O ESTADO DE S.PAULO
Publicado em 03/08/2022 - 06:00

TSE monta ação contra hackers após relatório alertar para ataques

TSE monta estratégia anti-hacker após alerta de ataques nas eleições

Relatório interno da Corte Eleitoral aponta risco de crime cibernético sofisticado às vésperas da votação de outubro; medidas para proteger sistema vêm sendo implementadas

VINÍCIUS VALFRÉ
BRASÍLIA

Alertado por grupo técnico que se dedica à segurança da informação, o Tribunal Superior Eleitoral (TSE) trabalha com a possibilidade de sofrer ataques hackers às vésperas das eleições de outubro. Diante do cenário global de "recrudescimento das ameaças", a Corte Eleitoral vem implementando medidas para proteger o sistema eleitoral em Brasília e também nos tribunais regionais.

Segundo relatório interno ao qual o **Estadão** teve acesso, o TSE não descarta ser alvo de um ataque como o que paralisou o Superior Tribunal de Justiça (STJ) por uma semana em novembro de 2020. A Corte foi alvo de "ransomware", um sofisticado crime cibernético que sequestra dados e só os devolve mediante pagamento de resgate. Servidores e ministros ficaram impossibilitados de acessar arquivos e e-mails. O andamento de milhares de processos ficou prejudicado.

"Pensemos num ataque de ransomware, às vésperas do pleito de 2022, em que todos os computadores da Justiça Eleitoral amanheçam criptografados, apresentando uma mensagem em sua tela de pedido de resgate para a liberação de seus conteúdos. São situações extremas, mas perfeitamente possíveis de ocorrer, caso os adequados controles não sejam implementados, não apenas no TSE, mas em todos os tribunais regionais", avisa o relatório interno de 2021.

Os técnicos alertaram ainda para a necessidade de debelar riscos de vazamento em massa do cadastro eleitoral, de manipulação do sistema de óbitos e direitos políticos para incluir candidatos inaptos e de acesso a dados restritos para venda ilegal no mercado paralelo.

"Ocorrências como essas colocariam em xeque todo o sistema eleitoral e até mesmo a estabilidade do regime democrático de direito, catalisando as forças contrárias aos princípios democráticos que existem em nossa sociedade", diz o documento elaborado por nove técnicos do TSE e de tribunais eleitorais nos Estados.

Diretor executivo do InternetLab, um centro independente de pesquisa da internet, Francisco Brito Cruz afirmou que o mapeamento de ameaças pelo TSE é positivo e que incidentes de cibersegurança não devem ser tratados com politização. "Seria um escândalo se o TSE não tivesse um planejamento, não investisse nessa área. Olhando a estrutura da administração pública brasileira, o tribunal é um dos que mais travam discussões sobre cibersegurança", disse. "O TSE caminha sob o fio da navalha. Sabemos que essas tentativas de enviesar a questão tem um efeito como propaganda política."

META. Uma das metas do TSE é preservar a credibilidade do sistema, considerado um dos mais seguros do mundo. Mesmo com ataques malsucedidos ou menos complexos, toda a segurança do pleito pode ser comprometida a partir da atuação coordenada de atores políticos. O presidente Jair Bolsonaro (PL) tem atuado para minar a credibilidade das urnas eletrônicas, mesmo tendo sido eleito por meio delas em 2018.

Na disputa eleitoral de 2020, os ataques cibernéticos detectados não afetaram os sistemas de apuração de votos, mas o fato ajudou a alimentar teorias conspiratórias. A ação, segundo apuração da equipe técnica do tribunal, usou dispositivos do Brasil, dos Estados Unidos e da Nova Zelândia. Apenas dados antigos foram expostos. Mesmo assim, bolsonaristas aproveitaram para lançar dúvidas sobre urnas eletrônicas e defender o voto impresso.

RISCOS MUNDIAIS. Com a popularização do 5G e das transações financeiras eletrônicas, crimes virtuais viraram um problema global. Empresas como Embraer e Apple também já sofreram prejuízos. O cenário mundial fez crescer a preocupação cibernética em todo o Judiciário. Na Justiça Eleitoral, ameaças efetivas e concretas não foram detectadas até o momento, segundo o **Estadão** apurou.

O relatório menciona a "necessidade de readequação" para contar com uma "estrutura mínima para ações preventivas e reativas compatíveis com os riscos" nas eleições de 2022. O documento recomenda a definição, para cada tribunal regional, de número de técnicos atuando diretamente na segurança da informação, revisão de processos de trabalho e realocação de servidores. Também foi recomendado que os gestores de segurança da informação se reportem diretamente à presidência ou direção dos TREs.

Procurado, o TSE afirmou que um programa nacional de cibersegurança vem sendo implementado em toda a Justiça Eleitoral, mas não quis dar detalhes por motivo de segurança. ●

Para lembrar

Apurações e tentativas de invasões ao sistema

● **Pedido de auditoria**

ANTONIO AUGUSTO/ASCOM/TSE - 21/10/2020

Depois da eleição de 2014, o Tribunal Superior Eleitoral aceitou um pedido do PSDB para auditar as urnas eletrônicas. A Corte concedeu acesso a dados, arquivos e alguns programas usados nos equipamentos para uma auditoria externa. Relatório da investigação concluiu que não foi possível identificar qualquer tipo de fraude na votação.

● **Denúncia de invasão**

Um inquérito foi aberto pela Polícia Federal dez dias após o segundo turno das eleições de 2018 para apurar uma denúncia de invasão ao sistema interno do TSE. A investigação foi solicitada pelo próprio tribunal. De acordo com a Corte, o episódio não representou risco à integridade das eleições, uma vez que o código-fonte dos programas utilizados passaram por "sucessivas verificações e testes, aptos a identificar qualquer alteração ou manipulação".

● **Vazamento de dados**

NELSON JR./STF - 7/6/2022

Em 2020, ataque hacker ao sistema do TSE acessou dados de servidores do tribunal e houve vazamento de informações no dia 15 de novembro, 1.º turno do pleito. Apesar do atraso na totalização dos votos, o então presidente da Corte, Luís Roberto Barroso, disse que a invasão não afetou o resultado das urnas.

Veículo: Impresso -> Jornal -> Jornal O Estado de S. Paulo

Seção: Política **Caderno:** A **Pagina:** 8