19 – Maio de 2000

Evite que sua iniciativa de E-business se transforme em E-problem

Ouve-se falar de e-business por toda parte. Fusões, aquisições milionárias, empresas virtuais de pouco mais de 3 meses valendo mais do que sólidas corporações de 50 anos de existência e ainda a comercialização indiscriminada de endereços no espaço. Ou seja, endereços virtuais (URLs como www.suaempresa.com.br) que criam num piscar de olhos ou no assinar de um cheque, novos ricos executivos que mal saíram da puberdade.

Esta é a nova economia, onde os comportamentos se diferem do mundo real e onde iniciativas que só existem no papel em forma de idéias, valem mais do que empreendimentos fisicamente concretos e palpáveis. Pensando justamente em pegar a onda do ciberespaço e ver sua empresa real modernizada, ou até mesmo iniciar uma nova atividade já no ciberespaço, muitos executivos correm atrás da tecnologia e logo inauguram seu negócio virtual.

O *webdeveloper* implementa os mais novos recursos de Java, Html e multimídia em prol da boa navegabilidade. O *marketeiro Internet* ajusta as diretrizes e ações para atingir o público diferenciado e de comportamento sensível ao contexto. O *webdesign* dá todo o brilho atrativo que a interface deve ter, explorando os banners dos anunciantes e cativando o consumidor. O *webmaster* coloca e mantém a aplicação, ou melhor, a empresa no ar. Chega então a hora de pensar na logística do processo e dimensionar a infra-estrutura para garantir o pagamento, a entrega, o recebimento e a satisfação do cliente. É exatamente aqui que os problemas começam a aparecer.

Formas de pagamento pouco seguras tomam conta do e-business. Surgem iniciativas amadoras de assinatura em arquivo, onde o armazenamento local não recebe qualquer proteção. Transferência de informações como números de cartão de crédito sem a privacidade e integridade oferecidas pela geração dinâmica e a troca de chaves de sessão. Ausência de certificados digitais para autenticar as máquinas servidora e consumidora e garantir o não repúdio. O possível descaso com a infra-estrutura tecnológica que pode pôr em risco a disponibilidade da aplicação.

Com todas estas deficiências, o que parecia inevitavelmente promissor pode transformar-se em um grande problema! O descrédito provocado por uma fraude, aliado à possível ineficiência logística de recebimento e agravado pela publicidade negativa que logo toma conta da mídia, podem pôr não só o negócio virtual em jogo, mas também atingir sua marca.

Reverter este quadro depois de instalado não é fácil e normalmente requer o dobro de esforço, se não mais, do que o necessário para fortalecer o posicionamento. Assim, quando se pensa em modernização e aproveitamento de todos os benefícios da nova economia, não deve-se deixar de analisar todos os elementos que fazem parte da iniciativa de e-business. Errar no ciberespaço é como andar para trás.

Seguem algumas dicas para evitar surpresas no ciberespaço:

Boas práticas genéricas:

- Evite utilizar a última tecnologia disponível, o que pode resultar em incompatibilidades e a conseqüente redução do seu mercado.
- Torne a compra virtual atraente ao consumidor agregando valor, seja na velocidade de entrega ou na personalização do atendimento.
- Estabeleça um canal direto de comunicação com o consumidor e esteja preparado – a qualquer momento - para adequar seu site às necessidades dele.
- Preocupe-se com a seleção da mercadoria. Comporte-se como se o consumidor estivesse em sua loja real, oferecendo o que há de melhor.
- Cumpra à risca todas as promessas feitas no site, como horário de entrega, devolução de mercadorias etc.
- Exale credibilidade implementando medidas de segurança não só no momento do pagamento, mas onde houver informação. Torne pública estas medidas e mostre sua preocupação em proteger também o consumidor.

Boas práticas de segurança:

- Garanta a proteção das informações que sustentam o negócio, em todos os ambientes:
  1. Examine o negócio e identifique todas as vulnerabilidades.
  2. Implemente criptografia SSL na aplicação web, a fim de estabelecer uma conexão segura com o consumidor, principalmente no momento da formalização do pagamento.
  3. Identifique e, se possível, autentique o consumidor com o uso de certificados digitais e smartcard, por exemplo. Assim, estará evitando o não repúdio.
  4. Implemente dispositivos de controle de acesso físico ao ambiente e adeque-o à infra-estrutura: climatização, incêndio etc.
  5. Implemente um firewall e configure-o de forma conservadora, ou seja, retire todos os serviços no primeiro momento, habilitando apenas os necessários, sob demanda.
  6. Implemente um roteador com filtro, inibindo tentativas de invasão e comportamentos suspeitos.
  7. Implemente um software de Intrusion Detection para combater tentativas de ataque documentadas e gerar ações automatizadas.
  8. Implemente uma VPN – Virtual Private Network - para relacionamentos business to business .
  9. Implemente um plano de contingência, a fim de garantir a operação das atividades essenciais do seu negócio online, em caso de acidentes.
  10. Atualize seus sistemas operacionais regularmente com os *hotfixes e patchs* disponibilizados pelos fabricantes.
  11. Atualize com regularidade os softwares antivírus.

12. Monitore constantemente o funcionamento do seu negócio, a fim de perceber com velocidade, sinais de invasão e mau uso dos recursos disponibilizados.
13. Implemente a *Classificação da Informação*, assim todos saberão o que fazer diante dos dados a serem manipulados, transportados, armazenados e descartados.
14. Tenha uma *Política de Segurança* personalizada, de acordo com a tecnologia, a cultura e o modelo de gestão da empresa. Isto norteará os usuários e técnicos quanto às melhores práticas de uso da tecnologia e o manuseio da informação.
15. Conscientize, sensibilize e divulgue a *Política de Segurança.*
16. Pense na possibilidade de ter um *Security Officer*, além de uma e equipe experiente e atenta aos problemas de segurança, capaz de reduzir o tempo entre a aparição de uma nova vulnerabilidade e a implementação da solução.

É importante ressaltar que cada iniciativa na Internet requer um nível de segurança próprio e adequado à natureza da atividade. Assim, se depois de todas essas dicas ficar claro que as atividades fogem à competência básica da sua empresa, é hora de entregar esta tarefa a quem realmente conhece o assunto: uma empresa especializada, com infra-estrutura dimensionada para suportar situações de contingência e futuras expansões. Uma empresa que disponha de especialistas capazes de combater ataques e invasões, identificar novas vulnerabilidades, antecipar a implementação das soluções, monitorar o ambiente 24 horas por dia, sete dias por semana e ainda manter o nível de segurança adequado.

Não há tempo para reinventar a roda, e a Internet não permite mais erros. Pense nisso.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Gerente de Produto da Módulo Security Solutions S.A.*
msemola@modulo.com.br