B00 – Fevereiro de 1999

Automação Bancária: e a segurança ?

Difícil recuar agora. Não é mais possível fechar os olhos para o que vem ocorrendo à nossa volta. Um movimento globalizado e rebocado pela tecnologia que vem se infiltrando em todos os setores da economia, servindo de tempero e permitindo que as empresas se diferenciem e agreguem valor aos seus negócios.

No setor bancário, não poderia ser diferente. Todo ano, o sistema financeiro precisa reavaliar as suas estratégias tecnológicas. Há muito, o Brasil está na ponta dessa evolução, otimizando processos, implementando novos sistemas e integrando o cliente. Seguindo essa tendência, milhões de reais estão armazenados nas memórias dos computadores.

É preciso automatizar ?
Com o estreitamento do mercado, a necessidade de se manter competitivo e a crescente demanda por serviços cada vez mais eficazes, foi importante seguir a tendência, materializando parte da solução na forma de Automação Bancária.

Um dos aspectos mais fortes é a estratégia de canais, segundo a denominação dos bancos. É sabido, que os bancos operam basicamente em cima de quatro canais de entrega: a agência bancária; o auto-atendimento; o call center e o home banking. Portanto, a automação bancária é uma das peças do quebra-cabeça tecnológico de maior importância.

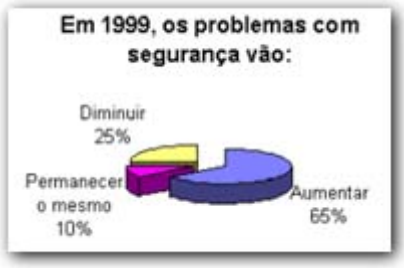
Ambiente complexo
Diversos elementos fazem parte de um ambiente de automação bancária. Desde a grande rede corporativa com sua malha de cabeamento estruturado, servidores, estações, hubs, switchs e roteadores, que juntos, configuram - na maioria dos casos - um ambiente heterogêneo. Não menos importantes, os links dedicados de dados, possíveis transmissores de rádio, infra-vermelho, satélite e as próprias aplicações (softwares) que se utilizam de toda a infra-estrutura de hardware. Do outro lado, os canais de entrega com seus terminais de auto-atendimento, teminais PDV, teclados pin, leitoras etc.

Já que falamos de conectividade, outro meio de transmissão de dados que tem se popularizado na maior parte das empresas, é a Internet. Apesar de ser uma malha pública e de segurança frágil, algumas soluções para implementação de VPN (*Virtual Private Network*) têm obtido excelentes resultados, permitindo a redução dos custos de transmissão e mantendo o padrão de segurança adequado à aplicações desse gênero.

Administração descuidada
O risco também é crítico no ambiente de Intranets. O modelo atual para segurança das redes tem assumido que o "inimigo" está do lado de fora da empresa enquanto que dentro, todos são confiáveis. Esta idéia tem feito com que os administradores de rede utilizem uma estratégia de segurança que restringe o acesso para qualquer usuário externo e por outro lado, libera de forma irrestrita o acesso aos servidores para a totalidade dos usuários internos. Esta estratégia, embora simples, não é adequada já que sabemos que a maior parte dos problemas ocorre em função de ameaças internas.

Automatizar com segurança

Apesar de toda polêmica em torno do assunto e do número cada vez maior de adesões corporativas, poucos compreendem e conhecem a infra-estrutura necessária para se ter a solução implantada adequadamente e que permita extrair os melhores resultados. É preciso ter cautela e consciência de que a tecnologia interfere no comportamento das pessoas e, em se tratando de uma atividade crítica - pois manipula valores virtualmente - a segurança passa a ser um assunto pontual e determinante para o sucesso da empreitada.



Fonte: 4ª Pesquisa Nacional sobre Segurança da Informação
Módulo Security Solutions S.A.
Conheça os resultados da pesquisa em www.modulo.com.br

O que é Segurança da Informação ?

Os princípios básicos da segurança são a confidencialidade, integridade e disponibilidade das informações. Quando aplicados, permitem reduzir os riscos com vazamentos, fraudes, erros, sabotagens, uso indevido, roubo de informações e diversos outros fatores que possam comprometer estes princípios. Mas os benefícios não param por aí. Consegue-se maior produtividade dos usuários através de um ambiente mais organizado e maior controle sobre os recursos de informática.

A segurança está atrelada à credibilidade e é pensando nisso - não só na tecnologia, mas na tecnologia aplicada ao negócio - que a empresa brasileira líder em segurança da informação, presta consultoria, visando a minimizar as vulnerabilidades deste ambiente informatizado tão complexo.

A solução

O planejamento deve estar modularizado e se inicia com a análise do ponto de vista de um ambiente desejado, apontando recomendações de segurança para melhoria do ambiente encontrado. Baseiam-se no levantamento dos riscos, identificando as vulnerabilidades e ameaças, permitindo assim, gerar elementos para a tomada de decisões estratégicas.

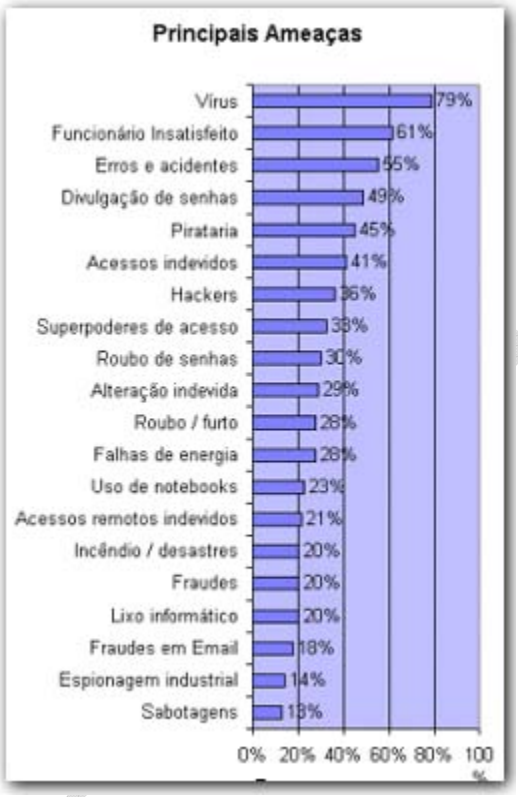
"A análise e a gestão inteligente
dos riscos é um dos mais
importantes desafios da empresa
empreendedora."

Passaporte para o Ano 2000

Luiz Kauffman

Vulnerabilidades e ameaças

As vulnerabilidades estão se tornando "comodities" e as ameaças para a segurança, antes restritas a especialistas e estudiosos, passam a estar disponíveis gratuitamente na Internet. Assim como os programas para fraudar senhas, disseminar vírus, monitorar redes, identificar fragilidades e atacar servidores que resultam na paralisação de redes etc.



Fonte: 4ª Pesquisa Nacional sobre Segurança da Informação
Módulo Security Solutions S.A.

A próxima etapa é a especificação de uma Política de Segurança adequada e moldada à empresa, formada por normas, procedimentos e instruções de segurança. Uma política baseada em regras estratégicas, táticas e operacionais, apoiada no desenvolvimento da cultura de segurança entre os usuários, uso de ferramentas tecnológicas e monitoramento constante. Seu principal objetivo, é reger as atividades ligadas à segurança da informação, mantendo-as dentro dos padrões de segurança que garantam a continuidade dos seus processos, evitando problemas que causem prejuízos à confiabilidade dos serviços.

É importante que haja um programa de conscientização e a sinalização da alta administração, demonstrando apoio à política, sem o qual não se consegue a adesão suficiente.

> "Apesar do alto índice de sensibilização, apenas 67% das empresas possuem uma Política de Segurança formalizada e, na maioria dos casos (69%), está desatualizada, não contemplam todos os ambientes ou não é conhecida pelos usuários."
>
> 4ª Pesquisa Nacional sobre Segurança da Informação
> Módulo Security Solutions S.A.

A solução completa é composta por:

- Política de Segurança Corporativa;
- programa de treinamento e capacitação dos técnicos e usuários;
- recursos e ferramentas específicas para a segurança e
- monitoramento constante do "log" e trilhas de auditoria.

Conclusão
Os esforços e investimentos em segurança continuam sendo subestimados pelas empresas. Contudo, é importante mudar este cenário, de forma que estejam atentas para a necessidade de uma Política de Segurança Corporativa que contenha diretrizes e orientações claras, objetivas e adequadas para minimizar os riscos e reduzir o impacto sobre seu negócio.

O que se espera nesta etapa do processo, é que as empresas possam assimilar as novas regras de segurança, transformando-as em parte integrante da sua cultura, incorporando-as às atividades de seu cotidiano com naturalidade. Tudo para fomentar esta nova fase da gestão de tecnologia.

Só desta maneira, atingindo a maturidade, terão um processo importante como a Automação Bancária, implantado com eficiência e com a certeza de estarem prontas para uma próxima evolução.