I-A1NEU

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

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

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

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

Begründung

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

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

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

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

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

Ist das auch bei Wahlcomputern möglich?

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

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

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

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

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

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

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

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

Auch abseits von Wahlcomputern hat e-Voting sehr viele Sicherheitsprobleme. Mögliche Angriffe auf per Mail versendete Wahlen sind Man-in-the-middle (https://www.youtube.com/watch?v=-enHfpHMBo4), Cross-Side-Scripting (https://www.youtube.com/watch?v=L5l9lSnNMxg, https://www.youtube.com/watch?v=vRBihr41JTo), SQL-injections (https://www.youtube.com/watch?v=_jKylhJtPmI) und und und (https://logbuch-netzpolitik.de/tag/e-voting). Die Sicherheit der Wahlen kann nur dann möglich werden, wenn alle Menschen ihre Mails verschlüsseln, ihre Daten verschlüsseln und ihre elektronischen Geräte auf dem aktuellsten Sicherheitsstand halten (https://www.youtube.com/watch?v=svEuG_ekNT0). Und selbst dann können immer neue Sicherheitslücken aufgedeckt werden (https://link.springer.com/content/pdf/10.1007/978-0-387-35586-3_37.pdf , https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234426 , https://www.usenix.org/legacy/events/evt/tech/full_papers/Estehghari.pdf , https://www.researchgate.net/profile/Thomas_Lauer/publication/228920801_The_Risk_of_eVoting/links/004635182c0960710c000000.pdf). Daher ist für die Zukunft zu erwarten, dass sich die genannten Probleme nicht lösen werden (https://netzpolitik.org/2018/schreckliche-idee-us-zwischenwahlen-auf-smartphones-und-mit-blockchain/ , https://netzpolitik.org/2019/wahlcomputer-hacks-und-pannen-so-unsicher-sind-die-us-wahlen/ , 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/)

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