UNISUL

SEGURANÇA EM COMÉRCIO ELETRÔNICO

MARCELO ESPÍNDOLA

RESUMO

O presente trabalho tem por objetivo mostrar os problemas mais comuns decorrentes no comércio eletrônico. Com isso, foi realizada uma pesquisa na literatura visando destacar os ataques mais comuns sofridos pelos consumidores e fornecedores, além de os principais meios de prevenção desses ataques. Através desta, pôde-se observar que, dentre os problemas mais recorrentes no comércio eletrônico estão, os ataques por Ddos*, Cross-site Scripting* ou XSS, *Cross-site RequestForgery* (CSRF), *Eavesdropping*, SQL *Injection*. Todavia,a fim de garantir confiabilidade, deve ser implantado alguns mecanismos para garantir a segurança dos usuários que utilizam a Internet para realização da algum tipo de transação eletrônica, como: Autenticação, transação eletrônica segura, criptografia e firewall.

PALAVRAS CHAVES

Comércio eletrônico, Ataques mais sofridos, Segurança.

1.INTRODUÇÃO

Comércio eletrônico é o nome dado ao processo pelo qual é possível realizar transações financeiras através do uso da internet. Essas transações podem dar-se por três diferentes meios, sendo estes: empresa e consumidor, empresa e empresa, ou ainda, intra-organizacional. Sendo que para todos os casos, estas transações podem ser de ordem regional, nacional ou mundial (TURBAN, E.; KING, D. 2004; FAGUNDES, E. M. 2004).

Destaca-se no comércio eletrônico a alta versatilidade com que este se apresenta ao usuário. Uma vez que sem sair do seu local de conforto, tem-se a viabilidade de realizar compras, vendas, conhecer produtos novos e realizar pesquisa de preços. Além disso, através desta ferramenta, é possível efetivar serviços bancários, como, transações, pagamentos, investimentos e transferências, a qualquer horário sem se deslocar da sua

casa ou do seu local de trabalho, aumentando assim, além do conforto, a integridade física do usuário.

Apesar de todas as vantagens apresentadas pelo comércio eletrônico, este também apresenta seus reveses, sendo o principal deles, o ataque cometido por *hackers*, deixando assim muitos usuários desconfiados quanto a seguranças de realizar transações comerciais por meio da internet. Com isso, visando conferir uma maior segurança no comércio eletrônico, com o passar dos anos ocorreram numerosas modificações na maneira como se dá as transações eletrônicas, gerando como melhoria direta, a tecnologia da informação e a comunicação, para articular diretamente fornecedor e consumidor.

A pesquisa foi realizada a fim de identificar os problemas mais recorrentes que acontecem no comércio eletrônico. Visando com isso, reunir informações que permitem identificar quais os tipos de ataques mais comuns sofridos, apontar quais os problemas que mais ocorrem na rede de comércio eletrônico na hora de efetuar compras, vendas e transações na rede, e analisar quais os mecanismos de defesa mais importantes para o desenvolvimento do comércio eletrônico.

Após identificar quais os ataques mais comuns sofridos pelos usuários em rede, faz-se importante, saber como prevenir-se dos mesmos. Com isso, conhecer os principais mecanismos de defesa torna-se essencial para tornar o acesso as lojas e estabelecimentos seguro. Assim sendo, é necessário reunir informações a respeito do funcionamento dos principais mecanismos de defesa com a finalidade de se prevenir contra ataques maliciosos sofridos na rede, e garantir um acesso seguro aos usuários da internet.

Fazendo-se valer do conhecimento dos ataques e problemas mais comuns, e dos principais meios de defesas de prevenção, é possível correlacionar causa-consequência e solução, podendo apontar qual a melhor maneira de se prevenir de um dado problema. Tornando assim, o comércio eletrônico um ambiente seguro e confortável para seus usuários.

2. PROBLEMAS MAIS COMUNS QUE OCORREM NO COMÉRCIO ELETRÔNICO

Um dos problemas mais comuns que ocorrem no comércio eletrônico é a forma de se preservar os dados dos consumidores. Todavia esses dados podem ser roubados e usados de má fé, como por exemplo fazer *spam* (envio de e-mail sem permissão para vários destinatários) (FAGUNDES, E. M. 2004). Com esses dados, os *hackers* podem se passar pelo consumidor e efetuar diversas transações como: compras, saques, pagamentos.

Ainda como problema decorrente, temos os virus que ameaçam e tiram o sono de qualquer comerciante digital. Outra adversidade é a invação de sites, na qual é feita a troca ou inserção de algumas informações, a mudança de valores de produtos ou serviços, levando a perda de credibilidade e prejuízo para o seu proprietário.

3. ATAQUES MAIS COMUNS DECORRENTES NO COMÉRCIO ELETRÔNICO

O comércio eletrônico cresceu consideravemente nas últimas decadas, e com ele os ataques em sites se tornaram cada vez mais recorrentes. Visando encontrar maneiras de se proteger desses assédios, conhecer as principais formas como estes ocorrem torna-se uma ferramenta indispensável no combate e proteção dos golpes na internet. Assim sendo, estão listados abaixo, os tipos de ataques mais comuns sofridos pelos sites de comércio eletrônico:

- *DDos*
- *Cross-site Scripting ou XSS*
- *Cross-site Request Forgery (CSRF)*
- *Eavesdropping*
- *SQL Injection*

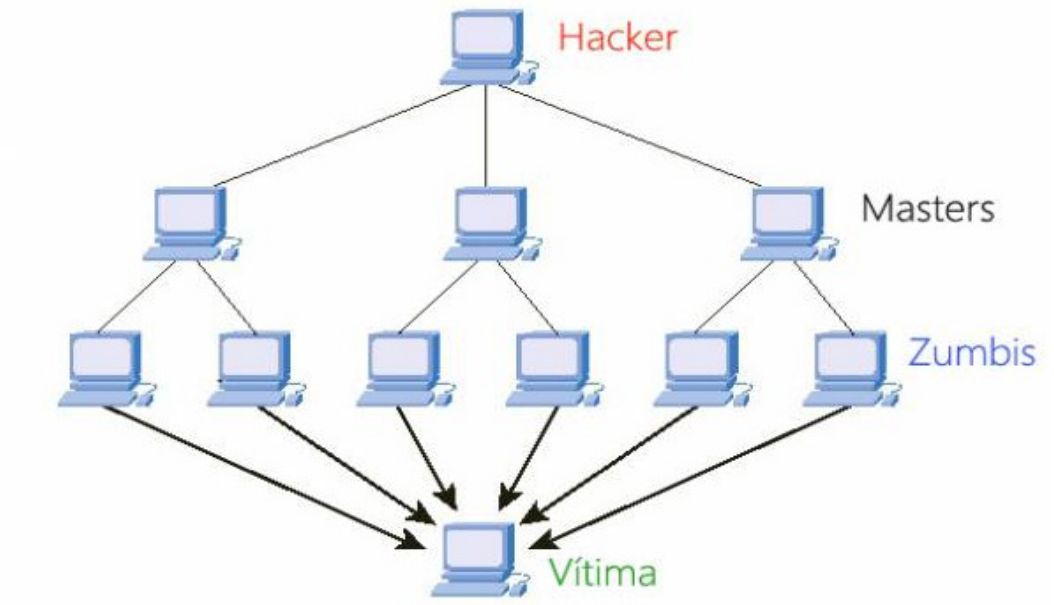
A fim de compreender essas formas de ataques cada uma delas será apresentadas e discultidas separadamente nos paragrafos seguintes.

3.1. DDos, ataque de negação de serviço

Segundo TURBAN, (2004, p. 322) No ataque de negação de serviço, é utilizada uma técnica de envio de várias solicitações de pacotes a um determinado computador ou servidor, fazendo com que os mesmos se tornem sobrecarregados e indisponíveis ao usuário. Com essa sobrecarga, o utilizador não consegue mais acessar o host, deixando o mesmo vunerável para as respostas das solicitações.

O alvo mais comum são servidores web, nesse ataque os computadores mestres gerenciam diversos outros computadores chamados zubis (figura 1). Contudo esse computador mestre submete várias máquinas a acessar um determinado recurso a um estipulado serviço, todos ao mesmo tempo. Sendo assim, de maneira constante, os zubis acessam ligadamente o mesmo recurso de um servidor. Como servidores web tem um restrito número de acesso simultâneo de usuários ao mesmo tempo, fica impossibilitado de atender aos pedidos, fazendo com que o mesmo fique travado ou reiniciando.

Figura 1: esquema do funcionamento do ataque DDos



CANAL TECH disponível: <https://canaltech.com.br/o-que-e/o-que-e/O-que-e-DoS-e-DDoS/> pagina 1

3.2.Cross-site Scripting ou XSS,

O *cross scripting* ou XXs traduz uma instabilidade procriada pela falha nas aceitações dos parâmetros de entrada do usuário e resposta de um servidor web. Esse

ataque faz com que o código HTML seja introduzido de forma desnecessária no navegador alvo.

O intuito dos ataques *Cross-site Scripting* é incluir *scripts* ou links em sites de aplicações web com o objetivo de desviar o usuário para uma página falsificada. Uma vez nessa página o usuário pode inserir suas informações confidenciais a um site desconhecido.

Os principais efeitos para usuários contaminados:

- Retenção de sessão de usuários;
- Alteração do código HTML (perceptível somente no lado do cliente);
- Desviar usuários para sites maliciosos;
- Mudança do objetivo DOM para apreender dados ou envio de *malware*;

3.3.Cross-site Request Forgery (CSRF)

O *Cross-site Request Forgery* é uma das instabilidades mais populares e perigosas em aplicações web. *Cross-site* é a insegurança explorada entre sites no caso no mínimo dois sites envolvidos, *request* quer dizer requisição e *forgery* significa forjar, contudo isso se resume em uma requisição forjada por um atacante em um site.

O CSRF é uma variedade de ataques que trilha a união de segurança entre um aplicativo web e seu usuário. O invasor mal intencionado deve atrair o usuário autêntico por meio de engenharia social ou por outros artifícios a concretizar atividades atribuídas no aplicativo, autorizando que virtualmente a ação possa ser executada no sistema sem o conhecimento do usuário final.

Os alvos mais comuns são geralmente aplicativos web ou transações valiosas tais como:

- Modificação de senha de acesso;
- Compras online ou alterações financeiras;
- Alteração de email ou dados pessoais;

Etapas para a execução em aplicações vulneráveis:

- O cliente se válida na aplicação alvo do ataque;
- O cliente recebe um link e o utiliza para acessar um aplicativo falso;
- Com esse aplicativo falso o navegado inicia uma requisição a aplicação alvo, transferindo todas as orientações para execução da transação;
- Como a sessão foi validada para o usuário no aplicativo alvo, a aplicação utiliza a requisição, e exerce a transação de acordo o requerimento enviado;

3.4. Eavesdropping (espionagem)

Técnica de espionagem onde os *hacking* se baseiam na violação da confidencialidade, onde o atacante por falta de segurança nos dados, utilizando recursos tecnológicos faz um monitoramento sem autorização da vitima podendo roubar seus dados e informações pessoais. Essa espionagem pode ser feita em diversos sistemas, os mais comuns são: sistema de telefonia, e-mail, mensagens instantâneas e outros serviços da internet. O ataque por *eavesdropping* dificulta ao atacado saber que esta sendo vitima e suas informações estão sendo saqueadas, uma vez que o atacante só consegue capturar e manter as informações, não sendo possível adulterá-las.

3.5. SQL Injection

Os ataques SQL *Injection*, são possibilitados onde existem banco de dados que possam ser acessados via web. Esse tipo de ataque é muito simples, pois se constitui na efetivação de comandos SQL, através de comandos de manipulação de dados ou comandos de definição de dados. Nos campos destinados a informação do usuário, esses comandos são realizados, ou seja são exibidos comandos SQL, todavia por motivo dessa falha nas aplicações acabam ocasionando alterações no banco de dados ou em acesso inadequado a aplicação.

Essa adversidade ocorre porque a autenticação do usuário é ratificada dentro da aplicação, tendo a instrução: pesquisar se existe usuário com o determinado login e senha. Habitualmente estaria sendo digitado o login e a senha, que ocasionaria em uma consulta no banco de dados para a validação. Só que no campo da senha é apresentado parte de um comando SQL, com parte desse comando independentemente de qual login

ou senha seja digitada a condição será sempre verdadeira, permitindo ao invasor o acesso mesmo não tendo permissão.

4. MECANISMOS DE DEFESA

Com intuito de garantir a segurança dos consumidores e comerciantes no comércio eletrônico, deve-se implementar os seguintes processos:

- Autenticação
- Transação Eletrônica Segura
- Criptografia
- *Firewall*

4.1.Autenticação

Segundo FROOMKIN, (1997, p. 213) autenticação é o processo que garante que consumidores e comerciantes realizem transações através de internet somente por meio de pessoas ou entidades certificadas.

Atualmente existem três ambientes distintos para as empresas realizarem suas transações on-line: interno, B2B e B2C.

Interno: neste ambiente o controle de acessa as transações se dá por meio de mecanismos do sistema operacional e banco de dados. As transações on-line dentro das empresas possuem um controle de qualidade rígido através da facilidade do sistema operacional, sistema de segurança ou *software* de segurança externo. Nesse ambiente, cada funcionário possui um perfil de acesso, ficando definidas as transações que ele pode acessar de acordo com as suas atribuições.

B2B: é um meio onde as transações são realizadas entre fornecedores e consumidores utilizando assinaturas e certificados digitais que dão confiabilidade ao site. Mesmo se tratando de um ambiente fora da empresa, no B2B, é possível introduzir um controle eficiente de acesso as transações. O contrato firmado entre as empresas deve apresentar cláusulas objetivas definindo a política de segurança adotada pelas empresas.

B2C: ambiente onde um grande número de consumidores realizam suas transações, no qual o site necessita obrigatoriamente de certificado de autenticação. Esse certificado é determinado por uma autoridade, a qual chega com a autoridade de registro a fim de verificar informações fornecidas por quem exige um certificado digital.

4.2.Transação Eletrônica Segura

Segundo WAYNER, (1997, p. 215) Transações eletrônicas segura (SET) é um protocolo para transferências criptografadas de pagamentos utilizando cartões de crédito.

O SET estabelece um padrão único para a proteção das compras, utilizando como pagamento o cartão de crédito, realizadas na internet ou em outras redes abertas.

O mecanismo SET de segurança e pagamento tem por objetivo: autenticação da conta do consumidor e vendedor; dar confidencialidade de informação; integridade de informação; e interoperabilidade.

No modelo SET as transações com cartão de crédito podem ser compreendidas nas seguintes etapas:

1. O cliente envia um formulário de pedido e uma assinatura, com autorização criptografada. Uma vez criptografado, o vendedor não consegue acessar o número do cartão de crédito.
2. O vendedor por sua vez repassa a autorização ao banco, e este pode descriptografá-la e ver o número do cartão de crédito.
3. O banco entra em contato com a fornecedora do cartão para confirmar se o cartão é válido.
4. A emissora do cartão autoriza e assina a transação.
5. O banco autoriza e o vendedor autoriza a transação.
6. O cliente recebe o produto.
7. O vendedor recebe o pagamento.
8. O vendedor recebe o pagamento de acordo com seu contrato.
9. O comprador obtém a fatura mensal da emissora de cartão.

4.3. Criptografia

Segundo DENNING, (1997, p. 216) A criptografia vem desde a época da Grécia antiga sendo que a origem da palavra vem de *kryptós* e *grafos* que respectivamente significa oculto e escrita.

Conforme definido por ALBERTIN (2004) criptografia é a arte ou a ciência de escrever em cifra ou em código, ou, ainda, como conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que somente destinatário a decifre e a compreenda.

Existem dois métodos de criptografia:

Criptografia simétrica (chave privada) utiliza no algoritmo de cifragem e decifragem a mesma chave. Este método garante a confidencialidade na troca de mensagens. Nele é necessário que o receptor e o emissor da mensagem troquem a chave previamente, entre eles, de forma segura.

Criptografia assimétrica (chave pública) utiliza uma chave para cifrar e outra chave para decifrar. Assim cada ator envolvido possui um par de chaves uma pública e uma privada, sendo que a privada é secreta não sendo compartilhada, e a pública deve ser de conhecimento de todos. O método consiste em criptografar a mensagem com a chave pública do destinatário, para que este, e somente este, consiga descriptografar com sua chave privada. O par de chaves (pública e privada) ainda permite que a mensagem seja assinada eletronicamente. Ainda, a criptografia assimétrica garante confidencialidade, integridade e autenticação na comunicação das mensagens.

Em tempo, a criptografia pode ser aliada a protocolos utilizados na Internet, sendo que os dois caso mais conhecidos são: SSL e HTTPS.

Uma aplicação da criptografia é o protocolo SSL (*Secure Socket Layer*) que garante que todos os dados transportados cheguem de forma sigilosa e segura, através de um canal criptografado entre um navegador e um servidor web.

Outra possibilidade de protocolo seguro é o HTTPS (*Hyper Text Transfer Protocol Secure*) nada mais é que uma camada adicional de segurança sobre o protocolo

HTTP, assim a comunicação é feita de forma criptografada, garantindo confidencialidade, integridade e autenticação, utilizando certificado digital.

4.4. Firewall

Firewall é uma ferramenta disponível em software ou hardware, que serve para determinar quais dados podem entram e saírem de uma rede, um computador ou servidor. Os sistemas operacionais modernos em sua grande maioria apresentam de um *firewall* integrado, o que trás uma segurança intrínseca aos usuários.

> Segundo ALBERTIN, A. L.. (2004, 227), Um *firewall* trabalha estabelecendo uma barreira entre a rede corporativa (rede segura) e a internet externa (rede não confiável). Essa barreira protege as redes corporativas vulneráveis contra espionagem na rede pública. Um *firewall* não é simplesmente um *hardware* ou um *software*, é um enfoque para implementar uma política de segurança que define os serviços de acesso a serem permitidos para vários usuários. Em outras palavras, um *firewall* implementa uma política de acesso por forçar as conexões a passarem por meio de um *firewall* onde elas podem ser examinadas e auditadas.

> Segundo FAGUNDES, E. M. (2004, 132) *firewall* é um método para proteger a rede corporativa de acessos não autorizados. Um *Firewall* é composto por um servidor (computador) e um *software* especialista. Ele é instalado entre a rede corporativa da empresa e a Internet. Todo o tráfego de dados que é trocado com outros computadores da Internet é filtrado pelo *firewall.*

5.CONCLUSÃO

No decorrer dos anos, com a proliferação da Internet, esta tem se mostrado uma poderosa ferramenta no âmbito social.Um dos destaques é a comunicação, no sentido de ampliação do mercado digital. Com esse avanço, o comércio eletrônico tem se tornado um mecanismo de compras, vendas e propagandas, proporcionando a atuação de inúmeras empresas no mercado. Porém, ainda que as vendas *on-line* tenham crescido estrondosamente nas últimas décadas, quando comparadas com as vendas em lojas físicas, representam uma parcela muito pequena do total de transações no comércio geral.

Um dos motivos pelo qual os usuários preferem não efetuar transações via internet, é a falta de confiabilidade no sistema. A respeito de segurança, tem se trabalhado muito no âmbito do pagamento virtual, gerando vários meios de se efetuar uma transação, com diversos mecanismos de segurança. Como por exemplo,a utilização da criptografia na transmissão de dados, bloqueando, com isso, acessos indevidos as informações confidenciais, garantindo a privacidade dos dados informados.

Todavia, os serviços prestados pela Internet não estão integralmente protegidos das ameaças virtuais.Uma vez que são gerados novos vírus e novas técnicas de invasão a *sites* a cada ano, aumentando com isso as fraudes eletrônicas, e tornando-se um problema crescente, que afeta de modo direto o comércio eletrônico. Assim sendo, pesquisas inovadoras, que visam estabelecer uma conexão mais segura entre os consumidores e comerciantes da internet, torna-se de suma importância para o crescimento da confiabilidade e credibilidade do seguimento.

ABSTRATCT

In this work was related the problems that happen most in the electronic commerce. So, was made a research in the literature to find which are the attack more common suffered by costumers and sellers, beyond the principals ways to prevent these attacks. With that, we could observe that between the more recurrent attacks in the electronic commerce are the attacks by Ddos, Cross-site Scripting or XSS, Cross-site Request Forgery (CSRF), Eavesdropping, SQL Injection. However, in order to ensure reliability, should be implanted some mechanism to ensure the safety of users that use the internet to make some kind of electronic transition, such as: authentication, safe electronic transition, cryptography and firewall.

Key words: electronic commerce, attacks more recurrent, safety.

6. REFERÊNCIAS

ALBERTIN, A. L.; MOURA, R. M. **Comércio Eletrônico**: Modelo, Aspectos e Contribuições de sua Aplicação. 5 ed. São Paulo: Atlas, 2004.

BHIMANI, A. **Securing the commercial Internet**. *Communication of the ACM*. 39, 6, 29-35, 1996

DE ANDRADE, M. M. **Introdução à Metodologia do Trabalho Cientifico**: elaboração de trabalhos na graduação. 6. ed. São Paulo: Atlas, 2003..

FAGUNDES, E. M. **Como Ingressar Nos Negócios Digitais**. Edição Inteligente. São Paulo: Vida e Consciência, 2004.

KALACOTA, R.; WHINSTON, A. **Electronic commerce**: a manager's guide. New York: Addison-Wesley, 1997

O´ BRIEN, J. A. **Sistemas de Informação e as Decisões Gerenciais na Era da Internet**; tradução da 11ª versão americana. 2 Ed. São Paulo, Saraiva, 2004

CANAL TECH disponível: <https://canaltech.com.br/o-que-e/o-que-e/O-que-e-DoS-e-DDoS/> Acesso em março de 2017

E-COMMERCE NEWS disponível:

<https://ecommercenews.com.br/noticias/dicas/conheca-os-principais-ataques-virtuais-ao-e-commerce-e-saiba-como-se-proteger-das-ameacas> Acesso em março de 2017

GUIA DO HARDWARE disponível:

<http://www.hardware.com.br/livros/redes/eavesdropping.html> acesso em março de 2017

IMASTERS disponível: <https://imasters.com.br/artigo/9879/seguranca/xss-cross-site-scripting/?trace=1519021197&source=single> Acesso em março de 2017

REDESEGURA disponível: <http://www.redesegura.com.br/2012/03/serie-ataques-os-ataques-cross-site-request-forgery-csrf/> Acesso em março de 2017

TRUTSSING, disponível:

<https://www.trustsign.com.br/blog/5-dicas-de-seguranca-para-sites-de-comercio-eletronico/index.html> Acesso março de 2017