Inhaltlicher Antrag

Antrag an die 63. Mitgliederversammlung des fzs e.V.

Initiator*innen: Franziska Chuleck (AStA der TU Darmstadt, Ausschuss Studienreform)

Titel: e-Voting ist und bleibt unsicher

Antragstext

1 Wahlen sind die allgemeinste Form der politischer Beteiligung und bilden das
2 Fundament unserer Demokratie. Ob innerhalb der Hochschulen oder außerhalb,
3 überall gelten die gleichen Grundsätze: demokratische Wahlen sind allgemein,
4 unmittelbar, frei, gleich und geheim.

5 Der fzs stellt fest, dass in den vergangenen Monaten immer mehr Hochschulen und
6 Studierendenschaften auf Online-Wahlen und e-Voting umstellen. Aufgrund der
7 Prozessabfolge sind Online-Wahlen und e-Voting derzeit nicht in der Lage die
8 Wahlgrundsätze demokratischer Wahlen zu gewährleisten. Dies ist den inhärenten
9 Prozessen geschuldet und wird auch in absehbarer Zukunft durch keinen
10 technologischen Fortschritt geändert.

11 Deswegen spricht sich der fzs gegen den Einsatz von Wahlcomputern und e-Voting-
12 Systemen aus, solange die Wahlgrundsätze nicht eingehalten werden können. Alle
13 Hochschulen und Studierendenschaften werden aufgefordert vom Einsatz solcher
14 Systeme Abstand zu nehmen. Der fzs fordert weiterhin, dass auch keine
15 Wahlcomputer und e-Voting-Systeme für die Wahlen außerhalb des Hochschulwesens
16 eingesetzt werden, um den allgemein gültigen Grundsätzen der demokratischen
17 Wahlen gerecht zu werden.

Begründung

18 Seit mehreren Jahren beschäftigen sich unterschiedliche Informatiker*innen mit
19 dem Problem des e-Votings. Die Konferenz der deutschsprachigen

20 Informatikfachschaften (kurz: KIF) hat sich bereits zweimal gegen den Einsatz
21 von Wahlcomputern und e-Voting-Systemen ausgesprochen
22 (https://wiki.kif.rocks/wiki/KIF345:Resolution_E-Voting,
23 https://wiki.kif.rocks/wiki/KIF460:Resolutionen/Elektronische_Wahlen). Auch der
24 Chaos Computer Club (kurz: CCC) rät dringend vom Einsatz solcher Systeme ab
25 (https://media.ccc.de/v/pw17-167-probleme_mit_e-voting,
26 https://media.ccc.de/v/34c3-9247-der_pc-wahl-hack ,
27 <https://netzpolitik.org/2015/31c3-e-voting-ist-und-bleibt-unsicher/>).

28 *Warum lehnen so viele Informatiker*innen e-Voting ab?*

29 Demokratische Wahlen sind allgemein, unmittelbar, frei, gleich und geheim. E-
30 Voting-Systeme genügen diesen Ansprüchen nicht. Im folgenden wird die Wahl mit
31 einem Wahlcomputer betrachtet.

32 Eine Person geht wählen, sie steht vor dem Wahlcomputer und möchte die Partei
33 A wählen. In einer Papier-basierten Wahl setzt sie in einer Wahlkabine ihr
34 Kreuz bei der Partei A, faltet das Blatt und wirft es unter Beobachtung in die
35 versiegelte Urne. Diese wird im Papier-basierten Verfahren unter Beobachtung,
36 nach Schließung der Wahllokale, wieder geöffnet und alle Stimmen gezählt. All
37 das kann beobachtet werden - bis auf das setzen des Kreuzes.

38 Ist das auch bei Wahlcomputern möglich?

39 Durch die vielen beim herkömmlichen Wahlverfahren involvierten Personen wird
40 eine Manipulation extrem erschwert. Im Gegensatz dazu kann bei einer Wahl mit
41 Wahlcomputern oder e-Voting-Systemen eine Manipulation nicht erkannt werden, da
42 die beteiligten Personen keine Kontrolle über die Geräte und Programme in
43 ihrem Aufgabenbereich haben. Die relevanten Kontrollen finden an wenigen mit
44 punktuellen Aufwand kompromittierbaren Stellen statt.

45 Die Person steht also in der Wahlkabine und möchte Partei A wählen. Wie kann
46 sie sicher sein, dass die Software auf dem Wahlcomputer genau das tut? Sie
47 könnte im Vorfeld die Software-Kontrollieren. Um nachvollziehen zu können, was
48 der Quellcode tut, sind mindestens rudimentäre Kenntnisse im Bereich der
49 Programmierung notwendig. Nur ein geringer Teil der Bevölkerung hat diese
50 Kenntnisse. Nun wird der Quellcode in für Maschinen verständlicher Code
51 überführt. Auch hier könnte eine Manipulation stattfinden. Um dies
52 auszuschließen, muss der sogenannte Compiler überprüft werden. Dafür sind
53 spezielle Kenntnisse aus dem Bereich der Informatik nötig, die nur sehr weniger
54 Informatiker*innen in der nötigen Tiefe besitzen. Aber nehmen wir an, die
55 Person hätte diese Kenntnisse und wäre auch in der Lage, das Compiat (der
56 für Maschinen verständliche Code) zu verstehen. Dieser Code läuft auf einem
57 Computer. Der nächste Schritt, an dem Manipulation stattfinden kann. Um die
58 Wahlgrundsätze einhalten zu können, müsste unsere wählende Person auch in
59 der Lage sein, die Hardware zu verstehen und zu testen, um eine Manipulation
60 auszuschließen. Die hierfür erforderlichen Kenntnisse besitzen auch wieder nur
61 sehr wenige Informatiker*innen. Jetzt gehen wir davon aus, dass unsere wählende
62 Person auch das kann.

63 In der Wahlkabine vor dem Wahlcomputer steht nun eine Person, die in der Lage
64 ist die Software in gänze mit Compilat und auch die Hardware zu verstehen. Wie
65 kann sich diese Person sicher sein, dass vor ihr der Wahlcomputer mit der
66 Hardware, die zuvor versprochen und überprüft wurde, und mit der Software, die
67 zuvor versprochen und überprüft wurde? USB-Sticks in Wahlcomputer stecken ist
68 eine ganz schlechte Idee (Traue keinem USB-Stick, der nicht dir gehört!), es
69 könnte darauf Schadsoftware geladen sein, die alles zerstört. Wie also soll
70 das überprüft werden? Defacto ist das nicht möglich. Unsere wählende Person,
71 die zwar alle nötigen Fähigkeiten hat, kann das nicht überprüfen. Sie muss
72 also darauf vertrauen, dass alles so ist wie es ihr versprochen wurde. Doch
73 damit entsprechen die Wahlen schon nicht mehr den Wahlgrundsätzen.

74 Aber wir nehmen an, dass das doch alles in Ordnung ist. Jetzt müssen die
75 Stimmen an den Server, der diese auszählt. Wie können die Stimmen zum Server
76 gebracht werden? Die erste Möglichkeit ist, die Stimmen über das Internet zu
77 übertragen. Hier müsste aber sicher gestellt werden, dass mit einer sicheren
78 Verschlüsselung die Daten gesichert werden. Unsere wählende Person müsste
79 also auch das prüfen. Kryptographie ist ein weiteres Spezialgebiet der
80 Informatik und insbesondere der Mathematik. Eine weitere Möglichkeit ist, den
81 Wahlcomputer physisch zum Server zu bringen. Hier müsste unsere wählende
82 Person sicherstellen, dass keine Manipulation passiert. Auch nicht durch einen
83 technischen Fehler. Als dritte Option ist wieder ein USB-Stick denkbar, mit
84 allen Problemen von vorher.

85 Vielleicht klappt das ja alles und die Stimmen kommen ohne Manipulation beim
86 Server an. Dieser zählt jetzt die Stimmen. Hier ergeben sich die exakt gleichen
87 Probleme wie zuvor mit dem Wahlcomputer in der Kabine - unsere wählende Person
88 muss alles überprüfen und dann darauf vertrauen, dass die Hard- und Software
89 genau so sind wie ihr das versprochen wurde.

90 Wir nehmen also an, dass wir beim wählen mit dem Wahlcomputer sicher gehen
91 können, dass wir vor der Hardware stehen, die uns versprochen wurde, mit der
92 Software, die uns versprochen wurde. Wir nehmen weitere an, dass unsere Stimme
93 auf sicherem Weg zu einem Server transportiert wird, der das tut, was uns
94 versprochen wurde.

95 Wahlen basieren allerdings auch auf dem Konzept von Misstrauen - jeder Schritt
96 in einer Papier-basierten Wahl wird penibel beobachtet und jeder Verdacht auf
97 Fälschung wird exakt untersucht. E-Voting basiert aber, wie oben beschrieben,
98 auf sehr großem Vertrauen. wir müssen darauf vertrauen, dass alles so läuft,
99 wie es uns versprochen wurde. Es ist auch für Informatiker*innen extrem schwer
100 jeden einzelnen Schritt vollständig nachvollziehen und überprüfen zu können.
101 Dafür sind einfach zu viele Spezialgebiete der Informatik betroffen:
102 Algorithmik, Compiler, Technische Informatik und Kryptographie. Jedes dieser
103 Gebiete hat noch weitere Untergebiete, die sich immer weiter spezialisieren.
104 Damit ist eine vollständige Überprüfung durch nur eine Person defacto
105 unmöglich. Und selbst, wenn es möglich wäre, müssten alle anderen Menschen
106 dieser Person trauen (https://www.youtube.com/watch?v=w3_0x6oaDmI ,
107 <https://www.youtube.com/watch?v=LkH2r-sNj0s>). Die in dem abgeschlossenen System
108 Wahlcomputer/e-Voting ablaufenden Prozesse sind für die breite Bevölkerung in
109 keiner Weise nachvollziehbar oder überprüfbar. Sie ist deshalb auf die

110 Aussagen von wenigen Menschen mit fachlicher Expertise angewiesen, denen sie
111 blind vertrauen müsste. Doch selbst diese können nicht verifizieren, dass die
112 tatsächlich eingesetzten Systeme mit den von ihnen überprüften identisch
113 sind. Die Systeme können so manipuliert worden sein, dass die Stimmabgabe
114 abgehört oder verändert wird.

115 Auch abseits von Wahlcomputern hat e-Voting sehr viele Sicherheitsprobleme.
116 Mögliche Angriffe auf per Mail versendete Wahlen sind Man-in-the-middle
117 (<https://www.youtube.com/watch?v=-enHfpHMB04>), Cross-Side-Scripting
118 (<https://www.youtube.com/watch?v=L5l9lSnNMxg>,
119 <https://www.youtube.com/watch?v=vRBihr4lJTo>), SQL-injections
120 (https://www.youtube.com/watch?v=_jKylhJtPmI) und und und ([https://logbuch-
121 netzpolitik.de/tag/e-voting](https://logbuch-netzpolitik.de/tag/e-voting)). Die Sicherheit der Wahlen kann nur dann möglich
122 werden, wenn alle Menschen ihre Mails verschlüsseln, ihre Daten verschlüsseln
123 und ihre elektronischen Geräte auf dem aktuellsten Sicherheitsstand halten
124 (https://www.youtube.com/watch?v=svEuG_ekNT0). Und selbst dann können immer
125 neue Sicherheitslücken aufgedeckt werden
126 (https://link.springer.com/content/pdf/10.1007/978-0-387-35586-3_37.pdf ,
127 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234426> ,
128 https://www.usenix.org/legacy/events/evt/tech/full_papers/Estehghari.pdf ,
129 [https://www.researchgate.net/profile/Thomas_Lauer/publication/228920801_The_Risk
130 _
131 _of_eVoting/links/004635182c0960710c000000.pdf](https://www.researchgate.net/profile/Thomas_Lauer/publication/228920801_The_Risk_-_of_eVoting/links/004635182c0960710c000000.pdf)). Daher ist für die Zukunft zu
132 erwarten, dass sich die genannten Probleme nicht lösen werden
133 ([https://netzpolitik.org/2018/schreckliche-idee-us-zwischenwahlen-auf-
134 smartphones-und-mit-blockchain/](https://netzpolitik.org/2018/schreckliche-idee-us-zwischenwahlen-auf-smartphones-und-mit-blockchain/) , [https://netzpolitik.org/2019/wahlcomputer-
135 hacks-und-pannen-so-unsicher-sind-die-us-wahlen/](https://netzpolitik.org/2019/wahlcomputer-hacks-und-pannen-so-unsicher-sind-die-us-wahlen/) ,
136 [https://netzpolitik.org/2019/was-vom-tage-uebrig-blieb-eu-webseiten-jetzt-eu-
137 kompatibler-der-oesterreichische-staatstrojaner-und-e-voting-disaster-in-
138 spanien/](https://netzpolitik.org/2019/was-vom-tage-uebrig-blieb-eu-webseiten-jetzt-eu-kompatibler-der-oesterreichische-staatstrojaner-und-e-voting-disaster-in-spanien/) , [https://netzpolitik.org/2016/e-voting-in-australien-das-mag-den-
lobbyisten-freuen-nicht-aber-den-waehler/](https://netzpolitik.org/2016/e-voting-in-australien-das-mag-den-lobbyisten-freuen-nicht-aber-den-waehler/))

139 In Anbetracht dessen ist es beunruhigend mit was für einer Regelmäßigkeit
140 Wahlcomputer und e-Voting-Systeme gefordert werden, auch in
141 Studierendenschaften. Der fzs sollte sich hier hinter die Wissenschaft stellen
142 und derartige Wahlsysteme ablehnen. Diese Ablehnung bezieht sich dabei sowohl
143 auf Wahlen an Hochschulen als auch außerhalb von Hochschulen. Die
144 demokratischen Wahlgrundsätze gelten überall, auch an Hochschulen. Sie müssen
145 daher auch überall eingehalten werden. Die KIF und der CCC haben sich
146 entsprechend positioniert. Mit diesem Antrag schließt sich der fzs dem an.