

# Mit einer Manipulation muss gerechnet werden

## Rainer W. Gerling über Wahlmaschinen

Am 24. September findet in Deutschland die Bundestagswahl statt: ohne Wahlmaschinen, aber nicht ohne Software. Wahlmaschinen sind in Deutschland durch ein Urteil des Bundesverfassungsgerichts vom 2. März 2008 nicht zulässig. Und das ist auch gut so, denn Wahlmaschinen hinterlassen einen faden Beigeschmack.

So hatte zuletzt die für die Wahlcomputer in Venezuela zuständige Firma Smartmatic behauptet, dass ihre Daten und die offiziellen Daten der Wahlkommission massiv voneinander abweichen würden. Grundsätzlich ist die informationstechnische Absicherung eines Wahlcomputers

eine größere Herausforderung als die Absicherung der IT eines Unternehmens oder einer Behörde. Potenzielle Angreifer auf die Wahlmaschinen sind auch Innentäter oder gar der Betreiber; gerade in weniger demokratischen Staaten eine reale Situation.

Und Wahlmaschinen helfen nur beim Auszählen der Stimmen. Bei der Stimmabgabe bringen sie keine Vorteile. Der Einwand, dass sie ungültige Stimmen verhindern können, gilt nicht, da die bewusste Abgabe einer ungültigen Stimme eine demokratisch legitime Option ist.

Beim Zusammenführen der Stimmen zum amtlichen Endergebnis wird heute auch Software (IVU.elect) eingesetzt. Und auch diese kann angegriffen werden. Dieses Risiko ist dem Bundeswahlleiter bewusst, und es wurden Maßnahmen ergriffen, um das Risiko zu minimieren. Dass diese Maßnahmen ausreichen, wird

beispielsweise vom Chaos Computer Club bezweifelt. Die Infrastruktur einer Wahl im Internet, bei der wir nicht mehr ins Wahllokal gehen müssen, sondern vom eigenen Computer wählen, kann direkt im Internet angegriffen werden. Dies wird nur von wenigen Ländern (Estland, Schweiz, USA) derzeit ernsthaft betrieben. Das Risiko ist hoch. Aber auch die Meinungsbildung vor der Wahl kann manipuliert werden. Sowohl bei der Präsidentschaftswahl in den USA als auch in Frankreich wurden im Wahlkampf vorab gestohlene Daten zum Nachteil eines Kandidaten veröffentlicht. Veröffentlicht von Wikileaks und vermutlich – so behaupten Nachrichtendienste – gestohlen von russischen Hackern (der Gruppe APT28).

Kann das bei uns auch passieren? Ja. Schon Mitte 2016 gab es Hackereinbrüche bei politischen Parteien und Politikern in Deutschland und 2015 den „Bundestag-

Hack“. Dabei wurden große Datenmengen entwendet. Auch hier war wohl die staatsnahe Hackergruppe APT28 tätig.

Mit einem Versuch, die Bundestagswahl durch die Veröffentlichung gestohlener Daten oder durch die Verbreitung von Fake News zu beeinflussen, muss gerechnet werden. Jeder Wahlberechtigte sollte das wissen und sich nicht leichtfertig beeinflussen lassen.



### Unser Gastautor

ist der IT-Sicherheitsbeauftragte der Max-Planck-Gesellschaft. Der habilitierte Physiker lehrt IT-Sicherheit an der Hochschule München.

Namentlich gekennzeichnete Kommentare geben nicht unbedingt die Meinung der Redaktion wieder.