ELEIÇÕES

Depois de hackers manipularem a eleição americana, surgiram dúvidas sobre a inviolabilidade do processo de votação eletrônica

Ameaças à segurança das urnas

» RENATO SOUZA

O Brasil nunca esteve tão conectado como agora, e o número de pessoas com acesso à 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 a muitas nações, chamou a atenção em nível global após o FBI apontar que a ação de hackers manipulou as eleições dos Estados Unidos em 2016.

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 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 mal-intencionadas mudem o resultado das eleições em 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 votação. De acordo com o TSE, em 2017, 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 em que uma das bibliotecas (subprogramas) estava sem assinatura eletrônica.

Teclado

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. Dessa 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.

Engenharia reversa para proteger os dados

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.

TSE promete novos testes neste ano

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.

Ausência de investimentos

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 4 horas após o desligamento da eletricidade.

O ataque de ransoware, 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 ser 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 ransonware demonstram o risco que corremos. Eu não sei que nível de proteção é utilizado pelo governo. Mas qualquer sistema possui vulnerabilidade", destaca. (RS)