O GLOBO ON LINE

Jornal O Globo - Info etc... Entrevista

Segunda-feira, 20 de janeiro de 2003

É preciso ter uma visão integrada dos riscos.

Por Marcos Sêmola - Janeiro/2003

Marcos Sêmola lança até o fim do mês o livro “Gestão da segurança da informação — uma visão executiva” (editora Campus, 176 páginas, R$ 35). A idéia do livro é ajudar as empresas e seus CSOs (Chief Security Officers) a aplicar uma filosofia de segurança de dados em todos os níveis hierárquicos. Professor da cadeira de Segurança da Informação para alunos de MBA da Fundação Getúlio Vargas e gerente nacional de soluções e produtos da Módulo Security Solutions, Sêmola, em entrevista ao **Info etc.** , expõe a complexidade das empresas em tempos de convergência e dá dicas de segurança a usuários domésticos. **André Machado**

Em que a era da informação mudou o conceito de segurança?

MARCOS SÊMOLA: A própria heterogeneidade de tecnologias, com altos dispositivos de conectividade, fez com que as empresas se ligassem e disponibilizassem mais as informações — para parceiros, funcionários, clientes... A economia hoje está totalmente integrada por processos eletrônicos, e compartilhando cada vez mais as informações. À medida que estas passam a ser distribuídas em LANs, WANs, MANs, redes com abrangência mundial, surgem mais pontos de acesso. Que podem ser usados por pessoas autorizadas ou não-autorizadas. Pronto, criou-se um cenário propício para que pessoas não-autorizadas efetuem fraudes, sabotagens, invasões e roubo de informações.

Dentro deste cenário, quais os maiores desafios?

SÊMOLA: O principal desafio da empresa é ter uma visão integrada dos riscos. A segurança se faz em pedaços, porém todos eles integrados, como os elos de uma corrente. Se você fortalece um elo (os sistemas) e deixa outro (as pessoas, ou “peopleware”) de lado, a corrente não fica segura. Por isso, o primeiro desafio é conseguir enxergar a segurança em todos os aspectos — físicos, tecnológicos e humanos — e tratar todos eles de forma igualitária. As questões de segurança não podem mais ser atribuídas simplesmente à ação de hackers. Dependem também do comportamento dos funcionários, de documentos formais que estabeleçam uma política de segurança e criem uma cultura nas pessoas, e da segurança física nas próprias instalações, em especial depois da tragédia de 11 de setembro.

Que medidas seriam as mais recomendadas?

SÊMOLA: Vamos fazer uma analogia com a medicina. Quando você tem um sintoma — uma dor abdominal, digamos — e visita um médico, a primeira coisa que ele faz é diagnosticar. Pede exames de sangue, uma ultra-sonografia, etc. A partir dos exames é que ele pode ter noção do problema e tomar uma atitude. Assim deve ser na área da segurança: 1) a empresa deve conhecer os riscos a que está sujeita; 2) deve avaliar o real nível de segurança de que necessita, porque cada negócio tem suas características próprias (a segurança da Casa da Moeda jamais será a mesma que a de uma padaria); e, depois, adotar uma política de segurança em que os funcionários sejam co-responsáveis. É preciso ainda treinar todo mundo para evitar reações inesperadas, pois o ser humano é imprevisível. E orientá-lo não significa definir punições, mas instruí-lo a manusear, transportar, armazenar e descartar corretamente as informações. Isso se chama ciclo de vida da informação. Não adianta guardar emails com criptografia s! e você os imprime e depois joga fora sem fragmentá-los.

E do ponto de vista da tecnologia, qual é o mínimo que se precisa ter em termos de segurança?

SÊMOLA: A segurança se faz com perímetros, como na área militar. A própria arquitetura do Pentágono, nos

EUA, é toda baseada em perímetros. Ou seja, barreiras que inibam ou atrasem tentativas de acesso indevido, dando tempo para a defesa. No caso tecnológico, temos os firewalls, que não devem evoluir muito tecnicamente, mas podem ganhar em performance e manutenção; os sistemas de detecção de intrusos (IDSs), que existem muito no papel, mas poucas empresas implementam. É um instrumento que ainda não está maduro. As empresas precisam perceber que o firewall, sozinho, não é suficiente. Outra tendência é a biometria, mas não para este ano, porque seus preços ainda inviabilizam certas aplicações. Se você pensa num banco com internet banking e milhões de correntistas, adquirir um dispositivos desses para todos eles é inviável. Por outro lado, a certificação digital está estourando, por ser um instrumento que também alavanca os negócios eletrônicos e as relações eletrônicas entre empresas,! com respaldo legal.

Você diz no livro que não se deve pensar reativamente em segurança, e tentar prever problemas. Mas a rapidez da evolução tecnológica dificulta isso. Há vulnerabilidades nos sistemas wireless, a telefonia vai chegando ao 3G... Como se preparar para a convergência?

SÊMOLA: Esse cenário não é novo, pois já sofremos integrações e convergências há algum tempo. O mundo wireless é mais um passo, e um passo até perigoso, porque aí falamos de uma convergência maior e num cenário tecnológico pouco conhecido. As redes wireless são muito novas. As empresas ainda estão tentando fazê-las funcionar direito, que dirá pensar em segurança... Isso virá depois, não adianta pôr o carro na frente dos bois.

Que absurdos você já viu na área de segurança?

SÊMOLA: Por exemplo, uma pessoa confidenciou-me que estava adotando um processo de manutenção de senhas com troca mensal, para evitar invasões. Uma medida positiva, já que grande das quebras de senha ocorre por tentativa e erro (isto é, força bruta). Mas o processo dela era o seguinte: em janeiro, a senha era fulana1, em fevereiro fulana2, em março fulana3 (**risos**). De outra feita, uma empresa queixou-se de ter sido invadida após instalar um firewall. Descobrimos que ele fora de fato instalado, mas nenhum filtro fora configurado. É como comprar um filtro de água e instalá-lo sem a vela.

Do ponto de vista do usuário final, quais são suas recomendações de segurança, em especial no trabalho?

SÊMOLA: Comecemos pelo crachá. O usuário deve mantê-lo sempre em segurança, pois é o dispositivo que o identifica em várias máquinas. A senha do login, por sua vez, deve ter um critério de criação e freqüência de troca baseado no valor das informações a que você tem acesso. Ou seja, criar uma senha de estagiário não é o mesmo que criar a de um CEO. E o dono da senha deve perceber que ela é a chave que o identifica eletronicamente e protegê-la a todo custo, modificando-a sempre que possível. O ideal é escolher senhas diferentes para serviços diferentes, jamais compartilhando uma mesma senha com vários sistemas. Sim, sei que é difícil lembrar todas as senhas que precisamos ter, então a solução é botá-las dentro de um arquivo fortemente criptografado. O meu até está na internet. O email deve ser bem gerenciado, com filtros e bloqueios adequados, assuntos separados por pasta e folders específicos para seus principais interlocutores. É bom desabilitar o preview das mensagens, para não re! ceber vír us inadvertidamente, bem como a execução de JavaScript e applets Java, para o mesmo fim. E lembre-se: mesmo o email de pessoas conhecidas não significa email confiável. Fique atento. Só abra e execute emails que realmente sejam importantes e foram solicitados por você. Trate a segurança de seu desktop como se ela fosse um perímetro pessoal. E instale e configure softwares que dêem mais segurança a ele, como um firewall pessoal freeware.

Jornalista André Machado - O Globo.