INVIOLABILIDADE

Ameaças à segurança das urnas eletrônicas

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 a 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 do mundo que possui 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.

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.

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.