua importância nos dias que vivemos hoje. Contudo, ao fim desta leitura será possível concluir o quão importante

é a Segurança da Informação no mundo do comércio eletrônico, entender as leis que garantem a segurança e privacidade dos usuários e a continuidade do negócio.

Palavras-chave: Segurança da Informação. E-commerce. Informações. Leis.

Abstract.

This study aims to understand the entire process that revolutionized technology, making us understand its entire history in a simple way, from its origins to the internet we know today. It is also possible, from the analyzes and readings carried out in academic sources, to understand about Information Security, and the important role that it plays in all the means in which data is stored, processed or transmitted. Especially in the period of greater connectivity at a global level, with the Covid-19 pandemic of 2020. In addition, this study addresses what Information Security is, its pillars and its influences, as well as, regarding E-Commerce, beyond its importance in the days we live today. However, at the end of this reading it will be possible to conclude how important Information Security is in the world of e-commerce, to understand the laws that guarantee the security and privacy of users and the continuity of the business.

Keywords: Information security. E-commerce. Informations. Laws.

1. Introdução

Este artigo cientifico tem o objetivo de levar os leitores a conscientização através de dados e pesquisas de fontes acadêmicas confiáveis, de que seus dados têm um valor descomunal para empresas no século XXI, a era da informação. E que de forma paralela ao crescimento e inovação tecnológica, surgem alguns riscos potencialmente perigosos e desconhecidos. Que devem ser tratados com prioridade e eficiência. Retratando a história de seu surgimento, contextualizando e comparando com situações atuais.

Logo, ao decorrer do texto será apresentado melhores práticas de segurança no ambiente computacional, que pode ser implantado em qualquer tipo de negócio que possui uma certa relação com dados de terceiros e está no mundo digital. Com base jurídica apontando direitos, benefícios, consequências e um pequeno guia de como realizar essas implantações, para garantir a continuidade dos negócios de forma legal, e protegido do mundo dos ciber-criminosos.

2. Internet

O nome internet deriva da junção de duas palavras de origem inglesa, international network. Traduzindo para o português, rede internacional. Ou seja, a internet é uma rede mundial de computadores interligados que, por meio dela, dados e informações são transmitidos para qualquer usuário que nela esteja conectado. É uma rede de várias outras redes, que consiste em milhões de empresas privadas, públicas, acadêmicas e de governo, com alcance local e global, e que está ligada por uma ampla variedade de tecnologias de rede eletrônica, sem fio e ópticas; é uma rede de conexões globais que permite o compartilhamento instantâneo de dados entre dispositivos.

Vaz (1971) descreve a internet como: “fenômeno social e deve ser vista como tal”. Consequentemente, toda essa inovação gerou um impacto no modo de se comunicar e interagir. segundo Limeira (2003) foi o surgimento das chamadas comunidades virtuais. Muitos autores concordam que as novas tecnologias de informação estão provocando mudanças nas formas de comunicação do homem atual.

Essa tecnologia parece ser antiga, porém, a mesma já existe há 50 anos. No Brasil, essa conexão só chegou nos anos 90. Desde que surgiu, abriu as portas para novos desenvolvimentos tecnológicos que continuam avançando até hoje, transformando o modo como vivemos e nos relacionamos. Há 40 anos, enquanto os principais meios de comunicação eram o telégrafo e o telefone, os computadores eram grandes máquinas que realizavam cálculos e armazenavam

informações. De forma geral, seu uso tinha fins exclusivamente científicos e governamentais.

3. História da Internet

A história da internet tem início no período da Guerra Fria (1945-1991), onde as duas superpotências envolvidas, Estados Unidos e União Soviética, que estavam divididos respectivamente nos blocos capitalista e socialista, disputavam poderes e hegemonias; um embate em termos ideológicos, econômicos, políticos, militares e tecnológicos. Devido ao conflito, os Estados Unidos buscavam uma maneira eficiente de proteger suas informações e comunicações no caso de um ataque nuclear soviético. As inovações que tentaram resolver esse problema levaram ao que se conhece hoje como Internet. Dessa forma, no início foi pensada como uma ferramenta de comunicação militar, onde as informações passariam divididas em pedaços para serem entregues com mais velocidade.

Segundo Reedy, em agosto de 1962 se deu a primeira descrição registrada através de networking, na qual J. C. R. Licklider, do MIT (Massachussets Institute of Technology) discutia o conceito de "Rede Galáctica". Ele previu um meio pelo qual um grupo de computadores, no qual todos pudessem acessar de maneira rápida dados e programas de qualquer local.

Em 1969, com uma comunicação entre a Universidade da Califórnia e um centro de pesquisa em Stanford, com base neste conceito foi criada pela DARPA1, uma rede experimental de computadores, chamada ARPANET (Advanced Research Projects Agency Network). Esta, conectava entre si quatro universidades americanas, o que permitia que cientistas dividissem informações a longas distâncias. Entre 1980 e 1990, a internet deixou de ser uma ferramenta usada somente pelo governo e passou a ser utilizada para fins acadêmicos. O formato atual que a internet apresenta, segundo Castells,

também resulta de uma tradição de base de formação de redes de computadores. Ademais, a Arpanet não foi a única responsável.

Nesse período compreendido entre 1990 e 2000, devido ao grande número de usuários, fez se necessário a transferência para instituições não governamentais, para que se encarregassem de estabelecer padrões e regras durante a utilização da internet. Em meio a essa época o Brasil tomou as primeiras iniciativas para tornar a Internet disponível a todos, projetando e implantando a infraestrutura necessária.

"A internet (ou a "Rede" como também é conhecida) é um sistema de redes de computadores interconectadas de proporções mundiais". (DIZARD, 2000, p. 24). De acordo com o canal de notícias Globo, os usuários de banda larga fixa no início do ano eram de 36,3 milhões, e fechou 2021 com 41,4 milhões de conexões, um crescimento de 14%. Superando o de 10% entre os anos de 2019 e 2020. Entretanto, no ano de 2022 aproximadamente 33 milhões de brasileiros ainda não possuem acesso à internet.

4. **O que é a segurança da informação?**

Segurança da informação é o estudo, a prática de políticas e técnicas que asseguram com que os dados e informações importantes fiquem livres de ameaças, sejam elas físicas ou lógicas. E "... deixando claro para todos os usuários que acessam e usam a informação, qual é a filosofia da organização sobre esse recurso, visando assegurar que toda informação da empresa e de seus clientes esteja protegida contra possíveis perdas, danos, destruição e/ou mau uso" (FONTES EDUARDO, 2006, p.25). Por conseguinte, a segurança da informação tem como objetivo preservar o valor que os dados, ou as informações possuem para um indivíduo ou uma organização.

As propriedades de base da segurança da informação são: confidencialidade, integridade, disponibilidade e autenticidade. Disponibilidade, é o princípio que garante a disponibilidade daquela informação sempre que for necessário. Integridade, que diz respeito a

informação ser alterada somente por quem tem autorização para alterá-la, impedindo que pessoas não autorizadas façam quaisquer modificações. Confidencialidade, garantia total do sigilo da informação, sendo exposta somente a pessoas autorizadas. E por fim, o princípio da autenticidade, que garante a veracidade das informações, como também, o não repúdio

De acordo com Silva et al (2003), as teorias e consequente aplicação do termo segurança dos sistemas de informação iniciou-se com os próprios técnicos que, após criarem os sistemas, verificaram a transição para gestores e outros usuários, como também a crescente utilização dos meios das redes de computadores, despertando a necessidade de assegurar estas propriedades devido a conectividade, oriunda da evolução tecnológica.

Entretanto é notório que a evolução da Tecnologia da Informação trouxe consigo algumas brechas de segurança, são essas chamadas de vulnerabilidades, que podem ser exploradas por um agente mal-intencionado e causar prejuízos consideráveis. Em razão disso, hoje se vê muito falar em segurança, como também, a Lei Geral de Proteção de Dados. Essas são as principais preocupações para as organizações, independentemente de seu tamanho, ter suas informações e informações de terceiros dentro dos princípios de segurança da informação é obrigatório para a continuidade do negócio e segurança de todos. Visto que, a informação no século XXI possui maior valor quanto qualquer outro ativo na empresa, e é de certa forma a base de sua sobrevivência.

Logo, analisando o real panorama e o avanço das tecnologias, fica evidente a necessidade da implantação de políticas de segurança para as organizações, utilização das boas práticas como por exemplo, ITIL e Cobit; ademais, um plano estratégico. Caso contrário o prejuízo para a organização será significativo.

5. Definição do E-commerce

De maneira concisa, o E-commerce é uma comercialização de produtos, serviços ou bens a qual é realizada a distância, precisamente através de tecnologias eletrônicas, que ao contrário do que muitos pensam nem sempre estão conectadas à internet. O e-commerce cresceu ainda mais com a chegada da internet, em meados de 1970, facilitando e automatizando cada vez mais o processo de pesquisa, compra e venda.

"O termo e-commerce descreve uma ampla variedade de transações eletrônicas, como: o envio de pedidos de compra para fornecedores, o uso de fax e e-mail para conduzir transações, o uso de caixas eletrônicos e cartões magnéticos para facilitar o pagamento e obter dinheiro digital, assim como, o uso da internet e serviços on-line. Tudo isso envolve fazer negócios no espaço de mercado, em vez do mercado físico." (Kotler, 2000, p.681)

Para ROWSOM (1998, p. 104) e GRAHAM (2000, p.56) o e-commerce é mais do que uma simples transação eletrônica de bens e serviços, inclui todos os tipos de esforços de pré-venda e pós-venda, assim como conjunto de atividades auxiliares, como novo enfoque para pesquisa de mercado, geração de conduções qualificadas de vendas, anúncios, suporte a cliente e distribuição de conhecimento.

Ademais, o e-commerce abrange uma gama enorme de diferentes tipos de negócios, desde sites destinados a consumidores (B2C, Bussiness to Consumer), serviços (B2B, Business to Bussiness), bens, organizações ou leilões. Ele permite com que todos os interessados realizem transações eletrônicas a qualquer momento, independente do dia, horário ou lugar. Dessa maneira, este tipo de negócio (digital), possibilita atender uma grande quantidade de consumidores, estejam eles perto ou longe de sua localidade. Diferente da loja física, que possui dias, horários, e determinados limites.

6. Segurança no E-commerce

Embora o e-commerce traga tantos benefícios a todos, ele também traz riscos ao negócio e ao empreendedor. Devido ao crescimento do acesso à

internet, a maioria dos empreendedores tem seu e-commerce em domínios na internet, que por sua vez podem ser acessados por pessoas de qualquer lugar do mundo. Desse modo, quanto mais conhecido ou visível seu negócio é, mais suscetível ele está de ser um alvo de pessoas má intencionadas; denominadas Crackers ou Hackers de chapéu preto, pela comunidade de Tecnologia da Informação.

Segundo Bruno Fraga (2019), os Hackers de chapéu preto, são indivíduos que geralmente possuem um amplo conhecimento sobre a invasão de redes de computadores e a ignorância de protocolos de segurança. Podem variar de amadores ao espalhar um vírus, a hackers experientes que visam roubar, modificar ou destruir dados, especificamente informações financeiras, pessoais ou credenciais. Sua principal motivação geralmente é para ganhos pessoais, como financeiro, mas podem também ser viciados na emoção do cibercrime.

De acordo com o site de notícias Uol, o Brasil é o 5º (quinto) maior alvo global de ataques de hackers. Principalmente com a chegada da pandemia do novo coronavírus (COVID19), que teve início em 2019, e obrigou os países do mundo inteiro a entrar em estado de quarentena por dias e até mesmo meses, afetando toda a economia e favorecendo ainda mais o cenário para esses atacantes. Pois, como a civilização estaria em casa, teriam que arranjar alguma maneira de continuar a se sustentar, logo, também houve o crescimento do e-commerce. Ademais, apenas nos últimos 4 (quatro) meses de 2021, o Brasil lidou com mais de 95 milhões de ataques de Malware. Isso devido à falta de conhecimento básico da população de como navegar na internet com segurança, como também, a escassez de profissionais qualificados no mercado para atender a alta demanda das vagas em aberto.

"... foi feito através da plataforma Toluna com 1.000 brasileiros questionando sobre a segurança dos dados online. Na pesquisa, 48% dos entrevistados afirmaram que deixariam de comprar em uma empresa se descobrissem que o site já sofreu ataques cibernéticos". Já em outra pesquisa, "72% afirmaram que evitam fazer negócios com lojas virtuais que não tenham

domínio de e-mail próprio. Entre os respondentes, 39% disseram que confiam mais em comprar no aplicativo da loja do que no site." (Ecommerce Brasil, 2021).

7. O que é a LGPD?

Ao passar do tempo, o mundo dos negócios foi impactado pela transformação e inovação tecnológica no Brasil e no mundo; este novo cenário levou empresas a seguir o mesmo caminho, levando suas operações para o meio digital da maneira que possível, além de colocar a empresa ao lado das demais na questão de tecnologia e competitividade. Este novo cenário teve diversos impactos na vida da população também, dentre eles, a facilidade para os consumidores, deixando tudo mais prático e confortável realizar tais ações pela internet.

Em uma loja virtual, há vários dados pessoais armazenados, principalmente dados sensíveis, como é o caso do CPF (Cadastro de Pessoa Física), por exemplo; durante uma compra, em um site da internet, o consumidor deixa muitas informações além do CPF, como, números de cartões, endereços, preferências, dados de navegação, e muitos outros. E poucos sabem o que acontece com suas informações após um cadastro.

Em face do exposto, foi criada a Lei Geral de Proteção de Dados — Lei 13.709/2018. Entrou em vigência em agosto de 2020; sua ideia é proteger a privacidade, dados e informações pessoais dos que navegam e consomem através da internet, mudando a forma de lidar com as informações dos seus titulares. Devido a esta lei, é necessário "mexer os pauzinhos" no que diz respeito ao armazenamento, tratamento e transmissão de dados, reforçando as questões das áreas em geral, mas principalmente de segurança da informação e tecnologia. Considerando os pilares de segurança, privacidade e transparência.

De forma direta, o objetivo da LGPD é garantir a Segurança de dados pessoais que são deixadas na internet, de forma que os consumidores e proprietários dos dados saibam como seus dados, são armazenados pelas

empresas, com quais outras empresas elas compartilham, como tratam, compartilham e utilizam esses todos esses dados.

8. Por que o e-commerce precisa se adequar à LGPD?

Em razão aos escarcéus com vazamentos de dados nos últimos anos, tanto negócios B2C e B2B, como por exemplo o vazamento do Facebook da empresa Meta, que expôs mais de 1,5 bilhões de dados dos usuários; e Serasa, com de mais de 223 milhões de CPFs vazados, e entre muitos outros. Pode se dizer que o motivo desses desastres foram justamente a falta de uma boa política de segurança da informação, que contém um procedimento adequado sobre como tratar e proteger esses tipos de dados. Logo, muitas empresas vendem dados pessoais e dados que revelam o gosto de seus clientes para outras organizações, a fim de gerar mais receitas enviando em teoria um anuncio perfeito, que vai de encontro ao desejo do potencial consumidor.

As empresas que tratam dados de pessoas físicas devem estar adequadas a essa lei, evitando assim multas altíssimas, sansões e concedendo a ANPD bloquear ou até mesmo eliminar os dados que são tratados pela empresa, e que violam a lei. Impedindo a continuidade do negócio.

É perceptível a preferência dos clientes por organizações confiáveis e transparentes, pois tem conhecimento de grande parte do que acontece. Desse modo, empresas que fazem a implantação da LGPD ganham mais notoriedade, confiança e boa reputação por parte de seus clientes e clientes em potencial.

9. Tipos de dados protegidos pela LGPD?

Segundo o site do governo brasileiro, o dado pessoal é aquele que possibilita a identificação, direita, ou indireta da pessoa natural. E são eles: nome e sobrenome; data e local de nascimento; RG; CPF; retrato em fotografia; endereço residencial; endereço de e-mail; número de cartão bancário; renda; histórico de pagamentos; hábitos de consumo; dados de localização, como por

exemplo, a função de dados de localização no celular; endereço de IP (protocolo de internet); testemunhos de conexão (cookies); número de telefone.

Caso o proprietário dos dados deseje saber quais são os dados que a empresa possui a seu respeito o mesmo pode solicitar, ou caso não se sinta mais confortável em ter seus dados no sistema da companhia, também possui o direito de pedir a exclusão permanente. Visto que dados pessoais são bens intangíveis, e a organização não pode ter dados além do que ela precisa para seus determinados fins. Qualquer pessoa que se sentir lesada por uma empresa no que diz respeito aos seus dados pessoais, tem o direito de processá-la com base na LGPD.

10. Dados sensíveis e não sensíveis.

Além dos dados pessoais citados acima, há mais dois tipos de categorias, são elas as de dados sensíveis e dados públicos. Dados sensíveis revelam o indivíduo de maneira mais profunda como origem racial ou étnica, religião ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e até mesmo sobre a saúde ou a vida sexual. O tratamento desses dados depende totalmente do conhecimento explícito do proprietário e com um fim definido. E só poderá usar sem o conhecimento do indivíduo em casos de obrigações legais. Já os dados públicos são dados que possuem um interesse público e são tratados com boa-fé, podendo ser tratado sem precisar de concentimento. Entretanto, em casos de compartilhamento a organização deverá pedir outro concentimento para realizar tal ação com outras entidades.

11. Como implementar a LGPD em seu e-commerce.

Para se adequar a LGPD é recomendado que faça um mapeamento de todas as áreas e ativos que tem contato com os dados que a Lei Geral de Proteção de Dados se assegura de vistoriar. Neste momento pode-se promover mudanças necessárias ao processo, proporcionando maior eficiência e

modernidade a empresa. Uma vez que estes processos estão sendo esmiuçados, surgem diversas oportunidades de melhorias que não haviam sido pensadas anteriormente ou não eram prioridade. Outra vertente da implementação e regularização é o descarte de qualquer tipo de dado pessoal que não é usando pela organização, a fim de evitar futuros problemas e levantar suspeitas.

12. Como fortalecer a segurança de um e-commerce.

Para fortalecer a segurança de um E-commerce, é necessário que haja cuidados a serem aplicados com frequência; através sesses cuidados, é possível diminuir as chances de invasões, danos prejudiciais aos consumidores, e ao comércio.

Um dos principais cuidados a serem tomados, é ter um método seguro de pagamento, considerando o fato que em 2022 a tentativas de fraudes em e-commerces cresceram em 23,6%, ter um meio de pagamento seguro é tão importante quanto escolher os produtos que serão oferecidos pelo e-commerce, já que para finalizar a compra de um determinado produto, o consumidor precisa se sentir seguro para inserir seus dados pessoais. Com tudo, é importante que o empreendedor pesquise meios de pagamentos, os mais usados, levando em conta os pós e contras; ou até mesmo estabelecer suas próprias políticas de pagamentos, privacidade, devolução e troca, deixando essas regras transparente na plataforma, e não escondida.

Uma dica para esta etapa, é a implantação de um certificado digital, o mesmo é similar a um documento, ele é válido para identificar a autenticidade do seu negócio e te permite assinar documentos com o mesmo valor de uma assinatura a punho. E junto ao certificado digital, o TLS (Transport Layer Security), uma vez instalada, ele pode garantir a proteção, privacidade e autenticidade das transações de dados entre o servidor e o usuário, através da criptografia. Garantindo que ninguém além do consumidor e o empreendedor tenha acesso.

Deste modo, escolher uma plataforma confiável, utilizar senhas fortes, investir em profissionais que possam desenvolver, e aprimorar a rede de forma segura, investir em auditorias, manter atualizado as dependências de softwares do comércio eletrônico, também são métodos simples que, quando aplicados, diminuem drasticamente às chances de consequências que podem levar uma empresa a falência.

13. Considerações finais

Contudo, com base das pesquisas realizadas em fontes acadêmicas e confiáveis, dos dados de fraudes causados pela falta da segurança da informação, pode-se concluir que a segurança da informação, diferente do que muitas empresas enxergam, não é um gasto a mais para o comércio, mas sim, um investimento, que, quando aplicado, assegurará o tanto o empresário como o consumidor final, o qual necessita de se sentir seguro para realizar uma compra via internet, trará mais credibilidade para a empresa, além de evitar sérias consequências e dores de cabeças para o empreendedor.

Considerando o fato do quão importante é mostrar na plataforma quais são os métodos de segurança implantados e utilizados na empresa, se possui ou não certificado TLS, quais são as políticas de segurança utilizado por aquele comércio, manter a transparência, afirmando ou não a capacidade de garantir os três pilares indispensável da segurança da informação: A confidencialidade, integridade e a disponibilidade.

14. Referências

MANCILLA, Omar. A importância da Internet para o Desenvolvimento das vendas no Brasil (Administração) 35 p. Instituto Municipal de Ensino Superior de Assis.

MARQUES, Luciana. A Importância do E-commerce como ferramenta de Marketing. (Graduação em Administração – A distância) 50p. Universidade de Brasília.

FRAGA, Bruno. Técnicas de Invasão: APRENDA AS TÉCNICAS USADAS POR HACKERS. Labrador, 2019.

CONTENT, Rock. Conheça a história da Internet, sua finalidade e qual o cenário atual: Nascimento da World Wide Web. 27 jan. 2020. Disponível em: https://rockcontent.com/br/blog/historia-da-internet/. Acesso em: 18 jul. 2022.

DIANA, Daniela. História da Internet. Toda matéria. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 12/08/2022

FONTES, Edison. Praticando a Segurança da Informação. São Paulo. Editora Brasport, 2008.

FONTES, Edison. SEGURANÇA DA INFORMAÇÃO. São Paulo. Editora Saraiva Educação SA, 2017.

GOVERNO. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasil, 2018. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em: 19 ago. 2022.

BRASIL. [Constituição Federativa do Brasil (2018)]. Lei Geral de Proteção de Dados Pessoais (LGPD).

7 casos de vazamento de dados em empresas de varejo. Disponível em: https://www.aser.com.br/7-casos-de-vazamento-de-dados-em-empresas-de-varejo/. Acesso em: 16 jul. 2022.

REDAÇÃO ONCLICK. Como preparar o seu e-commerce para a LGPD. Disponível em: https://onclick.com.br/artigos/lgpd-e-e-commerce-como-adequar-sua-empresa. Acesso em: 27 ago. 2022.