Sinal de alerta já aponta perigo

Uma das equipes que participa dos testes junto ao TSE conseguiu achar uma brecha no sistema

O ministro Gilmar Mendes, presidente do Tribunal Superior Eleitoral (TSE), afirmou que as falhas encontradas surgiram após atualização do sistema voltado para o pleito deste ano. O grupo mais bem-sucedido nos testes, que ainda estão em andamento, foi o do professor Diego Aranha, da Universidade de Campinas (Unicamp), que encontrou falhas em alguns pontos do software utilizado nas urnas eletrônicas logo no primeiro dia de testes. Entre os achados, está a possibilidade de alteração nos logs, que são os registros de voto. Essa mudança foi realizada em um equipamento, onde uma das bibliotecas (subprogramas) estava sem assinatura eletrônica.

Por conta dessa falha, a equipe de Diego conseguiu introduzir novos comandos na urna e fazer com que ela aceitasse um teclado acoplado externamente por meio de uma porta USB. Essa entrada existe em todas as urnas e tem algumas funções específicas, como permitir a conexão com uma impressora, a fim de que um comprovante físico de voto seja emitido. Por meio dessa técnica, a equipe conseguiu saber a sequência dos votos. Mas não foi possível alterar os resultados.

A equipe liderada pelo professor da Unicamp também conseguiu realizar alteração no texto que aparece na tela do equipamento, durante a votação. Para conseguir isso, o grupo do docente realizou alterações no código binário, que é uma linguagem usada por computadores. Desta forma, foi possível mudar o texto de "seu voto para..." e substituir por "vote em 99". O sucesso no ataque revela que o software não é tão íntegro como se imaginava e pode sofrer alterações importantes.

O secretário de Tecnologia da Informação do TSE, Giuseppe Janino, afirma que o processo eleitoral é seguro. "Nós temos um processo automatizado desde 1996. A tecnologia reduziu a intervenção do homem no processo, trouxe celeridade, precisão, integridade, auditabilidade e segurança", destacou.

TSE continua afirmando que o processo eleitoral brasileiro é seguro

Pode parecer cena de filme de ficção, mas ataques contra grandes redes de infraestrutura são uma ameaça real em território nacional. Eles podem ocorrer contra sistemas elétricos, de telecomunicação e de serviços de dados de órgãos públicos. Um exemplo da iminência desse risco é o ataque mundial do vírus WannaCry, que comprometeu o funcionamento do sistema de saúde do Reino Unido.

A urna eletrônica tem uma bateria com autonomia de até 12 horas, sem precisar ser conectada à energia elétrica em nenhum momento neste período. No entanto, o mesmo não ocorre com os servidores do governo federal, inclusive os que armazenam e recebem os dados gerais. Geralmente esses computadores, localizados em Brasília, têm autonomia de até quatro horas após o desligamento da eletricidade.

JOSÉ CRUZ/AGÊNCIA BRASIL

Gilmar Mendes, no início de dezembro, durante coletiva para divulgação do resultado parcial dos testes

O ataque de ransomware, em que o invasor sequestra e criptografa os dados, está se popularizando em diversos países, inclusive no Brasil. Prefeituras de pequenas cidades já sofrem com o problema. O especialista Gerlan Ferreira, analista de segurança da informação, destaca que, apesar de serem alvo constante de ataques, empresas e órgãos públicos brasileiros ainda não atentaram para a necessidade de investir em segurança na área de tecnologia. "O governo tem começado a investir mais nessa área de segurança. No entanto, ainda falta muito esforço em relação a isso. Esses ataques de ransomware demonstram o risco que corremos. Eu não sei que nível de proteção é utilizado pelo governo. Mas qualquer sistema possui vulnerabilidade".

O perito da Polícia Federal Ivo de Carvalho Peixinho usou uma técnica bastante sofisticada para alcançar seus objetivos. Por meio da engenharia reversa, que é uma forma de mapear o funcionamento de um sistema em operação, ele obteve a chave criptográfica usada para proteger as mídias de dados. Para isso, Ivo conseguiu rodar o programa da urna em um computador. Os códigos criptográficos estavam dentro do sistema das máquinas. Essa ação revelou que se cair em mãos erradas, o software pode ser minuciosamente analisado e "entregar" fragilidades no sistema de captação e registro dos votos.

Após receber os resultados, o TSE, responsável por garantir a realização das eleições em todas as unidades da federação, adota um plano de resposta. As fragilidades encontradas são corrigidas e, de acordo com a corte eleitoral, podem ser testadas novamente, se necessário. Novos testes devem ocorrer no começo de 2018, a fim de sanar qualquer problema que esteja persistindo. De acordo com o TSE, os procedimentos de engenharia reversa serão bloqueados pela equipe de tecnologia do órgão que trabalha na segurança da urna. **(Do Correio Braziliense)**