SEGURANÇA

Por Ricardo Humberto

A prioridade do momento

Cuidar da segurança das informações digitais que uma empresa lida é, a cada ano, mais crítico, mas não impossível. Mesmo com as rápidas mudanças tecnológicas, o mercado possui sempre boas soluções e especialistas sobre o assunto. Desde a preocupação com o mainframe, na década de 70, passando pela chegada dos micros, na década de 80, até a internet, a criticidade vem sendo controlada, fazendo a informação circular segura e acessível entre empresas, clientes e consumidores finais

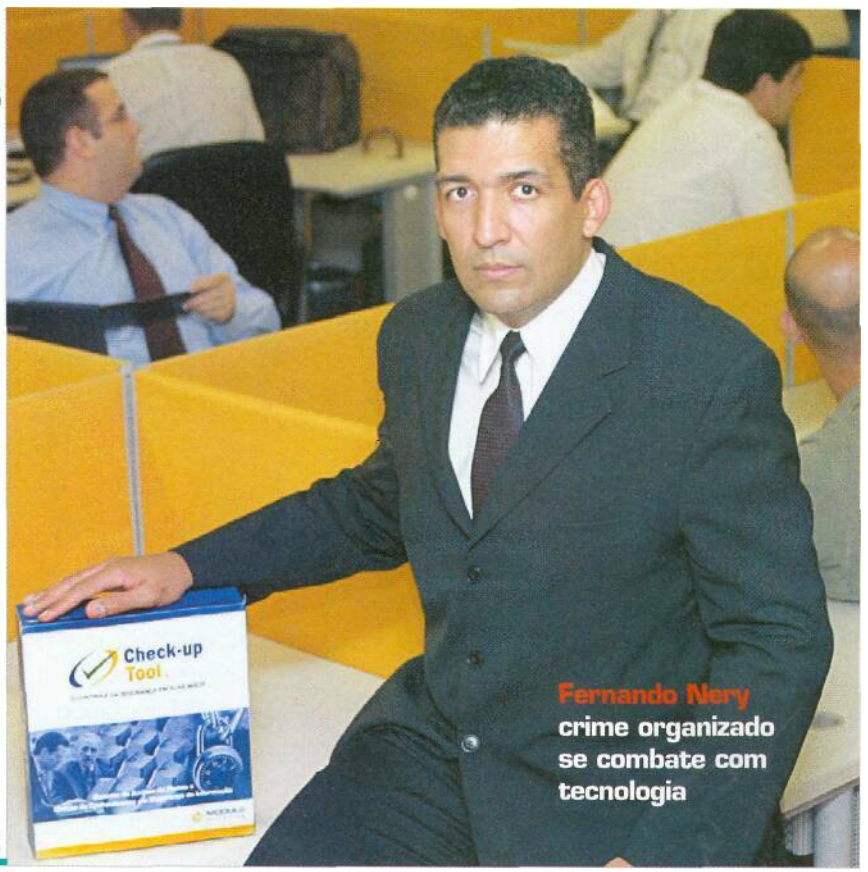
Apoio: Check Point We Secure the Internet. McAfee MODULO security 2005 • 20anos SCUA Segurança da Informação

CADA VEZ MAIS A SEGURANÇA DA INFORMAÇÃO DEIXA DE SER UM CUSTO PARA AS EMPRESAS, PELO MENOS PARA AS QUE PREZAM POR DESENVOLVIMENTO E CUIDAM DE SEUS NEGÓCIOS. O INTERNATIONAL DATA CORPORATION (IDC) EM RECENTE EVENTO, REALIZADO EM ABRIL, CONSTATOU QUE A PROTEÇÃO DA INFORMAÇÃO É UM DOS PRINCIPAIS ITENS DA LISTA DE PREOCUPAÇÕES DAS EMPRESAS NOS ÚLTIMOS TRÊS ANOS. E, em 2005, o item estará entre as prioridades de investimentos em TI, variando entre o primeiro ou segundo lugar. E foi essa a prioridade que levou executivos de diversos

segmentos ao Executive Meeting 2005, realizado no último mês de abril e que teve como objetivo discutir muito mais do que segurança. Empresas e fornecedores de tecnologia levaram as principais estratégias para combater fraudes e principalmente atender às novas legislações de regulamentação da segurança, como a Basiléia II e a lei Sarbanes-Oxley, que exigem novos processos internos.

E um dos principais caminhos do crescimento do item segurança nas companhias é que o assunto deixe de ser hermético e ganhe contornos de estratégia de negócio das corporações. Segundo Fernando Nery, sócio-fundador da Módulo, esse ainda é o grande desafio da área de tecnologia das empresas: que o departamento de segurança cuide das tecnologias e as ameaças de todas as áreas da empresa. "O crime organizado se combate com tecnologia, ainda mais numa época em que quadrilhas possuem tecnologia wireless e criptografia avançada", destaca o executivo. Outro dilema enfrentado pelas companhias é como falar em segurança da informação para grandes executivos. "A tarefa exige que os profissionais de segurança tenham o conhecimento de tecnologia e apliquem os mesmos nas diversas frentes de negócios da corporação", destaca Nery.

E as invasões são um perigo em diversos setores da economia, seja nos bancos com o volume de transações diárias realizadas na internet por seus clientes, empresas de telecomunicações com o perigo da clonagem de tecnologias, e as operadoras de cartões de crédito em evitar fraudes milionárias. Outro termômetro que evidencia a preocupação maior com a segurança é o crescimento das equipes que atuam nessa divisão, principalmente em companhias de grande porte.



Regulamentações

Nas instituições financeiras, o assunto ganha mais peso, além do monitoramento da segurança elas têm a preocupação de obedecer a mandatos do Banco Central e, portanto, precisam se adequar às novas regulamentações. Uma das leis é a Basiléia II, de 1988, que estabeleceu práticas mais transparentes de apresentação de balanços incluindo cálculo para o capital mínimo, riscos de crédito e operacionais dos bancos.

Outra regulamentação que virou palavra de ordem para o setor financeiro e para empresas globais é a Lei Sarbanes-Oxley,

focada no controle interno e que torna explícita a responsabilidade de CEOs e CFOs pela estrutura e controle das empresas (veja quadro nesta reportagem).

Uma das empresas que buscam a adequação às novas regulamentações foi a Petrobrás, que se alinhou à lei americana Sarbanes-Oxley em seu ambiente de TI. Segundo Alfred John Bacon, gerente de certificação de controles internos de TI da estatal, hoje é possível obter controles mais eficientes de governança corporativa, além de sistemas de acesso de usuários e processos de continuidade do negócio. "Com a Sarbanes-Oxley, mostramos que temos uma melhor gestão de controles internos e as melhores práticas para melhor documentar e avaliar os controles, sendo todos testados e aprovados", revela o executivo.

Com o intuito de permitir ainda mais segurança aos negócios da empresa, a Xerox do Brasil implementou um novo "Plano Diretor" de segurança da informação para se alinhar às novas agências reguladoras e leis nacionais. O objetivo foi se adequar às novas práticas corporativas de desenvolvimento de sistemas e também à Lei Sarbanes-Oxley.

Para tanto, a empresa implementou diversos processos para avaliar as possibilidades de invasões e colocar em prática políticas corporativas de sistemas de segurança da informação. Para Arnaldo Cadena, gerente de segurança da informação, infra-estrutura e arquitetura de TI da Xerox do Brasil, a empresa obteve diversos ganhos em adquirir as soluções de segurança da Módulo, sendo o principal deles barrar a possibilidade de informações estratégicas vazarem para hackers ou criminosos digitais. "Para nós, a informação é um ativo de muito valor e muito mais importante que qualquer produto comercializado pela companhia", destaca ele.

Ele lembra que uma falha de informação interna pode causar grande queda na participação de mercado. A companhia realizou também um intenso trabalho de conscientização em todos os departamentos para lembrar aos seus colaboradores a importância de proteger seus sistemas de ameaças externas.

Inteligência combativa

Imagine o estrago causado por um invasor entrando no sistema de um banco com 386 agências, 2,8 milhões de clientes e 10,6 bilhões de depósitos ao ano. Esse é o cenário do Banco Estadual do Rio Grande do Sul (Banrisul), que, mesmo investindo a robusta soma de 87,9 milhões de reais anuais, ainda se preocupou em fortalecer a proteção com um sistema mais eficiente de segurança adquirido junto a fabricante de software especializada na área Mcafee: a solução Intrusion Prevetion Systems (IPS). A plataforma se replica virtualmente em diversos

A Basiléia II

Com previsão para entrar em vigor a partir de 2007, o acordo de capitais Basiléia II exige dos bancos um sofisticado esforço gerencial e tecnológico para conhecer, mensurar e cobrir riscos operacionais, de crédito e de mercado, criando um novo paradigma para as melhores práticas de administração na indústria bancária. Quando forem publicados os novos parâmetros para gestão do risco bancário – pelo Banco de Compensações Internacionais (BIS) e pelo Banco Central do Brasil – será configurada a necessidade de um salto significativo na qualidade e no refinamento das bases de informações para gestão de riscos, o que implicará mudanças em vários níveis da infra-estrutura de TI dos bancos. As instituições que não se adequarem arcarão com o ônus de ter de provisonar cada vez mais capital próprio para fazer face a esses riscos. O maior desafio de Basiléia II aos gestores de risco e aos CIOs dos bancos será modelar uma sofisticada base de dados incorporando todas as variáveis associadas aos riscos operacionais, de crédito e de mercado, com uma amplitude temporal superior a cinco anos, com vistas à tomada de decisões baseada em informações de alta qualidade sobre as probabilidades de perdas futuras.

lugares da rede, discriminando ataques na web e criptografados, com alerta vermelho identificando qual a natureza da invasão. Segundo Vilmar Mendonça, coordenador da área de segurança de rede do Banrisul, o objetivo foi otimizar uma rede complexa composta de mainframe, Unix, Windows, ambiente de agenda e de clientes."Antes tínhamos diversos sensores que geravam vulnerabilidade no sistema *e* baixo desempenho da rede", lembra o executivo.

A preocupação do banco foi maior após o serviço de inteligência da Polícia Federal ter detectado o perigo de uma quadrilha especializada em golpes constantes a grandes redes, que ameaçava entrar no sistema do banco. E com a formação de uma rede de "inteligência coletiva" entre o Banrisul, a Polícia Federal e o Banco do Brasil, a quadrilha foi capturada. O executivo explica que, com a solução da Mcafee, o banco conseguiu fazer várias pontes físicas de comunicação, detecção e prevenção em tempo, com implementação de menor custo do mercado, sem prejudicar a rede, e de fácil configuração. "Temos uma visão microscópica do que está ocorrendo em qualquer local de nossa rede", ilustra Mendonça. Hoje, o banco já está numa fase de "perícia" e proteção ao cliente, uma parte que se autofragiliza rapidamente por aceitar os e-mails em anexo em seu computador pessoal. "E difícil controlar o cliente na outra ponta, ver quem utiliza vírus desatualizado", diz ele. A idéia é conscientizar seus usuários externos com orientação para protegê-los de forma massiva para que, ao entrarem no Internet Bank, estejam certos de que aquela é verdadeiramente a página de seu banco. B2B

Desafios da Lei Sarbanes-Oxley

Após a enxurrada de escândalos contábeis de 2001, os EUA exigem relatórios completos e transparentes nos quais as companhias mostrem que regulam os procedimentos internos. Esse foi o intuito da criação da Lei Sarbanes-Oxley, que determinou a certificação de controles internos e resultados financeiros divulgados obtidos de acordo com sólidos padrões de conduta. As empresas brasileiras que desejarem ter ações na Bolsa de Nova York têm até dezembro de 2005 para se adequar às novas exigências da legislação. O tamanho do desafio a ser enfrentado pode ser medido pelo grau de dificuldade registrado pelas corporações norte-americanas ao longo de 2004, ano em que se adaptaram às novas regras. Em estudo divulgado pela consultoria Ernst & Young no final do ano passado, as empresas brasileiras apresentaram mais obstáculos e consumiram mais recursos do que previam. Para quase um terço dos entrevistados, o custo financeiro e o número de horas de trabalho dedicadas à adaptação foram 50% maior que o estimado inicialmente. A pesquisa revelou um aumento de 13% para 46% no porcentual de corporações que esperavam concluir o trabalho de adaptação apenas 30 dias antes do limite legal.

acesse
www.modulo.com.br
www.petrobras.com.br
www.xerox.com.br
www.banrisul.com.br
www.mcafee.com.br

Fonte: B2B Magazine, ano 5, n. 53, p. 44-50, maio 2005.