Proteção de dados

Todo cuidado é pouco

Crimes por computador, manipulação fraudulenta de dados, acesso ilícito a informações, incêndios e outros desastres ameaçam os CPDs brasileiros, ainda muito desprotegidos

Rodolfo Lucena

Depois de um desastre grave no centro de processamento de dados, as atividades de toda empresa usuária declinam 90% em apenas dez dias, conforme dados disponíveis no exterior. No entanto, no Brasil, costuma-se pensar que um acidente sempre só acontece "com os outros". A constatação é da subcomissão de segurança física da Comissão Especial 21/Proteção de Dados, da Secretaria Especial de Informática (SEI). Através de questionários e visitas a CPDs de grandes e médias empresas, os integrantes da subcomissão verificaram uma série de problemas nas instalações existentes, desde a falta de sistemas adequados de proteção contra incêndios até problemas no controle de acesso e no transporte de fitas e discos para arquivos de segurança.

Além da subcomissão de segurança física, integraram também a Comissão Especial as subcomissões de segurança lógica, de segurança em banco de dados e de auditoria. Durante quatro meses, cerca de cem pessoas, representantes de mais de cinqüenta entidades — entre elas os ministérios militares, Conselho de Segurança Nacional, Abicomp, Abac, Sucesu, Assespro e CNAB —, traçaram um quadro da atual situação brasileira na área de proteção de dados, fazendo uma série de recomendações. O documento final, com os resultados do trabalho, deve ser divulgado ainda neste mês.

HIDRANTE NO CPD — O trabalho de campo realizado pela subcomissão de segurança física revelou que grande parte das empresas pesquisadas não está garantindo as melhores condições de segurança, tanto em termos ambientais quanto na prevenção contra incêndios. Numa das empresas visitadas havia até um hidrante no CPD: no caso de um incêndio, se o fogo não destruísse as instalações, o combate com água acabaria por danificar gravemente os equipamentos.

Um dos mais graves problemas observados é quanto à fiação. Sob os pisos falsos do CPD, misturam-se nas mesmas canaletas os fios elétricos e os fios para transmissão de dados. Além disso, em boa parte das instalações o material utilizado para as divisórias, piso, mesas, armários, etc., é altamente inflamável.

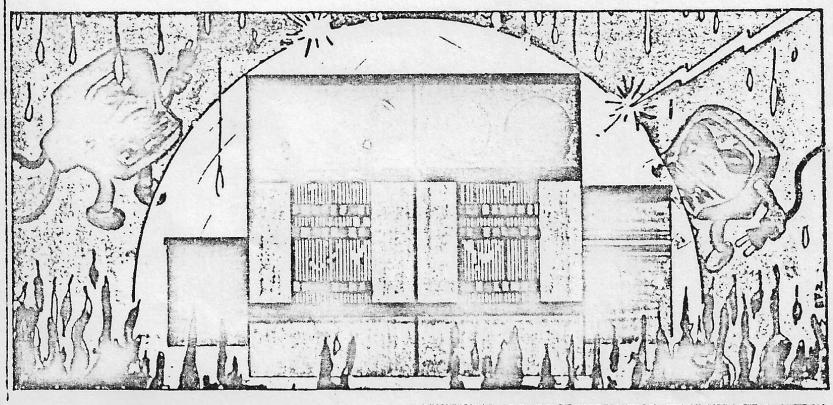
Até mesmo em termos de localização foram observados problemas pela subcomissão. Não poucas empresas simplesmente adaptam instalações inexistentes, "esquecendo" a preocupação com a segurança quando da fase de projeto — isto vem a acontecer só depois de tudo pronto.

Mesmo assim, na maioria dos casos, os CPDs têm apenas os dispositivos básicos de segurança previstos na legislação. São poucos, por exemplo, os que contam com sensores de calor e fumaça. Menor ainda é o número, entre as instituições pesquisadas, das que instalaram sistemas automáticos de extinção de fogo. Nestes casos, é mais utilizado o sistema à base de gás carbônico, em vez do mais indicado — o gás Halon 1301. E foi encontrado até um sistema de extinção à base de água, tipo "sprinkler" — "isto acaba com as máquinas", comenta um membro da Comissão Especial.

Menos caótica é a situação da proteção física dos dados. De modo geral, as empresas contam com sistemas de back up, equipamentos de no-break (principalmente quem tem sistemas on-line) e geradores, além de fitotecas. Mas, a partir daí, surgem os problemas: as instalações de fitotecas com os arquivos de segurança ficam, muitas vezes, no mesmo prédio onde está instalado o CPD, o que sempre é um risco; há descuido no transporte das fitas; e chegou a ser verificado um caso onde o combustível para os geradores era armazenado perigosamente próximo ao CPD.

Se em relação às máquinas e equipamentos a situação é esta, a proteção do pessoal também não é das mais elogiáveis. Segundo o observado nas empresas pesquisadas, a maioria que tem brigadas de incêndio o faz apenas por imposição legal, sendo mínima a preocupação com treinamento. Notou-se a ausência de sinalização para indicar as saídas, no caso de necessidade de evacuação rápida. E um certo desleixo em relação às portas corta-fogo, quando existentes: houve pelo menos um caso em que eram mantidas abertas, com calços.

FALTA DE CULTURA — Tal situação, avalia o coordenador da Comissão Especial e subsecretário de Assuntos Estratégicos da SEI, Kival Weber, é decorrente da falta de uma cultura em proteção de dados, em segurança física dos CPDs. Este problema também foi verificado pelas subcomissões que avaliaram a situação da "segurança lógica", da "segurança nas comunicações" e da "auditoria de sistemas". Na verdade, segundo a constatação dos integrantes da Comissão Especial nº 21, as instituições que há mais tempo se vêm preocupando com estes aspectos são os diversos órgãos das Forças Armadas e do governo federal, como o Itamaraty. Não por acaso, a única empresa nacional que até agora produz equipamentos para criptografia é a Prólogo, de Brasília, subsidiária da Imbel, criada em 1980 para de-



São Paulo

senvolver tecnologia na área de sigilo e produzir equipamentos militares (ver quadro).

A falta de uma cultura sobre a necessidade de segurança lógica — "o conjunto de métodos computadorizados e manuais destinados a proteger os recursos computacionais contra recursos indevidos" — faz com que, no Brasil, sejam raros os casos de empresas que tenham um órgão formalmente encarregado do assunto. Dentro da própria subcomissão, apenas uma tinha esta instância e, mesmo assim, colocada num nível hierárquico não adequado — no exterior, este problema é considerado uma preocupação dos níveis mais altos da empresa. Afinal, a maior parte dos "crimes por computador" é executada exatamente por pessoal da própria empresa, conforme estatísticas norte-americanas (ver tabela).

Assim, é recomendada uma série de medidas a nível da segurança do sistema operacional, do banco de dados e de aplicativos, além das preocupações com o acesso a informações, poder para tirar, inserir ou modificar dados. No primeiro aspecto, existem basicamente dois caminhos: os sistemas operacionais que contam, em seu núcleo, com uma camada de segurança ("security kernel"), que intermedeia o acesso a todos os elementos do SO que contêm informações (SCOM, KVM 370, Gnosis, entre outros); e a extensão ou complementação do sistema operacional através de controles de acesso.

Nos bancos de dados, o controle deve ser exercido a nível dos dados e não de arquivos (por exemplo: determinado usuário pode consultar a ficha cadastral dos funcionários, mas não conseguirá saber seu salário).

Nas aplicações, além de mecanismos para detectar ocorrências de violações, o essencial é evitá-las, e, para isso, a técnica essencial é a validação léxica (se o dado satisfaz uma ou mais condições), sintática (se um conjunto de dados satisfaz um conjunto de relações) e semântica (se os dados correspondem à realidade). Há, também, que reduzir ao mínimo as tentativas de violação, através dos mecanismos anteriores, do treinamento adequado de pessoal e da manutenção periódica dos sistemas.

CRIPTOGRAFIA E LEGISLAÇÃO — Cresce a preocupação com a segurança dos dados, principalmente por parte de instituições financeiras, das Forças Armadas e de outros órgãos do governo, como o Itamaraty, quando se entra na área de comunicações, de sistemas on-line, etc. (em outros setores, a preocupação maior é com a segurança dos sistemas batch, considerados mais vulneráveis a fraudes).

Aí as instituições dão maior ênfase à segurança dos dados do que à física (cabos telefônicos, enlaces de rádio, etc.). Como no Brasil não há uma norma geral para a interligação de sistemas distribuídos com segurança, proliferam as normas particulares. Com os sistemas nacionais disponíveis, fazem a cifração e a decifração de suas mensagens.

Ao lado da garantia do sigilo em suas comunicações, as instituições financeiras preocupam-se também com a defasagem da legislação atual em relação às novas tecnologias. As senhas ou PIN (personal identification number) dos portadores de cartões magnéticos, verdadeiras assinaturas eletrônicas, não têm valor legal. Um usuário poderia, por exemplo, negar ter realizado determinada transação e nem mesmo o recibo, se não contar com sua assinatura, valerá como prova. Por isso mesmo, uma das recomendações da Comissão Especial é a criação de um grupo da Secretaria Especial de Informática e do Ministério da Justiça que estude a revisão da legislação vigente, propondo as modificações necessárias em função dos avanços tecnológicos.

Finalmente, e não menos importante, a Comissão Especial enfatizou o papel da auditoria de sistemas para maior garantia da segurança em todos os aspectos — da física aos dados, chegando até a participação na elaboração dos contratos quando da compra ou aluguel de hardware ou software. A presença do auditor, destacou a Comissão Especial, pode ser também mais uma contribuição para enfrentar um problema bem mais amplo do próprio mercado, a pirataria de software. A auditoria periódica vai determinar quem está utilizando o quê, a documentação dos programas utilizados e como determinado software chegou à empresa. Se para os usuários de software "pirateado" isto pode parecer uma ameaça, para as empresas é mais uma garantia de segurança, a certeza de que, sempre, poderão saber como é feito e o que está sendo feito em suas dependências. ■

Criptografia à brasileira

Criada em 1980, no ano seguinte a Prólogo, subsidiária da Imbel, começou a operar efetivamente, desenvolvendo tecnologia na área de criptografia e equipamentos militares. Mas foi só no ano passado, na Feira Nacional de Informática, em Brasília, que a empresa apresentou ao público em geral sua linha de equipamentos para sigilo.

Um dos produtos lançados, então, foi o Vox 832 T, para sigilo nas comunicações telefônicas, que "mistura" o som na transmissão, impedindo que um eventual "escuta" consiga entender a conversa.

Outro produto apresentado na feira foi o Sixtex, um microcomputador de 16 bits, para automação de escritório, que opera uma série de pacotes com cifração, sendo, segundo a Prólogo, o único equipamento do gênero no Brasil.

Outros equipamentos para a área criptográfica são o CP 1, cifrador portátil de dados; o CD 1, que garante o sigilo na comunicação de dados, podendo ser aplicado em qualquer linha de até 9.600 bps; o Programa AS-2 T, para sigilo em comunicação por telex; e o CF 1, um editor de texto com cifração.

Equipamentos para criptografia da Prólogo