39 – Abril de 2002

Seu SPB é uma bomba relógio?

Dia 22 de abril de 2002 o país comemora mais um aniversário, mais precisamente 502 anos. A mesma data marca também o início da operacionalização do Sistema de Pagamentos Brasileiro, que promete revolucionar o sistema financeiro nacional.

Diariamente muito se escreve e, conseqüentemente, se lê sobre o assunto. O impacto das mudanças trazidas pelo SPB é tão forte que extrapolou os ambientes executivos das instituições financeiras, atingindo empresas dos mais diversos segmentos de mercado e envolvendo também diferentes perfis de profissionais com uma diversidade de preocupações, dúvidas e desafios, afinal todos acabam influenciados direta ou indiretamente por mudanças na forma de receber e pagar valores.

Os efeitos do SPB já estão sendo comparados ao Bug do ano 2000, que mobilizou muitos recursos físicos, tecnológicos, humanos e principalmente financeiros a fim de evitar surpresas em seus negócios quando os sistemas passassem a representar o ano terminado em 00. A preocupação com a impossibilidade de operar a partir do primeiro dia do novo ano e o risco de problemas em cascata provocados por sistemas e equipamentos "loucos" que estariam realizando cálculos equivocados, iniciando ou interrompendo processos fora do tempo e ainda manipulando informações sem aferição com a data correta, podem ter mostrado ao mundo a projeção de parte dos efeitos a que estaremos sujeitos agora.
Não é para menos, afinal a proposta do Banco Central do Brasil promove uma transferência de risco, até então centralizada no próprio BACEN, para as instituições financeiras. Desta forma, proporcionará a redução exponencial do risco sistêmico a que o país está sujeito, seguida de maior eficiência do sistema de pagamentos, compensação e liquidação de valores, que passarão a operar eletronicamente e em real time a partir de uma rede de computadores integrada.

Mais uma vez olhando para as mudanças, vemos que existem níveis ou perímetros distintos onde os efeitos se darão em série com se ocorresse um efeito cascata. Uma comparação bem-humorada para representar esses perímetros dentro da estrutura do SPB seria a cebola por sua constituição em camadas. O centro pode representar as empresas envolvidas diretamente com a fase inicial do sistema, ou seja, as instituições bancárias, câmaras de compensação e o próprio Banco Central. Imediatamente, externa ao núcleo, vemos mais uma camada que pode representar as operadoras de cartão de crédito, financeiras, seguradoras etc. As camadas exteriores da cebola, representariam as empresas que movimentam grandes valores, empresas médias e pequenas e o cidadão.

Até agora, estamos tratando de uma das dimensões, que esta relacionada aos impactos ligados à mudança operacional do sistema financeiro que atingirá a todos, cada um em seu perímetro e a seu tempo. Diante disso, não podemos esquecer os efeitos colaterais desta primeira fase, por exemplo, os reflexos na tesouraria das empresas por estarem despendendo altos valores para pagamento de bens de consumo e matéria prima - transação esta que se processará preferencialmente em real time (D+0) – e por estarem ao mesmo

tempo recebendo montantes inferiores processados preferencialmente como antes, ou seja, com a duração de um dia mais dois para compensação (D+2).
Outro grande efeito colateral de alto impacto está atrelado à redução da possibilidade de negociar os valores sob sua custódia (float), reduzindo seu capital de giro, durante o período de inércia em função do atual processo de compensação. Estimativas anunciadas segundo estudo da Federação as Indústrias do Estado de São Paulo (Fiesp) mencionam que a indústria de transformação irá perder capital de giro na ordem de R$1,3 bi por mês. Desta forma, todos terão de otimizar seu processo de gestão dos fluxos de caixa.

Todos benefícios do Sistema de Pagamentos Brasileiro para o sistema financeiro nacional e seus integrantes, e os efeitos colaterais que foram analisados acima, só irão se materializar se cada elemento fizer sua parte. Outra analogia interessante podemos fazer usando o motor de um automóvel. Imagine um veículo enorme movido por aproximadamente 164 motores de porte e potência variadas (164 instituições financeiras) que operam de forma integrada sob antigas regras, ferramentas e critérios. Imagine então que estas regras, ferramentas e critérios estejam recebendo sugestões de mudança que precisam estar prontas em data acordada pelos responsáveis por cada motor.

A sequência de perguntas que temos de fazer é:

- O “engenheiro” de seu “motor” tem pleno conhecimento das mudanças propostas?
- A equipe do projeto está afinada e pronta para atender as especificações até a data acordada?
- Seu “motor” estará pronto para ligar no dia 22 de abril de 2002?
- Você pode imaginar os reflexos para todo o “veículo” se muitos motores deixarem de funcionar no dia D?
- Você pode imaginar se apenas o seu “motor”, logo o mais potente de todos, for o motivo do comprometimento do veículo?

Neste momento, passamos a falar dos desafios e das preocupações que cercam cada uma das empresas envolvidas diretamente na operacionalização do sistema. Tudo pode ser entendido como uma grande rede de confiança composta por centenas de nós representados pelas instituições participantes, que tem que se preocupar com a sua função no processo. Todas tem de garantir os níveis de confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações que passarão a enviar e receber eletronicamente através do sistema.

Apesar de o segmento financeiro ser um dos que mais investem em segurança da informação e, portanto, ser um dos mais preparados e maduros para administrar riscos, em se tratando de SPB, proponho um teste de sanidade do seu “motor” a partir de perguntas que o tranqüilizará ou o deixará ainda mais preocupado.

1. Possui um responsável pelo SPB e uma equipe dedicada à sua implementação?

2. Os ativos físicos, tecnológicos e humanos foram adequadamente segmentados dos demais ambientes?

3. Os servidores que suportam a aplicação SPB são dedicados ao sistema e, portanto, não são compartilhados com outras aplicações?

4. O ambiente físico SPB recebeu recursos de controle de acesso e auditoria para atender aos níveis de criticidade que este processo de negócio requer?

5. Os sistemas operacionais foram instalados e configurados considerando o alto grau de confidencialidade que as informações necessitam?

6. Foram instalados dispositivos de segurança como Firewall sem que suas configurações padrão fossem displicentemente mantidas?

7. Foram realizadas análises técnicas de segurança abrangentes a fim de mapear as falhas de segurança de forma a possibilitar sua correção a tempo?

8. As aplicações especialistas SPB foram testadas e desenvolvidas – internamente ou por terceiros – dentro dos critérios de qualidade considerando manutenibilidade, documentação, padronização e engenharia de software?

9. A chave privada que permite a assinatura digital e garante a autenticidade das mensagens está sendo armazenada num equipamento (hardware HSM) especialista a fim de proteger adequadamente a sua confidencialidade, integridade e disponibilidade?

10. Possui normas, procedimentos e instruções específicas para o SPB, que definem critérios para acesso físico ao ambiente, acesso lógico ao sistema, manipulação do hardware criptográfico, backup, manutenção e operacionalização?

11. Possui mais de um fornecedor de certificado digital para suportar situações de indisponibilidade da autoridade certificadora?

12. Corrigiu todas as falhas de segurança previamente mapeadas e/ou implementou mecanismos de controle sobre as mesmas a fim de reduzir os riscos?

13. Implementou as recomendações de contingência que prevê a existência de um site backup espelho capaz de suportar situações de indisponibilidade?

14. Possui Plano de Contingência desenvolvimento e mantido especialmente para o SPB capaz de administrar situações de crise e garantir sua continuidade operacional?

15. Procurou orientação geral pela Norma de Segurança ISOO/IEC 17799?

Este checklist pode parecer severo, mas estamos diante de um novo e importante processo de negócio materializado na forma de sistemas, redes de computador e mensagens, que possui tolerância zero, ou seja, não permite estorno de ações, erros físicos, tecnológicos e humanos ou qualquer outra ocorrência que possa comprometer seu íntegro funcionamento.

Assim sendo, deixo no ar um último questionamento: Seu "motor" pode estar preparado para ligar, mas será que está pronto para suportar uma longa e interminável viagem?

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente Nacional de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br