Detecção de Fraudes na Web - Um Primeiro Olhar

A GlobalMinds (Brasil) e a Plurilock (Canadá) uniram suas experiências em uma parceria para aplicar a mais inovadora tecnologia anti-fraudes baseada em biometria comportamental.

Observamos que as principais fraudes na Web, podem ser classificadas em dois tipos:
-Fraude de aplicação: quando um indivíduo ou organização se vale do uso de uma identidade roubada como se fosse seu próprio certificado de identidade (por exemplo, passaporte, cartão de crédito etc).
-Fraude de transação: também chamada **fraude de comportamento**, ocorre quando um fraudador realiza transações usando credenciais falsificadas ou adulteradas.

A maioria das estratégias atuais de detecção de fraudes consiste no uso de **bases de regras** contendo a codificação de informação especializada e conhecimento passado de comportamento fraudulento. No entanto, devido à rapidez com que novos métodos de fraude são criados e utilizados, as bases de regras são obrigadas a constantes mudanças com tendência a crescer a um ritmo acelerado, atingindo rapidamente um tamanho incontrolável. Além disso, em muitos casos, estes conjuntos de regras devem ser configurados manualmente, de forma diferente para cada cliente / usuário, isto muitas vezes pode levar dias ou semanas até estar operacional e necessita ser atualizado com novas ocorrências. Também falta a capacidade de previsão para este tipo de sistema, fazendo com que eles percam as ameaças e fraudes que não tenham sido definidas previamente.

Outra característica-chave de muitos produtos existentes para detecção de fraude é o papel central desempenhado pela **identificação do dispositivo** para validar a identidade do usuário. A utilidade de se identificar o dispositivo é limitada, pois um fraudador pode assumir o controle do equipamento da vítima, descobrir e reproduzir seu histórico de uso, operar a partir desse ponto de acesso, falsificar ou adulterar o padrão de navegação e de transações da vítima.

A dependência do uso de informações baseadas apenas em regras de correspondência e de ambiente, limita a eficácia da maioria dos produtos existentes para detecção de fraudes.

Diante deste cenário adotamos uma abordagem inovadora para o problema:

Monitorar transparentemente o comportamento biométrico do usuário;
Analisar os dados; combinando padrões e técnicas de aprendizagem de máquina.

O PluriPass e BioTracker são a aplicação prática desta tecnologia.

*** Logo ao se digitar usuário e senha, o PluriPass combina o processo de autenticação habitual com o da biometria comportamental monitorando o modo como cada usuário insere suas credenciais, compara estes dados com os respectivos perfis. Isto amplia a eficácia do controle desde o primeiro momento de acesso a rede.**
*** Após autorizado o acesso, entra em cena o BioTracker com a autenticação contínua, que combina três diferentes estratégias de monitoramento: *Monitoramento da biometria comportamental, Processo de acompanhamento de sessão e Monitoramento do comportamento na rede*.**
Este sistema de acompanhamento permite ampliar a faixa de detecção de fraudes, identificando ações operadas por indivíduos ou executados de forma automatizada.

A combinação destas aplicações significa *Inovação e Confiabilidade*, elevando a segurança contra fraudes na web para nível nunca antes alcançado!

www.globalmindsit.com.br
GLOBALMINDS – Consultoria, Serviços de TI e Gestão
End.: Av. Almirante Tamandaré, 94 – Sala 610 - Coqueiros - CEP: 88080-160 - Florianópolis/SC
Tel.: (48) 3879-6500 - E-mail: globalminds@globalmindsit.com.br