91 – Setembro 2007

Proteja sua imagem virtual: biscoitos

Depois de falarmos de pescaria no último mês, que tal começarmos hoje com biscoitos?

Pois bem, você vai ao computador, digita o endereço daquele site de buscas que costuma utilizar e mal clica o mouse, já é saudado com uma mensagem nominal de boas vindas como se o computador o tivesse reconhecido instantaneamente.
Em seguida, você digita a palavra JAVA e a ferramenta traz para você centenas de links cuidadosamente ordenados, priorizando àqueles relacionados à linguagem de programação, ao invés daqueles relacionados à ilha vulcânica da Indonésia. Tudo como se o sistema pudesse ter lido seu pensamento e descoberto que você não é professor de geografia e, portanto, interessado na ilha, mas sim um programador de computador justamente à procura de novidades tecnológicas.

Como se não bastasse, durante as incursões de busca começam a surgir links patrocinados nas telas de resultado que insistem em oferecer equipamentos fotográficos, serviços de revelação de filmes e afins, até então inexplicavelmente, como se mais uma vez o sistema tivessem adivinhado que eu acabara de adquirir uma moderna câmera fotográfica dias atrás.

Pois o responsável por toda essa mágica é o tal biscoito, ou *cookie*, que mencionei no início do artigo. Não se trata de uma tecnologia totalmente nova, mas vem ganhando novas aplicações ano após ano. Em linhas gerais, são pequenos arquivos de dados trocados entre servidores de sites Internet e browsers de navegação, usados para autenticar, rastrear e manter informações específicas dos usuários. São arquivos simples sem condições de executar qualquer instrução por si mesmos e ainda não podem ser contaminados por vírus ou serem escritos para agir como tal. O principal motivador de seu uso é a possibilidade de tornar a experiência do usuário mais agradável, fácil e ágil, assumindo que depois de visitar um determinado site e fornecer certas informações pessoais, preferências e escolhas, o usuário não terá de informá-las novamente nas futuras visitas.

Foi por isso que o site de buscas usado na ilustração inicial descobriu seu nome e o saldou ao acessar o site novamente. Foi também pelo mesmo motivo, que depois de diversas buscas relacionadas a computador e tecnologia, ele presumiu que, ao procurar pela palavra JAVA, a probabilidade de seu interesse estar relacionado à ilha do Pacífico era menor do que a linguagem de programação. Ah! E não podemos nos esquecer da mágica dos links patrocinados. Neste caso, o mesmo mecanismo de busca armazenou em um *cookie* e "aprendeu" com as buscas recentes que você andou fazendo. Muitas dessas buscas estavam relacionadas a sites de comparação técnica de câmeras fotográficas, marcas e preços, o que o fez acreditar que você poderia ter adquirido ou tinha intenção de adquirir equipamentos fotográficos.

Analisando superficialmente, a tecnologia *cookie* e sua aplicação vêm transformando positivamente a experiência de qualquer usuário, afinal, quem não gosta de ser tratado pelo

SÊMOLA

nome, que não goste de ter um vendedor já conheça seus gostos, suas vontades e que por isso, você possa lhe oferecer um serviço customizado? Contudo, tudo tem seu preço.
Ampliando a análise, podemos ver potenciais problemas relacionados à privacidade do usuário. Podemos começar pelo problema de se armazenar senhas de acesso ou dados de cartão de crédito em arquivos de *cookie*, o que naturalmente representa risco caso o computador do usuário seja comprometido por uma invasão. Além disso, existe o risco inerente ao fato de que cada site Internet pode criar seu próprio *cookie*, definir sua própria regra interna de coleta e armazenamento de dados, e pior, sem que o usuário conheça essas regras e tenha, mesmo que passivamente, o direito de escolha. Na prática, ninguém sabe ao certo o que se coleta, por quanto tempo se coleta, como se armazena, por quanto tempo se armazena, e principalmente, como esses dados serão utilizados e por quem.

Em uma reação imediata por reflexo, é até possível julgar o assunto sem muita importância, especialmente quando nos limitamos a pensar no exemplo do site de buscas e naquelas poucas palavras soltas que escrevemos e ordenamos que localizasse. Mas na prática não funciona assim. É como se estivéssemos ajudando a montar um grande quebra-cabeça, onde cada peça revela um novo pedaço da imagem final, seu perfil, sua personalidade, sua individualidade. Reunindo palavras soltas de um usuário freqüente durante meses, é possível conhecer mais sobre ele do que se pode imaginar. Faça você mesmo um exercício. Como se você não se conhecesse, tome nota das palavras que procurou na última semana e com base nelas, veja se é possível traçar ao menos um primeiro perfil. Imagine agora um estranho conhecendo-as depois de monitorar você durante um ano inteiro. Esse conhecimento, supostamente privado, poderia lhe oferecer algum tipo de risco, seja pessoal ou profissional?

É verdade que as versões mais modernas dos navegadores Internet já permitem, mesmo que de uma forma ainda muito discreta, que o usuário aceite ou rejeite o cookie de um site específico, contudo, sabemos que muitos deles simplesmente não funcionam bem caso o recurso seja rejeitado, o que coloca o usuário em outra sinuca.

Como mencionei algumas linhas atrás, a mágica que o *cookie* proporciona encanta de verdade, mas tem seu preço. O que não significa dizer que não existam usuários interessados em pagar este preço por verem vantagem legítima nele. O tema é delicado e vem despertando a preocupação de diversos países como os Estados Unidos e membros da União Européia. Entretanto, o que decididamente me contraria, não é a existência do *cookie* ou ainda o tempo em que o arquivo expira e deixa de coletar dados, mas sim o fato de não existirem mecanismos padronizados, de fácil uso e ainda políticas definidas e transparentes o bastante para deixar que o usuário faça sua escolha, permitindo que ele próprio decida que nível de risco está disposto a correr.

Marcos Sêmola *é Diretor de Operações de Information Risk da Atos Origin em Londres, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*