VERKIEZINGSFRAUDE

Westen wankelt ook in digitale domein

Axel Arnbak

Verkiezingsfraude is van alle tijden, maar het manipuleren van het electorale proces is na verregaande digitalisering eenvoudiger dan ooit. Vooral in Amerika. Momenteel beheerst de hack van de Russische inlichtingendienst van de Democratische partij het nieuws, waaruit zou blijken dat het partijbestuur kandidaat Hillary Clinton voortrok boven haar concurrent Bernie Sanders. Toch kan het op 8 november pas echt misgaan. Dan brengen miljoenen Amerikanen hun stem uit via verouderde en onveilige stemsystemen, ook in cruciale 'swing states' als Pennsylvania, Ohio en Georgia. Wetenschappers tonen aan dat het verstoren en zelfs veranderen van digitaal uitgebrachte stemmen kinderspel is en dus niet is voorbehouden aan geavanceerde inlichtingendiensten zoals de Russische. Talloze beveiligingsexperts waarschuwen dat de integriteit van de verkiezingen in de machtigste democratie op aarde niet gewaarborgd kan worden.

De Democraten zijn ernstig in de verlegenheid gebracht door de hack van de Russische inlichtingendienst, die eerst inbrak op gevoelige e-mailaccounts en daarna de gewraakte e-mails openbaar maakte via klokkenluiderssite Wikileaks. Zulke inmenging van buitenlandse grootmachten in nationale politieke campagnes is zorgwekkend, maar net zo oud als de weg naar Rome. William Daugherty, oud-spion en emeritus hoogleraar beschrijft in zijn boek *Executive Secrets* hoe Amerikaanse inlichtingendiensten decennialang verkiezingen manipuleerden, bijvoorbeeld in Italië (jaren '60), Polen (jaren '80) en door de jaren heen in Latijns-Amerika. Als fenomeen is de hack van de Democraten dus niets nieuws, al laat Poetin met zijn digitale leger wel zien dat hij niet terugdeinst de VS en vooral Hillary Clinton in verlegenheid te brengen. Ook in het digitale domein wankelt het Westen.

Die geopolitieke context zou de zorgen van de Amerikaanse overheid over de gapende cybersecuritygaten in veelgebruikte stemcomputers moeten versterken. In de VS is het vooral een multidisciplinaire vakgroep van Princeton University, waar ik in 2013 deel van uitmaakte, die de vele kwetsbaarheden van het digitale stemsysteem al ruwweg twintig jaar lang 'live' demonstreert. Elke verkiezing gaan zij op de foto met onbewaakte stemcomputers in stemlokalen. Binnen zeven minuten weten zij veelgebruikte stemcomputers te hacken. Nu Amerikanen zich eerst moeten registreren om te stemmen, zijn de databases met geldige stemmers ook een interessant doelwit. Het uitschakelen van zo'n database veroorzaakt een foutmelding van de stem of een overbelasting van de lokale stemcomputer.

Veilig digitaal stemmen is mogelijk, maar de vereisten voor beveiliging zijn torenhoog

Nog ernstiger is een succesvolle hack van de systemen die de stemmen per district optellen, die je zelfs de mogelijkheid kan geven een uitgebrachte stem te veranderen. Verkiezingshacks zijn extra risicovol omdat ze maar één dag operationeel hoeven te zijn en gericht uitgevoerd kunnen worden: stemmers registreren zich vaak als Democraat of Republikein en uit demografische en historische gegevens kun je ook afleiden wie wat stemt in welk district. Winst of verlies van de landelijke verkiezing kan afhangen van slechts tienduizenden stemmen in een paar swing states.

Waarom is juist Amerika zo kwetsbaar? Natuurlijk spelen gebruikelijke cybersecurityproblemen een rol. En hebben de (vaak vrijwillige) functionarissen in stemlokalen geen kennis van computerbeveiliging. Maar vooral de registratieplicht en de Help America Vote Act werken averechts. Deze federale wet creëerde in 2002 een fonds van $ 4 mrd voor staten om kostbare stemcomputersystemen te kopen. Alle vijftig staten grepen hun kans. Pennsylvania kocht bijvoorbeeld 20.597 stemsystemen voor een vermogen. Sindsdien zijn die systemen nauwelijks vernieuwd en vaak zo lek als een mandje.

Veilig digitaal stemmen is mogelijk, maar de beveiligingsvereisten zijn net zo torenhoog als de belangen van ordentelijke verkiezingen. Het 400 pagina's tellende rapport van de Commissie-Van Beek uit 2013 beschrijft de noodzakelijke vereisten, die in de praktijk peperduur en nauwelijks uitvoerbaar zullen zijn. Nederland stemt dus met potlood. Maar de VS stemmen massaal elektronisch. Op 8 november beleeft dit realistische plot voor de volgende Bondfilm een wereldpremière.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak