camara-e.net
Câmara Brasileira de Comércio Eletrônico

CARTILHA ANTIFRAUDE

LOJAS & EMPREENDEDORES ONLINE

CARTILHA ANTIFRAUDE PARA LOJAS E EMPREENDEDORES ONLINE

SUMÁRIO EXECUTIVO

CARTILHA ANTIFRAUDE PARA LOJAS E EMPREENDEDORES ONLINE

INTRODUÇÃO

Há 20 anos o e-commerce brasileiro cresce continuamente. E continuará crescendo nos próximos anos. No entanto, será marcado pelo acirramento da concorrência e pelos desafios enfrentados em todo o ecossistema com a segurança de dados. Além de continuar inovando para atrair e fidelizar clientes para se destacar da concorrência, o lojista também precisa manter o foco na proteção das informações do consumidor e da própria loja. Afinal, quanto maior o número de clientes e lojas, maior o número de tentativas de golpes.

A fraude no comércio eletrônico ainda é uma das maiores responsáveis pela perda de receita no varejo online. Segundo dados da ClearSale, as compras fraudulentas feitas pela internet representam **4,40%** de todas as transações em lojas virtuais no Brasil, e **5,6%** das tentativas de fraude registradas no país acontecem em compras feitas pelo celular.

5,6% DAS TENTATIVAS DE REGISTRADAS NO E-COMMERCE ACONTECEM EM COMPRAS VIA CELULAR.

A maioria dos casos de fraudes detectados está nas regiões Norte e Nordeste, que registraram o maior crescimento em faturamento na Black Friday 2016.

Você deve estar se perguntando por que as fraudes online cresceram tanto. O motivo é simples: uma vez que atacar e fraudar serviços online de instituições bancárias ou comerciais é cada vez mais difícil, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários – no caso, as lojas online.

Por isso, se você está neste mercado e quer ampliar ou manter a sua fatia de participação, saiba que perder vendas não é uma opção, e a Gestão antifraude pode ser o maior trunfo do seu negócio.

Elaborada pelo Observatório de Gestão de Fraude (OGF), esta cartilha traz as boas práticas para você, lojista, manter em segurança os dados de sua loja e de seus clientes. Aqui você ficará sabendo como identificar a fraude online, como prever os ciberataques, quais são os tipos de golpes mais comuns e como se prevenir contra os cibercriminosos.

Boa leitura!

camara-e.net
Câmara Brasileira de Comércio Eletrônico

OBSERVATORE.ORG

OBSERVATÓRIO DE GESTÃO DE FRAUDE

O **Observatório de Gestão de Fraude (OGF)** é um projeto capitaneado pelos comitês de Meios de Pagamentos, Varejo Online e Gestão de Riscos da Câmara Brasileira de Comércio Eletrônico (camara-e.net). Nasceu da necessidade do setor de encontrar uma maneira eficiente de combater as fraudes online por meio da difusão do conhecimento entre as empresas que atuam no setor.

O OBSERVATÓRIO DE GESTÃO DE FRAUDES TEM OS SEGUINTES OBJETIVOS:

- Agregar cidadãos e instituições interessadas em conhecer a gestão de riscos na economia digital
- Promover boas práticas e cartilhas sobre a prevenção à fraude online
- Contribuir para uma opinião pública esclarecida sobre a gestão de riscos
- Constituir uma memória das práticas fraudulentas, enquanto instrumento para prevenção e detecção de fraude mais eficazes
- Apoiar as organizações na prevenção à fraude
- Promover o comércio eletrônico seguro no Brasil por meio do desenvolvimento dos meios de pagamento

ESTUDAR A FRAUDE É UM PROCESSO DE CONSTRUÇÃO E DESCONSTRUÇÃO DE SABERES E CONHECIMENTOS CIENTÍFICOS, SIMULTANEAMENTE DISCIPLINAR E INTERDISCIPLINAR, CONTRIBUINDO PARA A CONSOLIDAÇÃO DE UM OBJETO CIENTÍFICO DE UMA CIÊNCIA AINDA EM CONSTRUÇÃO: GESTÃO DA FRAUDE.

- Apresentar os principais golpes aplicados na Internet
- Informar sobre os cuidados que consumidores e lojistas devem tomar para proteger a vida online
- Fomentar o comércio eletrônico com transparência, ética e responsabilidade

camara-e.net
Câmara Brasileira de Comércio Eletrônico

FRAUDE ONLINE

Os golpistas utilizam técnicas de engenharia social e, por diferentes meios e discursos, procuram enganar e persuadir as potenciais vítimas a fornecer informações sensíveis ou a realizar ações que facilitam a fraude, como executar códigos maliciosos e acessar páginas falsas.

De posse dos dados das vítimas, os criminosos costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, identificados no artigo 171 do código penal como estelionato. Assim, o golpista é considerado um estelionatário.

Na Cartilha Antifraude para os **eConsumidores** apresentamos alguns dos principais golpes aplicados na Internet e alguns cuidados que devem ser tomados para se proteger. Mas como identificar a fraude quando o crime é praticado contra os lojistas? A seguir, apresentamos as Boas Práticas que mantêm as lojas online seguras.

POPULARMENTE CONHECIDO COMO 171, ESTELIONATO É UM CRIME COM PENA PREVISTA EM LEI DE 1 A 5 ANOS DE RECLUSÃO E MULTA.

COMO PREVER CIBERATAQUES?

A fraude, um dos maiores medos de quem tem um e-commerce, pode não ser uma preocupação inicial, mas uma vez descoberta a sua gravidade ela se torna a grande vilã do negócio. Você ou a plataforma na qual sua loja está hospedada está preparado para lidar com o problema? Ou você só vai perceber que há algo errado após um registrar um grande chargeback (estorno de compra)?

Uma maneira eficaz de prevenir golpes é manter uma equipe antifraude. Essa equipe ficará encarregada de monitorar as pequenas mudanças nas tendências em transações que precedem um ataque. Esse monitoramento permite detectar padrões típicos dos cibercriminosos e do consumidor.

Fraudadores, independentemente da natureza do ato ilícito que pretendem cometer, seguem padrões. Consumidores também. E é por meio do monitoramento desses padrões que a fraude pode ser descoberta antes de causar estragos.

Os consumidores normalmente apresentam um determinado padrão de navegação, como fazer pesquisas em vários sites ou então usar os comparadores de preço. Também pagam geralmente com cartão e realizam compras pequenas.

FRAUDADORES E CONSUMIDORES TÊM PADRÕES DE NAVEGAÇÃO DIFERENTES, FÁCEIS DE IDENTIFICAR.

Quem pretende cometer um crime tende a se comportar de outra maneira: entra direto no site que foi eleito para vítima, pois preço não é a questão. Ele paga com boleto e ainda compra em grande quantidade.

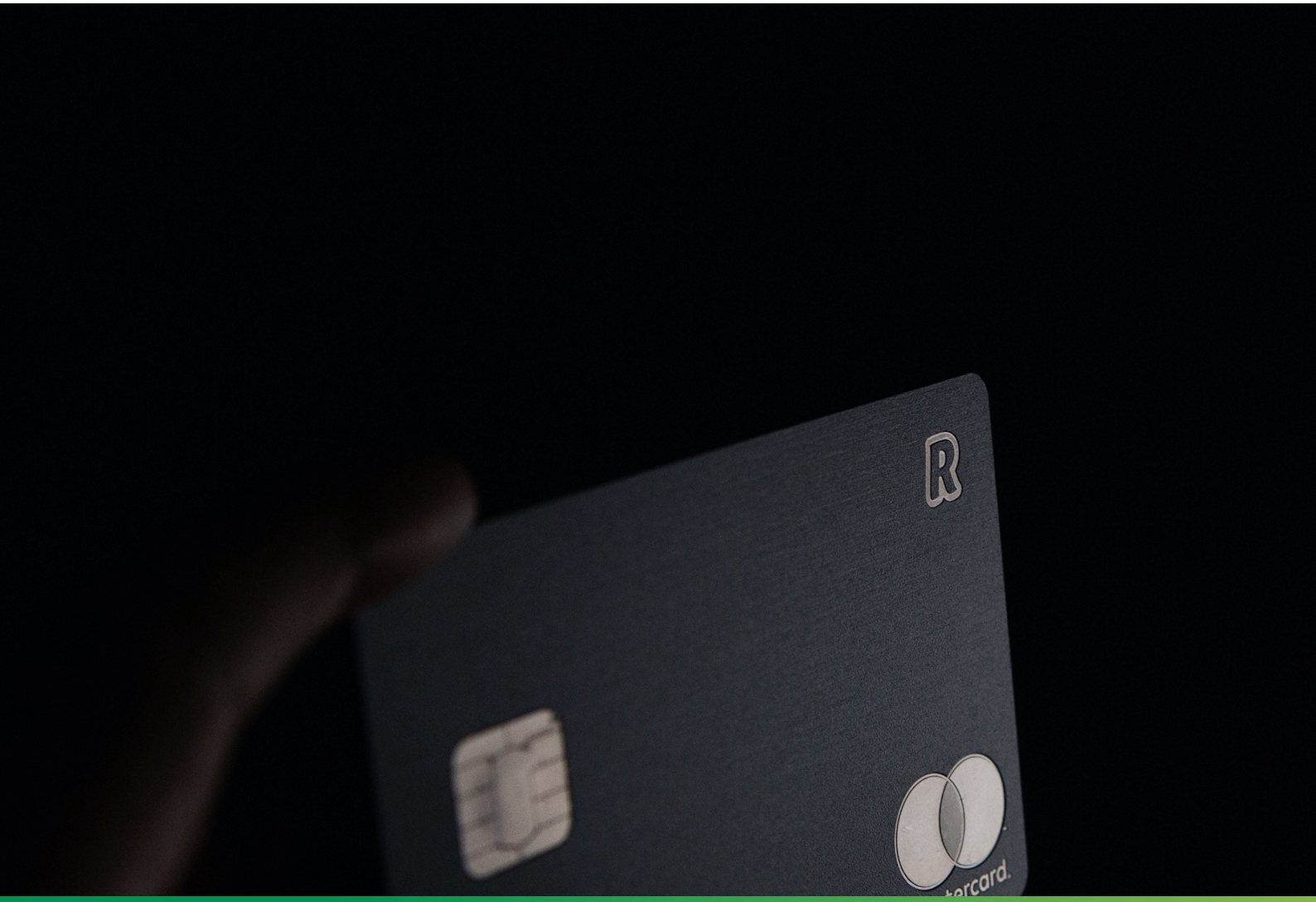
Analisando esse cenário, é possível identificar padrões comuns de fraude antes mesmo da tentativa efetivamente virar um pedido.

Os fraudadores são muito dinâmicos, às vezes mais espertos que seu sistema de prevenção à fraude. Uma vez identificada uma vulnerabilidade, seu negócio estará exposto, e o dano financeiro resultante pode vir rapidamente.

A notícia de uma fraqueza em um sistema antifraude se espalha com facilidade entre os golpistas. Muitas vezes, diversos fraudadores atacam um site a mesmo tempo, pegando tudo que podem antes que a segurança corrija o erro. Daí seguem em frente, procurando a próxima vítima vulnerável.

Os ataques podem ter os mais variados objetivos, como tornar o site-alvo indisponível ou utilizar o site-alvo como disseminador de vírus. Nas próximas páginas você vai conhecer as fraudes mais comuns com que os lojistas precisam lidar.

OS GOLPISTAS ESTÃO ORGANIZADOS. ELES ESPALHAM RAPIDAMENTE A NOTÍCIA DA EXISTÊNCIA DE VULNERABILIDADES. E ATACAM EM MASSA.



FRAUDE CONTRA CARTÃO DE CRÉDITO

Esta fraude se caracteriza pela obtenção ilegal de dados de cartão de crédito do consumidor de três formas: captura de dados em trânsito, ataques ao cliente e ataques ao site de comércio eletrônico.

Em casos mais sofisticados, os golpistas combinam elementos desses três métodos, e causam um grande estrago. Vamos ver como os criminosos conseguem esses dados.

CAPTURA DE DADOS EM TRÂNSITO

O QUE É

Uma venda através de um site de comércio eletrônico é, pode ser explicada, de maneira simplificada, como um conjunto de dados que parte da estação do consumidor com destino ao servidor da loja virtual e deste para os servidores das instituições responsáveis pela autorização da transação. E é nesse trajeto, quando as informações estão transitando entre as máquinas, que os golpistas atuam, explorando vulnerabilidades de segurança do computador do consumidor, do servidor da loja ou dos servidores da instituição financeira.

COMO PREVENIR

Uma página Web geralmente é construída com base no protocolo HTTP (protocolo de transferência de hipertexto, em português), um protocolo de comunicação que possibilita a transmissão de dados pela internet. O problema do HTTP é que, em redes públicas, essas páginas estão vulneráveis a ataques de pessoas mal intencionadas.

Num e-commerce, esse protocolo funciona bem para a maioria das páginas de um site, mas é um desastre para os canais em que trafegam os dados pessoais e financeiros do cliente, pois é uma conexão insegura. Qualquer um que interceptar o pacote de dados nessas conexões pode ler seu conteúdo.

A melhor solução para esse problema é adotar o protocolo HTTPS – SSL, que torna a conexão segura adicionando uma camada de proteção na transmissão de dados. Em páginas ou sites com endereço HTTPS, a comunicação é criptografada, e só o remetente e o destinatário conseguem resolver o enigma dessa camada de proteção.

ATIVE O PROTOCOLO DE CONEXÃO SEGURA HTTPS- SSL EM PÁGINAS DO SITE EM QUE SÃO CADASTRADAS INFORMAÇÕES PESSOAIS E FINANCEIRAS DO CLIENTE.

Se o site da sua loja não usa protocolo HTTPS, peça ao administrador de sistemas ou aos administradores da plataforma de e-commerce contratada para ativar a conexão segura. Você estará criando uma barreira que vai dificultar em muito o trabalho dos cibercriminosos.

ATAQUES AO CLIENTE DE CARTÃO DE CRÉDITO

O QUE É

Nesse tipo de fraude ao cartão de crédito, os criminosos buscam se aproveitar da ingenuidade do usuário para obter dados pessoais e financeiros, como senhas e números de conta bancária e de cartão de crédito.

Para isso, ele envia mensagens que induzem a vítima a clicar em links ou a baixar arquivos que, uma vez abertos, exibem telas em que o usuário deve fornecer as informações desejadas pelo fraudador.

Mas você deve estar pensando que esse não é um problema que afeta você como lojista, mas o consumidor. Você não poderia estar mais enganado, pois o fraudador usa o nome da sua loja para enganar o seu cliente, fazendo-o pensar que é você quem está pedindo a ele esses dados. Do ponto de vista jurídico, você é responsável pelos dados pessoais confiados à loja pelo seu cliente.

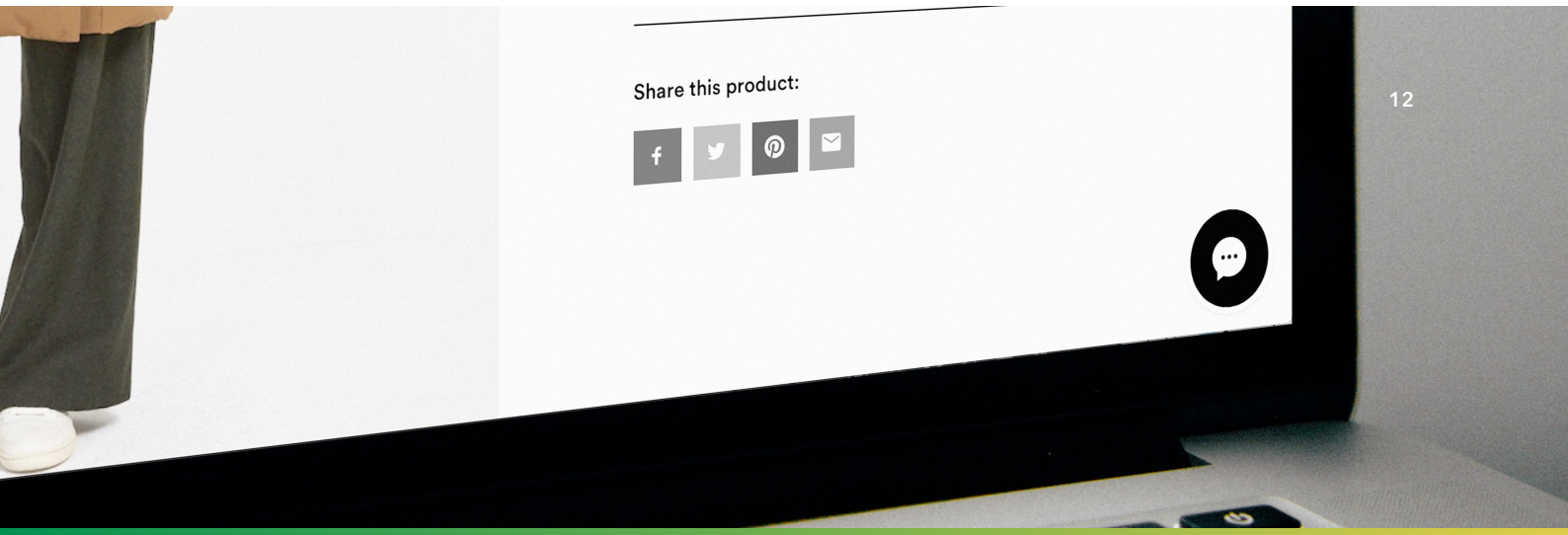
COMO PREVENIR

A melhor arma para se proteger sua loja e seu cliente das telas fraudulentas, é deixar claro

VOCÊ É RESPONSÁVEL JURIDICAMENTE PELA GUARDA DOS DADOS QUE O CLIENTE INFORMA NA HORA DA COMPRA.

para o consumidor, na hora em que ele preenche o cadastro e coloca ali seus dados pessoais e financeiros, que a empresa não envia solicitações de recadastramento ou solicitação de dados pessoais por e-mail ou pelas redes sociais. Essa recomendação deve ser feita por todos os canais da loja: pelo SAC, no e-mail de confirmação de cadastro, na página de cadastro e nos termos de uso.

Caso seja necessário que ele altere essa senha, faça a comunicação informando que ele deve entrar no site, digitando endereço da loja no navegador (e não por link enviado no e-mail) e seguir as orientações de troca de senha partir do login.



ATAQUES AO SITE DE COMÉRCIO ELETRÔNICO

Uma empresa pode sofrer ataques por meio de vulnerabilidades em sua infraestrutura tecnológica (servidores e equipamentos de rede), nos processos internos e nos sistemas informatizados. Ataques de DDoS, em que vários computadores atacam outro ao mesmo tempo, tornando o site indisponível, e do tipo "man-in-the middle", que intercepta os dados durante o tráfego, por exemplo, exploram essas vulnerabilidades. Mas você sabe quais são essas vulnerabilidades e como evitar que os criminosos consigam explorar as brechas abertas por elas? Veja a seguir.

VULNERABILIDADE DE INFRAESTRUTURA

O QUE É?

É uma brecha nos sistemas operacionais de servidores e computadores e em dispositivos de rede, que permite que pessoas mal intencionadas invadam o site, acessem dados de clientes e das lojas e até tirem o site do ar.

Todo servidor, sistema operacional e dispositivo de rede possui uma configuração básica de instalação. E apesar de não ser a opção mais segura, a maioria das empresas mantém a configuração básica para disponibilizar os equipamentos o mais rápido possível.

Esses ambientes são os que os criminosos mais procuram, pois há muita documentação disponível na internet sobre a fragilidade e a vulnerabilidade de sistemas que usam esse tipo de configuração.

Por isso vale a pena personalizar a configuração dos sistemas e dispositivos que compõem a infraestrutura tecnológica do seu site. Também é

GOLPISTAS ATACAM SITES DE COMERCIO ELETRÔNICO EXPLORANDO VULNERABILIDADES NA INFRAESTRUTURA, NOS PROCESSOS INTERNOS E NOS SISTEMAS INFORMATIZADOS

importante manter um processo contínuo de atualização com as correções disponibilizadas pelo fabricante.

Certifique-se ainda de que essas configurações sejam efetuadas no local em que seu site está hospedado: em servidor próprio ou na infraestrutura de terceiros.

COMO PREVINIR?

Existem duas soluções básicas para evitar vulnerabilidades na sua infraestrutura do site. A primeira barreira é conhecida como firewall e funciona como um muro de proteção para o sistema. É como o fosso que circundava os castelos para evitar a entrada de inimigos. A segunda barreira é a adoção de mecanismos de controle de acesso. Tomando como exemplo o mesmo castelo, é o portão que se abre para o pátio principal somente com a permissão da guarda real. Saiba como instalar essas barreiras para proteger o seu site:

- **1ª. BARREIRA - FIREWALL**

Primeira camada de proteção do perímetro, o firewall deve ser instalado na rede. É ele quem determina quais equipamentos podem conectar-se aos servidores mais críticos de sua empresa e impede acessos não autorizados.

- **2ª. BARREIRA - SENHAS FORTES**

Qualquer dispositivo conectado à internet está sujeito a invasões. Isso inclui smartphones, roteadores, wearables e até impressoras com conexão sem fio. A segunda barreira, que não substitui o uso de firewalls, mas complementa a sua proteção, é a ativação de mecanismos de controle de acesso.

Nem todos os funcionários da sua loja precisam ter acesso a todas as informações para desempenhar suas atividades. Por isso, configure as permissões de acesso de acordo com o perfil de cada funcionário. Por exemplo: a pessoa responsável pela atualização do catálogo de produtos não precisa ter acesso às informações financeiras e pessoais dos clientes.

Quanto maior for o acesso concedido de maneira inadequada, maior será o potencial para a ocorrência de fraudes e para erros operacionais com base neste acesso.

Outra medida de proteção é exigir que o usuário ou o cliente cadastre senhas fortes, contendo letras maiúsculas, minúsculas, caracteres especiais e números. São mais difíceis de adivinhar e de quebrar.

- **VULNERABILIDADE DE PROCESSOS INTERNOS**

Esta vulnerabilidade está relacionada ao comportamento de funcionários e colaboradores da sua loja. De nada adianta estabelecer uma política de controle de acesso se os seus colaboradores tiverem o hábito de compartilhar usuários e senhas. Em caso de fraudes ou outros tipos de incidente não será possível determinar quem realizou a ação.

- **VULNERABILIDADE EM SISTEMAS INFORMATIZADOS**

A existência de falhas em sistemas de mercado, que os expõem a ataques remotos, é de conhecimento de boa parte da comunidade que interage diariamente com a tecnologia. E é o tipo de vulnerabilidade que chama a atenção da mídia e que se torna um assunto do cotidiano. A solução para esses problemas é criada pelos próprios fabricantes do software ou por empresas de antivírus.

Mas a maioria dos empreendimentos de e-commerce desenvolve sistemas internos que, ao contrário do que se pensa, podem possuir vulnerabilidades tão ou mais graves quanto as que ocorrem em produtos de mercado. Hoje, muitos dos ataques aos servidores de internet ocorrem porque há falhas que permitem acesso não autorizado ou tornam o sistema indisponível.

Vale observar, no entanto, que não existe software inviolável. Existem políticas de segurança que, aplicadas de maneira correta, protegem com eficácia todo o ciclo de vida do software (especificação, desenvolvimento e manutenção).

Deixe claro a seus funcionários e prestadores de serviço que as senhas são de uso pessoal e que não seguir essa orientação pode resultar em algum tipo de punição que você considere certo estabelecer.

VULNERABILIDADE EM SISTEMAS INFORMATIZADOS

A existência de falhas em sistemas de mercado, que os expõem a ataques remotos, é de conhecimento de boa parte da comunidade que interage diariamente com a tecnologia. E é o tipo de vulnerabilidade que chama a atenção da mídia e que se torna um assunto do cotidiano. A solução para esses problemas é criada pelos próprios fabricantes do software ou por empresas de antivírus.

Mas a maioria dos empreendimentos de e-commerce desenvolve sistemas internos que, ao contrário do que se pensa, podem possuir vulnerabilidades tão ou mais graves quanto as que ocorrem em produtos de mercado. Hoje, muitos dos ataques aos servidores de internet ocorrem porque há falhas que permitem acesso não autorizado ou tornam o sistema indisponível.

Vale observar, no entanto, que não existe software inviolável. Existem políticas de segurança que, aplicadas de maneira correta, protegem com eficácia todo o ciclo de vida do software (especificação, desenvolvimento e manutenção).

As falhas mais comuns no desenvolvimento de software são:

- **FALHAS DE DESIGN** - São os problemas gerados no planejamento da Aplicação Web sem a preocupação adequada com o nível de segurança. Exemplos desses problemas são o controle de acesso a usuários somente por meio de menus e a simplificação no acesso à base de dados.

- **FALHAS DE ARQUITETURA DO SISTEMA** - São as vulnerabilidades associadas à segmentação de redes, implementação de ativos de TI e informações que possam comprometer o ambiente analisado. Trocando em miúdos: são falhas que comprometem o banco de dados do seu negócio. E uma empresa que perde suas informações, perde tudo. Imagine-se perdendo todo o banco de dados, sua base de clientes com histórico de compra que lhe permite direcionar melhor o pós-venda, ou toda a sua relação contábil ou o controle de estoque. E essa falha ocorre quando a arquitetura do software não prevê camadas extras de proteção para, por exemplo, ou se utiliza de protocolos de comunicação com brechas que permitem burlar o processo de criptografia.

- **FALHAS NO CÓDIGO** - São as relacionadas à maneira como as empresas constroem suas aplicações corporativas, frameworks e demais componentes do software. É a camada onde são identificadas as falhas mais comuns.

- **FALHAS NA ADMINISTRAÇÃO DO SISTEMA** – São aquelas que aparecem quando pessoa que administra o sistema de sua loja não aplica os conceitos de proteção esperados. Um exemplo disso é a mudança de controle por senhas fortes para controles mais fracos, se a avaliação do nível de risco dessa mudança.

camara-e.net
Câmara Brasileira de Comércio Eletrônico

AV. ANGÉLICA, 2.503
5° ANDAR, SALA 56
SÃO PAULO/SP

T 55 (11) 3237-1102
W CAMARA-E.NET

CONCLUSÃO

O FRAUDADOR NÃO UTILIZA COMPUTADORES SUPERAVANÇADOS. ELE REALIZA SUA AÇÃO CRIMINOSA USANDO COMPUTADORES COMUNS, COM OS MESMOS SISTEMAS OPERACIONAIS E NAVEGADORES DE INTERNET QUE A GRANDE MASSA DA POPULAÇÃO.

ELE TAMBÉM NÃO ATUA NA CALADA DA NOITE. ESTUDOS MOSTRAM QUE AS COMPRAS EM LOJAS VIRTUAIS COM CARTÕES DE CRÉDITO ACONTECEM COM MAIS FREQUÊNCIA E EM MAIOR QUANTIDADE ÀS QUARTAS-FEIRAS, ENTRE 17H30 E 23H50.

FONTES:

CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO - HTTP://CAMARA-E.NET
CLEAR SALE: MAPA DA FRAUDE 2018 - HTTP://LP.BR.CLEAR.SALE/MAPA-DA-FRAUDE
KONDUTO: HTTP://EBOOKS.KONDUTO.COM/RAIO-X-DA-FRAUDE