ELEIÇÕES

Depois de hackers manipularem a eleição dos Estados Unidos, surgiram dúvidas sobre a inviolabilidade do processo de votação por meio de sistema eletrônico usado no Brasil

Risco à segurança da urna

RENATO SOUZA

MARCELO CAMARGO/AGÊNCIA BRASIL

Urnas em preparação no TRE-DF: a convite da Justiça Eleitoral, especialistas em tecnologia testaram em 2017 a segurança das máquinas e encontraram três vulnerabilidades

Brasília – O Brasil nunca esteve tão conectado como agora e o número de pessoas com acesso internet avança a cada ano. Todo esse crescimento amplia a demanda por informação, interação e capacidade de mobilização social. No entanto, ao mesmo tempo que isto permite aos brasileiros conhecer um novo mundo baseado nas interações virtuais, também cria grandes ameaças à democracia. Em ano de eleições, esses desafios precisam ser levados bem mais a sério. Ataques cibernéticos, notícias falsas e uso de robôs para manipular a opinião pública são grandes entraves que ameaçam processos democráticos ao redor do mundo. O alerta, que chegou tarde em muitas nações, chamou atenção a nível global após o FBI apontar que a ação de hackers manipulou as eleições dos Estados Unidos no ano passado.

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), 63,8% dos domicílios brasileiros têm acesso à internet banda larga por meio de computadores convencionais. Quando se fala em conexões por celular, a porcentagem de lares com acesso à rede chega a 94,8%. Desde a última eleição geral, em 2014, a quantidade de residências conectadas deu um salto. Naquele ano, 50% das casas tinham serviços de internet, o que representava 97 milhões de pessoas. Agora, esse número pode passar de 130 milhões, bem próximo dos 144 milhões de eleitores registrados pelo Tribunal Superior Eleitoral (TSE).

O Brasil é um dos poucos países que tem um complexo sistema de votação eleitoral por meio da urna eletrônica. Além de garantir o voto secreto e universal, chegando aos locais mais remotos do país, o equipamento é de fácil utilização e pode receber uma quantidade incontável de votos. Mas essa mesma tecnologia é alvo de dúvidas quanto à segurança no armazenamento das informações, segundo especialistas.

O temor é de que uma falha na urna eletrônica possibilite que pessoas má intencionadas mudem o resultado das eleições a nível regional ou até que alterem o destino de um país inteiro com um ataque generalizado ao sistema de votação. Para garantir que isso não ocorra, o TSE faz uma série de testes públicos com as urnas, antes de cada pleito. A convite da Justiça Eleitoral, especialistas de vários estados montam equipes e elaboram ataques contra a urna.

Para definir as estratégias e encontrar vulnerabilidades no sistema, os hackers têm acesso privilegiado aos softwares (programas) e hardwares (componentes físicos) que compõem o aparelho de votações. De acordo com o TSE, neste ano, 14 especialistas integraram os grupos de ataque. O resultado foi preocupante, pois as equipes encontraram três vulnerabilidades, que de acordo com o tribunal, não estavam presentes nos pleitos anteriores.

ICEX/DIVULGAÇÃO

Equipe do professor Diego Aranha, da Unicamp, encontrou falhas no software usado nos equipamentos

ATUALIZAÇÃO O ministro Gilmar Mendes, presidente do 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 causa 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.

CÓDIGO 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. 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, além da retirada das chaves de dentro do código.