92 – Outubro 2007

Hora da segurança deixar de ser cereja

Muitas tortas já foram idealizadas, fabricadas e consumidas, mas já é hora da segurança da informação deixar de ser apenas a cereja do bolo. Quero dizer, deixar de ser apenas um ingrediente extra, praticamente descartável, colocado em segundo plano e por vezes esquecido, para se tornar um ingrediente básico e fundamental para qualquer receita de qualidade.

Qualquer que seja o propósito da festa e o número de convidados, o bolo sempre precisa ser visualmente atraente, gostoso e acima de tudo, precisa ser feito com ingredientes frescos e saudáveis adequadamente misturados como manda a boa receita, para que ganhe estrutura e suporte as intempéries e os longos períodos de espera até ser finalmente consumido.

Aqueles bolos de última hora em que a massa racha, o recheio desanda, mas mesmo assim consegue atrair os olhares dos convidados por conta da cobertura ou da cereja que se usou para mascarar a falta de estrutura e qualidade, já não funcionam mais, ou funcionam apenas até a primeira mordida. Quantos já não se viram engajados em descartar uma fatia de bolo de festa logo depois de experimentá-la?

Estamos vivendo este mesmo momento com a segurança da informação. Projeto de software que sai da prancheta sem considerar este componente, ou é interrompido antes mesmo de chegar ao consumidor final, ou chega até ele internamente desestruturado, mas embrulhado em um belo papel de presente capaz de convencer no primeiro momento, mas enlouquecer o consumidor depois de desembrulhado. Os números falam por si só. Centenas de vulnerabilidades são descobertas mensalmente nos programas de computador mais populares do mercado. Mas o problema está longe de se limitar aos produtos comerciais. Dentro das empresas o problema parece ainda mais caótico. Softwares desenvolvidos por equipes internas, em geral, sofrem pela falta de tempo, padronização, documentação, recursos, mas especialmente pela falta de consciência e competência específica para reunir todos os componentes básicos de uma receita de qualidade.
Quando perguntadas sobre os aspectos de segurança, as equipes de projeto respondem na maioria dos casos: não temos especialistas multidisciplinares e verba suficiente para pensar nisso agora. A pressão para entregar o produto funcional é muito alta. Por isso, deixamos que o marketing cuide desse aspecto e embale bem o produto para que o usuário se sinta confiante e seguro.

Duras verdades de projeto que precisam ser endereçadas:

- *Segurança custa caro, mas sua falta pode custar muito mais;*
- *Os impactos da falta de segurança estão hoje mais ligados aos resultados de negócio e podem ser mais facilmente quantificados;*
- *Segurança é um componente estrutural de qualquer projeto e precisa estar na receita desde o início;*
- *Para que a segurança não seja a responsável pelo atraso do projeto, ela precisa ser planejada e orientada ao contexto;*

- *Como componente importante, a segurança também precisa de orçamento próprio e equipe especializada para se integrar amigavelmente ao projeto;*
- *A sustentabilidade de um produto é, mais do que nunca, vital. Parecer seguro é importante, mas não mais do que ser efetivamente seguro, quero dizer, ter sido amparado por medidas de redução de riscos.*

É assim que o mercado, em geral, tem funcionado até então. Empresas vendendo e consumidores comprando apenas a "paz de espírito" através da promessa de segurança em produtos e serviços. Mas já é hora de acabar com isso. A relação de causa e efeito da falta de segurança em produtos e serviços de tecnologia da informação já ultrapassou os patamares toleráveis. Os investidores e *stakeholders* já andam descontentes com a perda de lucratividade e com a dificuldade de absorver os prejuízos diretos e indiretos. Onerar os preços para os usuários finais já não funciona como antes, pois afeta a competitividade, cada vez mais acirrada, e provoca perda substancial de oportunidades de negócio.
A indústria do dinheiro de plástico, por sua vez, já cansou de exercitar apenas a criatividade no combate à fraude e partiu para uma grande fusão de padrões de segurança, o que originou o PCI-DSS ou Payment Card Industry – Data Security Standard. A partir de agora, não basta dizer que é seguro. É preciso efetivamente programar medidas mais abrangentes e se submeter a auditorias qualificadas regulares para mostrar que, entre outras coisas, seu software de pagamento adotou as melhores práticas de segurança para aplicações e seu perímetro operacional está em conformidade com o PCI.

Não me refiro ao PCI como a solução do problema, assim como também não o fiz com a BS7799, ISO15408, ISO 17799 e a mais recente ISO27001. São apenas padrões que buscam definir as melhores práticas, e é só. Entretanto, têm grande importância na medida em que se tornam reconhecidos mundialmente e são usados como referência comum para auditorias e para as próprias equipes internas de segurança. Assim como uma bússola, indica apenas a direção, deixando a orientação precisa, comum aos GPS ou sistemas de posicionamento global, para os desdobramentos das normas e as políticas corporativas.

Seja como for, somente paz de espírito adquirida ao comprar uma marca ou uma bela campanha de marketing, já não sustenta empresas e consumidores. A brincadeira agora é para valer. Os softwares, mesmo que as falhas façam parte de sua natureza, estão fazendo tarefas cada vez mais importantes e valiosas. Suportam a operação de empresas inteiras, direta ou indiretamente, e são alvos freqüentes não mais de amadores, mas de profissionais da fraude. O resultado disso, é que os vazamentos, as invasões, os roubos de informação e os prejuízos ocorrem e, por seu volume, já não podem mais ser varridos para debaixo do tapete. Portanto, é hora de conceber o bolo com seriedade e planejar a segurança desde o início, priorizando os componentes estruturais e evitando a todo custo o sorriso azedo do consumidor depois da primeira mordida.

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*