



DOCUMENTO ESTRATÉGICO

Detecção de Fraudes:

A Primeira Linha de Defesa na Batalha
Contra Fraudes





ÍNDICE

+ Relacionamento com os Consumidores	3
+ Proteção Invisível	3
+ A Primeira Linha de Defesa Contra Fraudes	5
+ Saiba Mais	6
+ Sobre a VeriSign	6



Detecção de Fraudes:

A Primeira Linha de Defesa na Batalha Contra Fraudes

- Em 2006, os americanos perderam aproximadamente US\$ 49,3 bilhões com fraudes e 8,4 milhões foram vítimas de fraude de identidade.¹
- As vítimas da fraude de contas ativas pagaram em média US\$ 587 do próprio bolso em custos do consumidor, e o custo médio da fraude de novas contas chegou a US\$ 792.²
- A perda média com fraude online em novas contas mais que dobrou, de US\$ 2.678 em 2005 para US\$ 5.962 em 2006.³
- Embora a porcentagem de perda de receita por fraude continue a diminuir, o valor total de perdas com fraudes online atingiu US\$ 3,1 bilhões em 2006.⁴

+ Relacionamento com os Consumidores

Por necessidade, as empresas devem se tornar extremamente confiáveis no mundo anônimo da Internet, uma vez que os consumidores preenchem suas contas online com detalhes cada vez mais pessoais. É possível que seu banco de dados saiba mais do que alguns amigos mais íntimos e familiares de seus consumidores: saldos de contas bancárias, fundos de aposentadoria, histórico de crédito, histórico médico, hábitos de compras, preferências de entretenimento e muito mais. Quando os consumidores criam um login, eles começam um relacionamento com sua empresa confiando que você protegerá as suas informações e as manterá sempre seguras.

Você faz o suficiente para proteger a confiança deles?

Sistemas de detecção de fraudes podem fornecer a primeira linha de defesa ao impedir acesso não-autorizado a dados e contas particulares. Como seguranças, eles observam as atividades até que algo inesperado ocorra. Então eles entram para avaliar a situação e tomar uma decisão quanto a permitir o acesso ou não. Um sistema eficiente de detecção de fraudes permite que os consumidores interajam com você pela Internet sem alterar seus comportamentos ou instalar qualquer coisa em seus computadores. Ao mesmo tempo, você tem uma forma conveniente e não-intrusiva de avaliar o risco da transação e responder adequadamente.

A conveniência e cortesia da Internet

Apesar da crescente incidência de roubos de identidade e dos custos das fraudes online se elevando, os consumidores preferem a velocidade das transações online e a conveniência de ter as informações nas pontas dos dedos, em qualquer lugar do mundo em que decidam fazer o acesso. Um relatório da Forrester de 2006 descobriu que os consumidores que consideram que seus prestadores estavam fazendo um bom trabalho quanto à proteção contra fraudes online também tinham um alto nível de satisfação com seus bancos, corretoras e seguradoras. Além disso, mais de um terço dos usuários europeus da Internet que não realizam operações bancárias online o fariam se tivessem uma garantia de proteção contra fraudes. Um sistema eficiente de detecção de fraudes pode ajudar as empresas a oferecer aos consumidores um hábito online seguro e confiável que encoraje a adoção e crie fidelidade a sua marca e seus serviços.

+ Proteção Invisível

Os melhores sistemas de detecção de fraudes são como os mais discretos seguranças. Eles têm instintos excelentes, ampla experiência e uma abordagem firme, porém amigável, para resolver disputas. Eles entendem que cada usuário é diferente ao mesmo tempo em que reconhecem o comportamento individual consistente. Eles também sabem que os criminosos aperfeiçoam continuamente seus métodos e tentam adotar a aparência de um usuário legítimo. Compilamos uma pequena lista de qualidades a serem consideradas ao escolher um sistema de detecção de fraudes, como a primeira linha de defesa, para suas aplicações online.

¹ 2007 Identity Fraud Survey Report (Consumer Version) How Consumers Can Protect Themselves (Relatório da Pesquisa sobre Fraude de Identidade 2007 (Versão do Consumidor) Como os Consumidores Podem se Proteger), Javelin Strategy & Research, fevereiro de 2007

² 2007 Identity Fraud Survey Report (Consumer Version) How Consumers Can Protect Themselves, Javelin Strategy & Research, fevereiro de 2007

³ Gartner como citado em comunicado à imprensa, 6 de março de 2007, www.emarketer.com

⁴ Online Fraud Report (Relatório sobre Fraudes Online), CyberSource, 9th Annual, 2008 Edition, p. 4.



COMO AS FRAUDES OCORREM

- *Phishing*
- *Pharming*
- *Man in the middle*
- *Telefonemas com engenharia social ou SMS*
- *Key loggers que contêm trojans*
- *Fraudes de amigos e familiares*

Instintos Excelentes

É claro que as máquinas não possuem instintos, mas elas possuem uma forma sistemática de analisar interações. A maioria dos sistemas de detecção de fraudes utiliza um mecanismo de regras, um mecanismo de comportamento ou ambos para avaliar o nível de risco. Quanto melhor for o sistema de detecção, mais eficiente será sua prevenção de fraude sem reduzir a velocidade das transações legítimas.

Um mecanismo de regras analisa uma transação para determinar se esta quebrou ou não uma regra antes de permitir o acesso. Uma regra pode estabelecer um número máximo de senhas que um consumidor pode tentar, ou impedir a criação de uma nova conta com o mesmo endereço de e-mail de uma conta existente. A configuração de regras e intervenções correspondentes possui uma ampla faixa de eficiência. Um mecanismo de regras que é muito flexível oferece proteção irregular. Um mecanismo de regras que é muito rígido atrasa o cliente, causando frustração e aumentando as chamadas de suporte. Um mecanismo de regras que é fácil de modificar permite que uma empresa ajuste as regras a um nível de risco apropriado para abordar as necessidades específicas do negócio.

Um mecanismo de comportamento aprende como o consumidor usa o sistema para identificar o risco de forma dinâmica. Ele responde quando o comportamento do consumidor muda, mesmo se a mudança não quebrar uma regra geral. Por exemplo, um mecanismo de comportamento entra em alerta quando um consumidor que sempre realiza o login de sua casa de repente o faz em outro país. O mesmo mecanismo de comportamento não interfere quando um consumidor que geralmente realiza o login de diferentes locais do mundo troca de lugar. Um sistema de detecção de fraudes com um mecanismo de regras e um mecanismo de comportamento não exige que um consumidor mude de comportamento. Na verdade, ele cria valor por sua consistência para ajudar a evitar fraude.

Quando esses mecanismos trabalham juntos, eles podem designar um nível mais específico de risco e aplicar uma intervenção mais apropriada. O consumidor precisa fornecer uma prova adicional de que é quem ele diz ser? Ou eles devem ser proibidos de entrar no sistema e ter as evidências sobre suas tentativas coletadas?

Muita Experiência

As aplicações online de hoje passaram a ser profundamente integradas aos sistemas empresariais. Ainda assim, muitos sistemas de detecção de fraudes enfocam estritamente o nome do usuário e a senha. Os fraudadores aprenderam a explorar esta falta de proteção integrada por meio da fraude de canal cruzado (cross-channel fraud). Eles autorizam seu próprio acesso ligando para o atendimento ao cliente e usando sistemas de resposta de voz interativa ou chat para alterar as informações existentes da conta. Um sistema de detecção de fraudes eficiente aplica uma visão ampla dos dados e atividades para responder às táticas dos fraudadores, que estão em constante alteração.

Primeiro, um sistema de detecção de fraudes deve ampliar seu escopo interno para além dos logins, para analisar os dados de todos os sistemas relevantes. Por exemplo, uma aplicação online de transações bancárias deve aplicar a detecção de fraudes ao login, assim como ao atendimento telefônico ao cliente, e aos dados da transação para detectar anomalias. O endereço IP de um criminoso é uma fonte essencial de informações para detecção de fraudes. O sistema deve ser capaz de identificar a localização geográfica, o tipo de conexão e o prestador de serviço de Internet (ISP) com base no endereço IP. Ele deve então relacionar as informações com os dados internos, assim como listas de suspeitos e padrões de ataque globais. Gerenciar o crescimento exponencial nos dados sem diminuir a velocidade da transação requer um mecanismo de detecção altamente escalonável e confiável.



Em segundo lugar, quanto mais seus sistemas de detecção de fraudes souberem sobre as atividades externas, melhor eles podem proteger os ativos empresariais e de consumidores. Os objetivos dos criminosos evoluíram de invasões elaboradas para obter notoriedade para organizações criminosas bem organizadas que enfocam informações de alto valor para obter lucro. Um método de ataque que funciona em um banco ou sistema de saúde será compartilhado em toda a organização criminosa e será rapidamente explorado até que os sistemas de segurança se adaptem para impedi-lo. Um sistema de detecção de fraudes com “olhos e ouvidos” rastreando as tendências globais será capaz de reconhecer novos tipos de fraudes e rapidamente responder com políticas para bloquear os ataques.

Intervenção Firme e Amigável

Suas aplicações online são muito mais que uma conveniência ou uma forma de reduzir os custos de atendimento ao cliente; elas criam um relacionamento muito mais pessoal e particular entre você e o seu consumidor. Acrescentar uma seqüência complicada de login que exija que os usuários dominem sua interface ou um sistema de detecção de fraudes que constantemente interrompa as atividades desestimula os consumidores a executar transações pela Internet. Um sistema de detecção de fraudes deve trabalhar nos bastidores e intervir de maneira firme, porém amigável, quando apropriado.

Um sistema de detecção de fraudes oferece uma camada invisível de proteção entre você e seu consumidor. Quando comportamentos de risco são detectados, uma resposta apropriada fará com que consumidores legítimos se sintam mais seguros em vez de incomodados. A autenticação com base em risco utiliza o nível de risco detectado para determinar como o sistema vai confirmar a identidade do consumidor. O administrador do sistema controla se o sistema utiliza um método de autenticação de baixo nível, como pergunta e resposta de segurança ou reconhecimento de imagem, ou se requer uma autenticação forte, como uma mensagem SMS, um e-mail, uma chamada automatizada ou uma chamada do atendimento ao cliente.

Além do risco, o perfil de seu consumidor também pode determinar a resposta. Alguns sistemas de detecção de fraudes permitem que os consumidores gerenciem seu método preferencial de notificação, como uma mensagem SMS, um e-mail ou telefonema. Você também pode decidir aplicar gerenciamento do risco aos consumidores de outra forma. Por exemplo, um risco moderado detectado em um consumidor de alto valor ou premium pode ser ajustado para gerar sempre uma chamada de atendimento ao cliente.

Em caso de ataque ou quebra, o sistema deve ajudar a empresa a resolver o problema rapidamente enquanto coleta evidências necessárias para a resolução de disputas ou potencial ação legal.

+ A Primeira Linha de Defesa Contra Fraude

Um sistema eficiente de detecção de fraudes faz com que os consumidores se sintam seguros e bem-vindos ao aprender seus comportamentos, proteger suas informações de conta e responder adequadamente ao risco com conhecimento de mudanças internas, assim como padrões de fraude globais. Um Sistema de Detecção de Fraudes Eficiente Possui:

- Mecanismo de regras fácil de usar e um mecanismo de comportamento com auto-aprendizagem para gerenciar o risco de forma eficiente.
- A escala e a flexibilidade ideais para combinar dados de call centers e outros sistemas relevantes com monitoramento de transações e login, assim como inteligência global de segurança.
- Opções de métodos de intervenção em tempo real para autenticação, incluindo perguntas e respostas de segurança, assim como e-mail, mensagens de texto SMS e chamadas automatizadas.

Prevenir e proteger contra fraudes ajuda as empresas a oferecer conveniência e confiança para os consumidores com proteção abrangente para aplicações e transações online.



+ Saiba mais

Para obter mais informações sobre a proteção de identidade VeriSign Identity Protection, ligue para 55 11 5853 2900 ou envie e-mail para: faleconosco@verisign.com.

+ Sobre a VeriSign

A VeriSign é a fornecedora confiável de serviços de infra-estrutura de Internet para o mundo digital. Bilhões de vezes por dia, a VeriSign ajuda empresas e consumidores de todas as partes do mundo a se comunicar e realizar transações com segurança.

Visite nosso site em www.Verisign.com.br para obter mais informações.

©2008 VeriSign BRASIL LTDA. Todos os direitos reservados. VeriSign, o logotipo da VeriSign e o círculo com marca de verificação são marcas registradas ou marcas comerciais da VeriSign e de suas subsidiárias nos Estados Unidos e em outros países. Todas as outras marcas comerciais são propriedades de seus respectivos titulares.

00026467 13/10/08

GB 017/08