OS 18 PONTOS VULNERÁVEIS APONTADOS PELOS PERITOS

357

1. A rede pode ser acessada a partir dos cabos que chegam aos painéis eletrônicos situados nas galerias

2. Portas de comunicação abertas no equipamento de rede do sistema, localizado na sala de controle, permitiriam que qualquer computador pudesse ser conectado à rede

3. Cabos de rede não utilizados na sala de controle do sistema estendem-se até as mesas dos senadores e aos dois painéis eletrônicos no plenário, o que facilitaria o acesso ao sistema

4. Unidades de disquete e disco ZIP nos computadores do sistema não estão bloqueadas

5. Dois computadores estranhos ao sistema e que estão conectados a uma rede externa possibilitariam conectar as duas redes

6. A comunicação de dados do sistema é feita sem uso de criptografia

7. A armazenagem de dados no sistema também é feita sem uso de criptografia

8. Um arquivo de rascunho temporário de votação secreta ou nominal é gerado no disco do computador principal. Esse arquivo temporário contém a vinculação do votante com o voto e poderia ser copiado e editado enquanto a votação não fosse encerrada

9. Os nomes dos arquivos usados pelo sistema são muito óbvios, facilitando a descoberta da natureza de seus conteúdos

10. Inexistência de um procedimento formal para controle da instalação de novas versões dos programas

11. Os códigos-fonte dos programas de votação estão armazenados nos mesmos discos rígidos em que se encontram os programas de votação. Isso facilitaria a geração de novos programas executáveis ou o uso indevido dos códigos-fonte

12. O ambiente de desenvolvimento de programas está instalado nos computadores do sistema, o que daria acesso a ferramentas que facilitam a leitura dos dados e a geração de versões

13. Todos os operadores utilizam uma única senha para ingresso no sistema operacional

14. A senha escolhida para o "administrador" do sistema operacional é de fácil dedução e de conhecimento de todos os operadores

15. Os arquivos relativos ao sistema são compartilhados entre todos os computadores conectados à rede. Isso permitiria a visualização até mesmo por um computador intruso

16. O senador não escolhe sua própria senha

17. O acesso às senhas dos senadores pode ser feito por listas impressas ou cadastro armazenado em disco rígido, o que permite que sejam conhecidas por outras pessoas

18. Com o conhecimento da senha de um senador é possível a alteração de seu voto durante o tempo em que a sessão de votação estiver aberta