Rede do Senado é um queijo suíço

Fraude na lista da votação secreta para a cassação de Luiz Estêvão abre debate sobre segurança nos sistemas de votação

MARCELO NÓBREGA

O que fazer com a segurança de uma rede de computadores, quando seus operadores autorizados se unem para violá-la? Esta é a pergunta que os especialistas na área se fazem, depois da notícia de que dois funcionários do Prodasen, o centro de processamento de dados do Senado, e um empregado da Kopp, empresa que criou o placar de votação e o sistema que o gerencia, entraram no programa e modificaram a proteção da lista da votação secreta para a cassação do senador Luiz Estêvão, em junho do ano passado, para exibir nomes e votos dos senadores.

Em março, três peritos da Unicamp apresentaram um laudo com 18 itens, mostrando que a segurança da rede que controla as votações do Senado é completamente falha. O relatório foi considerado "tecnologicamente muito bem feito" por Fernando Nery, presidente da Módulo, empresa que gerencia a segurança da urna eletrônica nas eleições e do Imposto de Renda. Com base nas descobertas, três *experts* analisaram para o **JB** a fraqueza do sistema e ainda mostraram que é possível recuperar a lista de um disquete ou HD, mesmo que tenha sido apagada.

"O certo, num sistema desse porte, seria haver três ou mais níveis de autorização, e o uso de biometria" (a tecnologia de autenticação do indivíduo), opina Andre Diamand, diretor da Future Technologies, que presta serviço para o Exército, Justiça Federal e o banco HSBC. Um erro primário: na rede do Senado, todos os usuários conheciam a senha do *root*, ou administrador, e podiam se registrar como se fossem ele. A senha de cada senador não é escolhida pelo próprio: é possível portanto alterar seu voto enquanto a sessão de votação estiver aberta.

A ausência de criptografia nos dados armazenados, temporários ou permanentes, também causa calafrios nos especialistas. "É impossível imaginar um sistema desse porte sem criptografia", afirma Marcelo Bezerra, diretor técnico da multinacional de segurança ISS.

Diamand considera que a rede do Senado ignora os quatro princípios básicos de uma política de segurança.

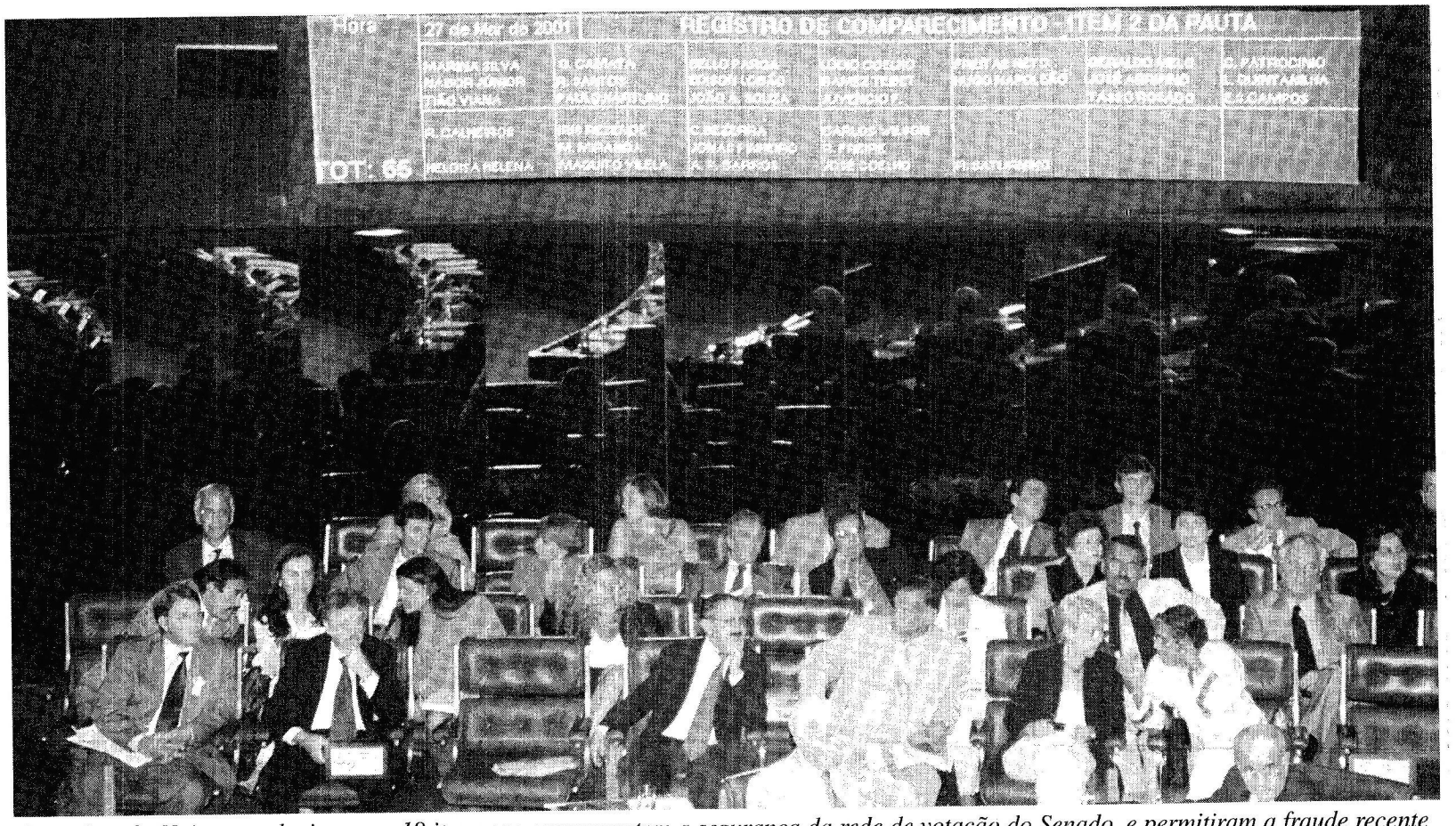
- Proteção de infra-estrutura: "Um invasor poderia instalar um *sniffer* (grampo eletrônico) e 'escutar' o tráfego de informações em qualquer lugar da rede".
- Autenticação forte: "Um sistema de *username/senha* não é seguro numa rede dessas".
- Confidencialidade das informações em tráfego e armazenadas: "Os nomes usados pelos arquivos são óbvios."
- Integridade das informações: "A rede está aberta para ações maléficas de usuários cadastrados e invasões *hackers* externas".

Além disso, o código-fonte e o programa estavam no mesmo micro, segundo a Unicamp. Um programador poderia recompilar (reprogramar) o software numa nova versão, sem ser percebido, alterando-o para exercer novas funções. O ideal, num caso desses, seria ter o código em outro micro, protegido.

O analista de sistemas Sergio Rosa, presidente do Proderj de janeiro de 1999 a março de 2000, defende o uso do software livre em sistemas governamentais. "O código-aberto permite uma fiscalização mais transparente", afirma. Segundo ele, se o programa fosse de uma empresa privada, como seria possível monitorar integralmente suas atualizações?

A Kopp Tecnologia se considerou isentada de responsabilidade pelo relatório da Unicamp. Seu principal argumento: a fraude partiu de usuários cadastrados. "O sistema foi entregue de acordo com as especificações do edital", diz seu presidente, Eliseu Kopp.

Marcia Gouthier



Os peritos da Unicamp relacionaram 18 itens que comprometem a segurança da rede de votação do Senado, e permitiram a fraude recente