Aktuelle Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen

Bernhard Beckert[*], Jurlind Budurushi[†], Armin Grunwald[‡], Robert Krimmer[§], Oksana Kulyk[¶], Ralf Küsters[‖], Andreas Mayer[**], Jörn Müller-Quade[††], Stephan Neumann[‡‡], Melanie Volkamer[§§]

10.09.2021

Version 1.0

Kontakt: online-wahl-experten-am-und-ausserhalb-des-kit@lists.kit.edu

[*] https://formal.iti.kit.edu/beckert/index.phtml
[†] https://jurlindbudurushi.com
[‡] https://www.itas.kit.edu/kollegium_grunwald_armin.php
[§] https://www.etis.ee/CV/Robert_Krimmer/est?lang=ENG
[¶] https://okskulyk.github.io/
[‖] https://sec.uni-stuttgart.de
[**] https://www.hs-heilbronn.de/andreas.mayer
[††] https://crypto.iti.kit.edu/head_of_institute.php
[‡‡] https://www.stephanneumann.it
[§§] https://secuso.aifb.kit.edu/Team_Volkamer.php

Zusammenfassung

Seit Beginn der Pandemie stehen viele Institutionen (inkl. Vereinen, Unternehmen und Behörden) vor der Frage, wie sie ihre Wahlen und geheimen Abstimmungen organisieren sollen – ohne die Gesundheit der Wähler*innen und Wahlhelfer*innen zu gefährden. Einige Wahlverantwortliche haben sich für die Durchführung von Online-Wahlen bzw. digitalen Abstimmungen entschieden. Erfahrungen anderer Wahlverantwortlicher, die bereits vor der Pandemie online gewählt haben, gab es in Deutschland kaum. Vor der Pandemie wurde das Thema Online-Wahlen in Deutschland – bedingt durch das sogenannte Wahlgeräte-Urteil des Bundesverfassungsgerichts (2009) – kaum diskutiert. Nach über einem Jahr Pandemie sieht die Lage anders aus: Inzwischen fanden einige Wahlen und Abstimmungen online statt. Allerdings entsprechen die dazu eingesetzten Systeme häufig nicht dem Stand der Forschung. Für zukünftige Nutzungen von Online-Wahlen und digitalen Abstimmungen (insbesondere auch nach der Pandemie) ist es daher wichtig, dass Wahlverantwortliche, Kandidat*innen und Wähler*innen verstehen, welches Risiko die bisher eingesetzten Systeme mit sich bringen und wie einzelne Entwicklungen im Kontext von Online-Wahlen und digitalen Abstimmungen einzuordnen sind. Nur so können informierte Entscheidungen im Hinblick auf die einzusetzenden Ansätze getroffen und die Demokratie auch in Zukunft geschützt werden.

Keywords (de) — Online-Wahl, Internet-Wahl, Verifizierbarkeit, Verifikation, Nachfolliehbarkeit, Evaluation, Zertifizierung, Transparenz, Öffentlichkeitsgrundsatz, Manipulationssicherheit, Cyberangriffe, Wahlgeheimnis, Ende-zu-Ende, E2E, individuelle Verifizierung, universelle Verifizierung

Keywords (en) — Electronic Voting, Internet Voting, Online Voting, Verifiability, Verification, Evaluation, Certification, Transparency, public nature of elections, cyber attacks, vote secrecy, vote privacy, Insider, End-to-End, public verifiable, individual verifiability

Inhaltsverzeichnis

1 Absichtserklärung

Im Hinblick auf die Sicherheit von digitalen Abstimmungen und Wahlen sind eine Vielzahl rechtlicher und technischer Anforderungen[1] zu berücksichtigen. Wesentliche Teile dieser Anforderungen beziehen sich auf das Wahlgeheimnis sowie die Öffentlichkeit, Nachvollziehbarkeit und Überprüfbarkeit der individuellen Stimmabgabe und der Auszählung der abgegebenen Stimmen.

Wir sind eine Gruppe von Expert*innen auf dem Gebiet der digitalen Abstimmungen und der Online-Wahlen, die insbesondere an Methoden zur Umsetzung der Öffentlichkeit, Nachvollziehbarkeit und Überprüfbarkeit der individuellen Stimmabgabe sowie der Auszählung aller abgegebenen Stimmen (auch als Ende-zu-Ende-Verifizierbarkeit bei gleichzeitiger Sicherung des Wahlgeheimnisses) forschen[2]. Aus der Erfahrung im Austausch mit Wahlausrichtern u. a. im Rahmen der E-Vote-ID Konferenz[3] ist uns bewusst, dass die Auswahl eines digitalen Abstimmungsverfahrens mindestens aus den folgenden Gründen nicht trivial ist:

1. Digitale Abstimmungsverfahren bzw. Online-Wahlsysteme setzen auf komplexen kryptographischen Verfahren auf. Um die Sicherheit kryptographischer Verfahren zu validieren, bedarf es entsprechender mathematischer Beweise.
2. Es gibt nicht *das* Verfahren bzw. *das* System, welches optimal für jegliche Art von Wahl ist. Die grundsätzliche Eignung der Verfahren bzw. Systeme hängt von der Einsatzumgebung ab – eine Abwägung von Vor- und Nachteilen sowie eine Risikobewertung sind notwendig.
3. Die Anbieter von Online-Wahldienstleistungen stellen häufig die Vorteile ihrer Verfahren bzw. Systeme in den Vordergrund, ohne dabei die entsprechenden Nachteile der jeweiligen Einsatzumgebung zu benennen – somit werden Verfahren und Systeme oftmals als *sicher* angepriesen.
4. Wahlausrichter haben in der Regel ein nachvollziehbares Interesse daran, ihre Online-Wahl als Erfolg zu interpretieren. Somit wird von der Komplexität und den Herausforderungen bei der Implementierung eines Verfahrens bzw. Systems sowie den Rest-Risiken wenig berichtet, sodass leicht der Eindruck entsteht, dass man 'einfach' das gleiche Verfahren bzw. System für andere Wahlen verwenden kann.
5. Es existieren eine Reihe von Anforderungskatalogen, die unterschiedliche Anforderungen formulieren und oft nicht auf die Annahmen (bzw. das Angreifermodell) eingehen. Dadurch ist es schwer, im Rahmen einer Risikobewertung über Rest-Risiken zu sprechen.

Daher ist es uns ein Anliegen, Wahlausrichter dabei zu unterstützen, eine informierte Entscheidung bzgl. der Verfahrens- bzw. Systemauswahl zu treffen. Unser Anliegen ist es, mit diesem Dokument darauf aufmerksam zu machen, welche Aspekte allgemein für die Risikobewertung wichtig sind (Kapitel 2) sowie auf potenzielle Bedrohungen und Missverständnisse in Bezug auf bereits durchgeführte Online-Wahlen hinzuweisen (Kapitel 3 bis Kapitel 6), damit Risiken besser abgeschätzt werden können und eine

[1] Siehe z.B. die Anforderungen auf europäischer Ebene: `https://rm.coe.int/0900001680726f6f` (Stand: 23.08.2021)

[2] Dabei sind ein Großteil der Expert*innen im Land Baden-Württemberg und insbesondere am Karlsruher Institut für Technologie (KIT) tätig - siehe auch `https://evoting.kastel.secuso.org/` (Stand: 23.08.2021).

[3] `https://www.e-vote-id.org/` (Stand: 23.08.2021)

informierte Entscheidung getroffen werden kann. Darüber hinaus möchten wir Hintergrundinformationen zu verschiedenen Dokumenten – insbesondere im Kontext von Anforderungsdokumenten (Kapitel 7 und Kapitel 8) – zur Verfügung stellen.

Allgemeine Hinweise: Im Dokument adressieren wir unterschiedliche Kontexte und Themen. Jeder Abschnitt soll für sich verständlich sein. Dies hat zur Folge, dass teilweise Redundanzen im Gesamt-Dokument zu finden sind.

2 Hintergrundinformationen

2.1 Security-Prinzipien

Für eine informierte Entscheidung in Bezug auf die IT- bzw. Informationssicherheit von IT-Produkten sind insbesondere die Aspekte Angreifermodell, Annahmen zum Benutzer*innenverhalten und Vertrauenswürdigkeit der Aussagen zu diesem Angreifermodell und der Annahmen wichtig. Dies gilt entsprechend auch für virtuelle Abstimmungen und Online-Wahlen. Daher werden diese im Folgenden mit Bezug auf geheime Abstimmungen und Wahlen kurz erläutert:

1. Das *Angreifermodell* (vereinfacht gesagt, die Annahmen an die Grenzen der Angreifermächtigkeit) definiert, *wer das Wahlgeheimnis wie verletzen* kann und *wer die Stimmen bzw. das Ergebnis wie unbemerkt verändern* kann. Mit 'wer' sind beispielsweise Wahlausrichter selbst, Cyber-Angreifer, Server-Administratoren oder Online-Wahldienstleister gemeint. Mit 'wie' ist neben der Vorgehensweise auch gemeint, wie aufwendig der Angriff wäre. Sowohl mit Blick auf das unbemerkte Verändern von Stimmen als auch mit Blick auf das Wahlgeheimnis ist es empfehlenswert sich die Annahmen bezogen auf einzelne Stimmen versus viele / alle Stimmen anzusehen[4].
2. Die *Annahmen an das Benutzer*innenverhalten* definieren, welches Verhalten notwendig ist, um die Sicherheitseigenschaften (also insbesondere der Schutz des Wahlgeheimnisses und die Erkennung von Manipulationen an Stimmen bzw. Ergebnisse) zu gewährleisten. Benutzer*innen sind dabei neben den Wähler*innen insbesondere auch die Wahlausrichter, Mitarbeiter*innen von Online-Wahldienstleistern, Server-Betreiber bzw. weitere Personen im digitalen Wahlprozess. Hierzu würde z. B. die Verwendung von sicheren Passwörtern sowie die sichere Aufbewahrung von Passwörtern durch Benutzer*innen zählen.
3. Die *Vertrauenswürdigkeit der Aussagen* zu diesem Angreifermodell und der Annahmen kann unterschiedlich tiefgehend überprüft werden, z. B. kommen die Aussagen vom Online-Wahldienstleister oder gibt es eine Evaluation durch unabhängige Experten, die das Angreifermodell und die Annahmen bestätigt? Im Fall einer Evaluation ist die Frage wie tiefgehend diese durchgeführt wurde (z. B. welche Dokumente / Beschreibungen wurden untersucht bzw. wurde der Source Code analysisert).

All diese Informationen sind wichtig, um das Risiko abzuschätzen, das mit der Durchführung der Online-Wahl einhergeht. Wenn das Risiko abgeschätzt ist, stellt sich die Frage, ob das ermittelte Risiko für eine konkrete Wahl vertretbar ist.

[4] In der Regel skalieren Angriffe auf Online-Wahlsysteme besser als Angriffe auf die traditionellen Wahlsysteme.

2.2 Ende-zu-Ende-Verifizierbarkeit

Ende-zu-Ende-Verifizierbarkeit bedeutet, dass Wähler*innen überprüfen können, dass ihre Stimme so wie beabsichtigt abgeschickt wird (auch als cast-as-intended bezeichnet), dass ihre Stimme in der elektronischen Urne, die ausgezählt wird, so wie abgeschickt gespeichert ist (auch als stored-as-cast bezeichnet) und dass alle in der elektronischen Urne gespeicherten Stimmen (und damit inkl. der eigenen Stimme) korrekt ausgezählt werden. Darüber hinaus sollte es möglich sein zu prüfen, dass nur Stimmen von Wahlberechtigten in der elektronischen Urne enthalten sind. Je nach Literatur spricht man hierbei von der sogenannten Eligibility-Verifizierbarkeit.

Ende-zu-Ende-Verifizierbarkeit ist damit der einzige Weg, bei geheimen Wahlen und Abstimmungen verlässliche Aussagen hinsichtlich (nicht)stattgefundener Manipulationen zu treffen[5]. Ohne Ende-zu-Ende-Verifizierbarkeit ist es nicht möglich nachzuweisen, dass der Betreiber der Online-Wahl oder Cyber-Angreifer das Wahlergebnis unbemerkt verändert haben.

Durch die geschickte Kombination verschiedener kryptographischer Methoden ist es möglich, Öffentlichkeit, Nachvollziehbarkeit und Überprüfbarkeit der individuellen Stimmabgabe sowie der Auszählung aller abgegebenen Stimmen (also Ende-zu-Ende-Verifizierbarkeit) bei gleichzeitiger Sicherung des Wahlgeheimnisses umzusetzen.

Darüber hinaus ermöglicht der Einsatz von Ende-zu-Ende-verifizierbaren Systemen einen gewissen Grad des Öffentlichkeitsgrundsatzes[6] zu erreichen.

Zuletzt sei darauf verwiesen, dass Ende-zu-Ende-Verifizierbarkeit Vorteile im Vergleich zur Veröffentlichung des Quellcodes bringt: Unabhängig davon, ob genau der veröffentlichte Quellcode im Einsatz ist, kann überprüft werden, ob die Stimme unverändert in das Ergebnis eingeht und das Ergebnis korrekt berechnet wurde. Die Veröffentlichung des Quellcodes ist dennoch zusätzlich empfohlen, um analysieren zu können, inwieweit das Wahlgeheimnis gesichert ist, sowie allgemein, um das Vertrauen in das System zu erhöhen.

3 Online-Abstimmung im Rahmen des CDU-Bundesparteitags

3.1 Beschreibung der Situation

Aufgrund der Corona-Pandemie fand im Jahr 2021 der Bundesparteitag der CDU erstmalig digital statt. Ein Novum dieses Parteitags war darüber hinaus, dass die 1.001 Delegierten erstmalig über den zukünftigen Vorsitzenden der CDU digital abstimmen konnten. Dabei handelte es sich um eine geheime Abstimmung. Wegen der absehbaren Bedeutung des CDU-Vorsitzes für die Kanzlerschaft im Jahr 2021 war der digitale Parteitag und die digitale Abstimmung von großem medialem Interesse.

Zur Durchführung der digitalen Abstimmung setzte die Partei auf den Online-Wahldienstleister Polyas[7]. Zur Durchführung der Online-Abstimmung wurde eine neue Version, Polyas Core 3.0, des BSI-zertifizierten Polyas Core 2.2.3 eingesetzt, durch das

[5] `https://www.youtube.com/watch?v=w6gFwp30ii4` (Stand: 23.08.2021)

[6] Siehe zum Öffentlichkeitsgrundsatzes die Rechtsprechung des Bundesverfassungsgerichts zur Vereinbarkeit der elektronischen Wahl mit den Wahlrechtsgrundsätzen (Urteil vom 30. Mai 2013 – 1 N 240/12 –, juris)

[7] `https://www.polyas.de/blog/de/allgemein-de/der-cdu-bundesparteitag-und-polyas` (Stand: 23.08.2021)

„[. . .] die eigene Stimmabgabe sowie das gesamte Wahlergebnis überprüfbar geworden“ sind.

Zwar ist die genaue Spezifikation sowie der Quellcode dieser neuen Version nicht öffentlich, aber die Funktionsweise des digitalen Abstimmungsverfahrens wird in mehreren Quellen beschrieben, u. a. dem Cyber-Sicherheits-Podcast der Allianz für Cybersicherheit[8]. Im Folgenden zitieren wir zwei konkrete Quellen:

1. Polyas selbst schreibt[9]: „Die 1.001 Delegierten erhielten zufällig gemischte Zugangsdaten zum Abstimmungssystem, die aus einer Wähler-Kennung und einem Passwort bestanden gemeinsam mit ihren Wahlunterlagen. Anhand dieser Codes konnte das POLYAS System die Wahlberechtigten eindeutig authentifizieren, ohne deren genaue Identität zu kennen.

   Wurde ein Stimmzettel in die digitale Wahlurne gelegt, erhielten die Abstimmenden einen Verifikations-Code, der ihre Wahlentscheidung anonym belegt. Nach Ablauf des Parteitages legte die Wahlleitung der CDU alle anonymen Verifikations-Codes sowie die dazugehörigen Voten aus, sodass die Stimmberechtigten überprüfen können, ob ihre Entscheidung so gespeichert und ausgezählt wurde, wie sie das wollten. Hierfür sind weder technische Vorkenntnisse noch Expertenwissen notwendig und das Wahlergebnis kann als gesichert und die Wahl als integer gelten.“
2. Die CDU schreibt auf ihrer Webseite zum „1. digitalen Parteitag der CDU – So funktionierten die Abstimmungen“[10]:

   „Nach jedem Wahlgang haben die Abstimmenden in der digitalen Wahlkabine einen Verifikations-Code erhalten. Dieser Verifikations-Code ist anonym für jeden abgegebenen Stimmzettel in der digitalen Wahlurne hinterlegt. Nach Auszählung der Wahlurne können alle Verifikations-Codes und die dazugehörigen Voten in eine Liste zusammengestellt werden, um von der Wahlleitung und den Stimmberechtigten zur Überprüfung des Ergebnisses eingesehen zu werden. Jede Delegierte und jeder Delegierte kann anhand der Verifikations-Codes überprüfen, ob seine Stimme richtig gezählt wurde. Hierfür sind weder technische Vorkenntnisse noch Expertenwissen notwendig. Weder POLYAS noch die CDU-Bundesgeschäftsstelle können eine Verbindung zwischen Delegiertem und dem anonymen Verifikations-Code herstellen.“

3.2 Einordnung der Situation

Wir möchten zunächst auf einen konkreten Angriffsvektor im Bezug auf die Forderungen nach Öffentlichkeit, Nachvollziehbarkeit bzw. Überprüfbarkeit hinweisen. Dann diskutieren wir die Bedeutung des Verweises auf ein BSI-Zertifikat durch die Firma Polyas.

3.2.1 Überprüfbarkeit durch Verifikations-Code

Zunächst beschreiben wir den Mechanismus zur Umsetzung der Forderungen nach Öffentlichkeit, Nachvollziehbarkeit bzw. Überprüfbarkeit: Zur Gewährleistung, dass

[8] `https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/_/infos/20200303_podcast_04.html` (Stand: 23.08.2021)

[9] `https://www.polyas.de/blog/de/allgemein-de/der-cdu-bundesparteitag-und-polyas` (Stand: 23.08.2021)

[10] `https://archiv.cdu.de/artikel/1-digitaler-parteitag-der-cdu-so-funktionierten-die-abstimmungen` (Stand: 23.08.2021)

die Stimme wie beabsichtigt abgegeben und in der digitalen Wahlurne gespeichert wird, stellt das digitale Abstimmungsverfahren den Delegierten nach ihrer Stimmabgabe einen sogenannten Verifikations-Code zur Verfügung, der ihre Wahlentscheidung anonym belegt. Nach Abschluss des Parteitags stellte die CDU alle anonymen Verifikations-Codes sowie die dazugehörigen Stimmen bereit.

Der Einsatz derartiger Codes wurde in wissenschaftlichen Arbeiten bereits diskutiert. Sogenannte Clash-Attacken (Clash Attacks)[11] stellen eine Bedrohung dar. Einfach ausgedrückt würde ein Angreifer denselben Code an mehrere Delegierte ausstellen, die denselben Kandidaten gewählt haben. Die dadurch 'frei werdenden' Stimmen kann der Angreifer anderen Kandidat*innen zuordnen. Der Angreifer könnte dabei

1. ein Cyberkrimineller, der sich entweder Zugriff auf die Wahlserver oder auf (einzelne) Endgeräte[12] der Delegierten verschafft,
2. der Online-Wahldienstleister (z. B., weil dieser erpresst wird) oder
3. der Wahlserver-Administrator (z. B., weil dieser erpresst wird) sein.

Zur Veranschaulichung stellen wir Clash-Attacken anhand eines fiktiven Beispiels dar: Angenommen, zwei Delegierte, nennen wir sie Alice und Bob, stimmen in einer fiktiven Wahl für Kandidaten Charly, dann könnte ein Angreifer beiden denselben Verifikations-Code, sagen wir ABCD, zurückliefern, allerdings nur eine Stimme für Charly zählen. Angenommen, beide würden von der Möglichkeit der Überprüfung Gebrauch machen. Dann würden sowohl Alice wie auch Bob den erwarteten Code ABCD neben dem Kandidaten Charly finden. De facto wäre aber nur eine Stimme für Charly gewertet anstatt zwei Stimmen. Dieser Angriff kann selbstverständlich geschickt skaliert werden und somit größeren Schaden anrichten als die Unterschlagung einer einzelnen Stimme. In diesem Beispiel können Alice und Bob den Angriff nur aufdecken, wenn sie sich gegenseitig offenlegen, wie sie gewählt haben, und ihre Verifikations-Codes vergleichen, also letztlich nur durch die Verletzung ihres eigenen Wahlgeheimnisses.

Zusammenfassend besteht also die Möglichkeit eines Angriffs zur Manipulation des Wahlergebnisses, solange das Wahlverfahren nicht grundlegend geändert wird. Wie genau eine solche Änderung aussehen könnte, ist offen, da es gleichzeitig nicht möglich sein sollte, dass eine Teilmenge der Wähler behaupten kann, denselben Code bekommen zu haben. Mit dieser Erkenntnis ist es dann wichtig, das Risiko zu bewerten, dass

1. ein Cyberkrimineller sich Zugriff auf die Wahlserver oder auf (einzelne) Endgeräte der Delegierten verschafft,
2. der Online-Wahldienstleister unautorisierte Änderungen am Wahlsystem vornimmt (z. B., weil dieser erpresst wird) oder
3. der Wahlserver-Administrator unautorisierte Änderungen am Wahlsystem vornimmt (z. B., weil dieser erpresst wird).

Uns ist nicht bekannt, ob und inwieweit risikomitigierende Maßnahmen zur Abwehr des dargestellten Angriffs ergriffen wurden. Dies wäre zu prüfen, um die oben zitierten Aussagen einordnen zu können.

[11] Siehe z. B. [9]

[12] Mit Endgerät ist die technische Umgebung gemeint, über die Delegierte ihre Stimme abgeben z.B. der Laptop oder das Smartphone. Es ist nicht erforderlich, dass Cyberkriminelle physischen Zugriff auf die Endgeräte erhalten. In der Regel verschaffen sich Cyberkriminelle über das Internet Zugriff auf die Endgeräte.

Bei der Bewertung des entsprechenden Risikos sollte berücksichtigt werden, dass die Abstimmungen des Bundesparteitags aus rechtlichen Gründen in Form einer analogen Briefwahl bestätigt werden mussten und bestätigt wurden.

Auch wenn an dieser Stelle das Beispiel der Online-Abstimmung im Rahmen des CDU-Bundesparteitags angeführt wird, bleibt festzuhalten, dass Polyas-Systeme auch für Abstimmungen von anderen Parteien genutzt werden[13]. So führte beispielsweise die FDP Nordrhein-Westfalen nach der Landtagswahl 2017 eine Online-Abstimmung per Mitgliederentscheid über den Koalitionsvertrag mit der CDU unter Zuhilfenahme eines Polyas-Systems durch[14]. Weitere technische Hintergründe zum eingesetzten System liegen uns nicht vor.

3.2.2 Aussagekraft des Verweises auf das BSI-Zertifikat

Polyas Core 2.2.3 wurde 2016 nach dem Common-Criteria-Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, 18. April 2008, BSI-CC-PP-0037-2008[15], evaluiert und vom BSI zertifiziert. Zur Einordnung dieser Aussage sind u. a. folgende Fakten relevant (siehe auch Kapitel 7):

- Das Schutzprofil ist auf den Seiten des BSI im Archiv-Bereich zu finden und wird dort mit der Überschrift „Schutzprofile nach Common Criteria (CC) für IT-Produkte, die nicht mehr für Produktzertifizierungen zur Verfügung stehen“ geführt[16]. Demnach wird dieses Schutzprofil nicht mehr für Zertifizierungen neuer IT-Produkte durch das BSI eingesetzt.
- Jegliche Änderung an dem System, welches evaluiert wurde, führt dazu, dass das Zertifikat nicht mehr gilt. Eine neue Funktion wie die der Verifikations-Codes kann zu einer Verletzung der Sicherheitseigenschaften führen und muss daher neu bewertet werden. Entsprechend gilt das Zertifikat für das System, welches bei der CDU zum Einsatz kam, nicht.

4 Online-Wahlen der Universität Jena

4.1 Beschreibung der Situation

Die Friedrich-Schiller-Universität in Jena gehört zu den ersten Hochschulen, die Online-Wahlen erprobt haben. Im Jahr 2013 führte eine Novellierung der Wahlordnung der Friedrich-Schiller-Universität dazu, dass Online-Wahlen grundsätzlich für alle Gremienwahlen möglich sind (§ 16 (1) Wahlordnung[17]). Soweit bekannt, werden zur Durchführung von Online-Wahlen Systeme der Firma Polyas eingesetzt. Dabei kam zunächst ein System zum Einsatz, bei dem die Wähler*innen per Post Zugangsdaten zugeschickt

[13] `https://www.polyas.de/parteien` (Stand: 23.08.2021)

[14] `https://www.polyas.de/parteien/mitgliederentscheid/erfahrungsberichte/fdp-nrw` (Stand: 23.08.2021)

[15] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862a_pdf.pdf` (Stand: 23.08.2021)

[16] `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Schutzprofile-Protection-Profiles-PP/SchutzprofileProtectionProfiles_Archiv/schutzprofile_pps_archiv_node.html` (Stand: 23.08.2021)

[17] `https://www.hanfried.uni-jena.de/vhbmedia/Wahlordnung.pdf` (Stand: 23.08.2021)

bekamen. Seit 2016 erfolgt die Anmeldung über das universitätseigene Serviceportal[18]. Wähler*innen erhalten dort einen Link und werden an das Wahlsystem weitergeleitet. Dadurch müssen keine Briefe mit separaten Zugangsdaten verschickt werden. Das Verfahren bezeichnet die Firma Polyas als 'Secure Link'.

Während es im Kontext der Gremienwahlen an der Friedrich-Schiller-Universität in Jena schon mehrere Gerichtsverfahren gab, liegt der Fokus im Folgenden auf dem Urteil der 2. Kammer des Verwaltungsgerichts Gera mit dem Aktenzeichen 2 K 606/16 Ge[19]. Die folgenden beiden Abschnitte finden sich im Urteil:

1. *Secure Link* „Der Kläger verweist in diesem Zusammenhang zwar zutreffend auf die im Zertifizierungsreport enthaltenen Auflagen und Hinweise (s. dort S. 24): ‚Dem Benutzer wird für die Anmeldung eine HTML-Seite mit Eingabefeldern für PIN/TAN (Wähler) bzw. Benutzername/Passwort (Wahlvorstand) präsentiert. Im Rahmen der Gestaltung der umgebenden WWW-Applikation besteht grundsätzlich die technische Möglichkeit, die Anmeldung anders zu gestalten, etwa durch vorgelagerte Schritte zur Authentifizierung mit anderen Mechanismen (Smartcard, Biometrie, Single-Sign-On). Derartige Erweiterungen sind in der evaluierten Konfiguration nicht zulässig.'

   Er verkennt jedoch, dass dort gerade nicht die Erweiterung des zertifizierten elektronischen Wahlsystems durch eine Authentifizierung mittels eines Secure Links ausgeschlossen wird. Es werden stattdessen ausdrücklich nur vorgelagerte Schritte zur Authentifizierung mittels Smartcard, Biometrie oder Single-Sign-On für unzulässig erklärt. Es sind keine Anhaltspunkte dafür gegeben, dass das BSI diese aufgeführten Mechanismen beispielhaft benennen wollte. Ein entsprechender Zusatz (‚etc.' oder ‚insbesondere') ist nicht gegeben."

2. *Öffentlichkeitsgrundsatz* „Das Thüringer Oberverwaltungsgericht hat unter Anwendung der Rechtsprechung des Bundesverfassungsgerichts zur Vereinbarkeit der elektronischen Wahl mit den Wahlrechtsgrundsätzen ausgeführt (Urteil vom 30. Mai 2013 – 1 N 240/12 –, juris): ‚[. . .] Entgegen der Ansicht des Klägers entspricht § 26 Abs. 7 Satz 3 WahlO auch dem Grundsatz der Öffentlichkeit. [. . .] dass der Grundsatz der Öffentlichkeit der Wahl die Ordnungsmäßigkeit und Nachvollziehbarkeit der Wahlvorgänge sichert und damit eine wesentliche Voraussetzung für begründetes Vertrauen der Bürger in den korrekten Ablauf der Wahl schafft. Dieser Grundsatz ist auch auf außerparlamentarische Wahlen anwendbar. Dafür spricht zum einen, dass sich der Grundsatz der Öffentlichkeit unmittelbar aus dem Rechtsstaatsprinzip ableitet (BVerfG, a.a.O., Rz. 110). Zum anderen sieht auch die Wahlordnung der Antragsgegnerin in § 26 Abs. 6 Satz 1 vor, dass die Stimmauszählung universitätsöffentlich ist. [. . .] So müssen sowohl Wähler, Wahlvorstand als auch Bürger bei einer Wahl überprüfen können, ob die abgegebenen Stimmen auch unverfälscht von den Wahlgeräten erfasst werden (Rz. 155). Darüber hinaus müssen die Wahlorgane und Bürger nachvollziehen können, ob die gültigen Stimmen den Wahlvorschlägen zutreffend zugeordnet und die Stimmen auch zutreffend ermittelt wurden (Rz. 156). Dagegen reicht es nicht aus, wenn im Wahlgerät selbst ein Rechenprozess (internes Datenverarbeitungsprogramm) stattfindet, den lediglich IT-Experten entschlüsseln können.

[18] `https://www.duz.de/beitrag/!/id/398/online-hochschulwahlen--mein-gutes-recht` (Stand: 23.08.2021)

[19] `http://www.thovg.thueringen.de/webthfj/webthfj.nsf/6DE61C659283F975C125815B0036E1DD/\$File/16-2K-00606-U-A.pdf` (Stand: 23.08.2021)

> Insoweit fordert das Bundesverfassungsgericht ausdrücklich, dass auch der technische Laie das Ergebnis nachvollziehen können muss.‘ Mindestanforderungen zur Gewährleistung des Grundsatzes der Öffentlichkeit stellen daher die Kontrolle der Wahlhandlung durch den Wähler sowie die nachträgliche Überprüfung der Ergebnismitteilung dar. [...] Anlässlich der mündlichen Verhandlung wurden die mittels des Tools zur Reproduzierbarmachung generierten Wahlunterlagen vorgelegt. Diese beinhalten nicht nur eine Gesamtübersicht der bereits computerbasiert ausgezählten und addierten elektronischen Stimmen im Hinblick auf die einzelnen Wahlbereiche. Es erfolgt des Weiteren eine Aufschlüsselung der Einzelstimmen in den einzelnen Wahlbereichen in tabellarischer Form. Eine selbstständige Addition der Stimmen durch den die Wahl Anfechtenden wird auf diese Weise ermöglicht. Vor diesem Hintergrund ist die mit der Durchführung einer elektronischen Wahl möglicherweise verbundene Einschränkung des Wahlgrundsatzes der Öffentlichkeit hinzunehmen.“

Auch das Urteil des Thüringer Oberverwaltungsgerichts (4 KO 395/19)[20] äußert sich zum Öffentlichkeitsgrundsatz bei den Online-Wahlen an der Universität Jena: „... Diese Beschränkung ist jedoch verfassungsrechtlich zulässig, wenn die vom Bundesverfassungsgericht in der Grundsatzentscheidung aus dem Jahr 2009 zur Bundestagswahl enthaltenen Mindestvorgaben eingehalten sind. Diese Mindestanforderungen beinhalten zunächst die Möglichkeit der Kontrolle der eigenen Wahlhandlung und Stimmabgabe durch den Wähler. Diesen Anforderungen werden die § 25a Abs. 2 Sätze 6 und 8 WahlO gerecht. Danach kann der Wähler bis zur endgültigen Stimmabgabe die Eingabe korrigieren oder die Wahl abbrechen und erhält eine Information über die endgültige Stimmabgabe.“[21]

4.2 Einordnung der Situation

In Bezug auf die Frage, ob diese Urteile eine informierte Entscheidung zum Einsatz des gleichen Systems an anderen Hochschulen ermöglichen, möchten wir im Folgenden die beiden ausgewählten thematischen Bereiche diskutieren.

4.2.1 Secure Link

Zunächst möchten wir die Argumentation bzgl. des Secure Links diskutieren.

Der Zertifizierungsreport für das von der Firma Polyas durch das BSI zertifizierte Online-Wahlsystem POLYAS CORE Version 2.2.3[22] formuliert Auflagen zu dem Anmeldeverfahren. Es wird dort explizit darauf hingewiesen, dass ein System evaluiert wurde, welches eine Anmeldung mittels PIN/TAN für Wähler*innen vorsieht.

[20] `http://www.thovg.thueringen.de/webthfj/webthfj.nsf/7511A105D8820A68C12586D5002E259E/\$File/19-4KO-00395-U-A.pdf?OpenElement` (Stand: 23.08.2021)

[21] § 25a Abs. 2 Sätze 6 ff WahlO (durch Änderungen der Wahlordnung ergibt sich eine Verschiebung der Nummerierung:„[6]Die Speicherung der abgesandten Stimmen muss anonymisiert und so erfolgen, dass die Reihenfolge des Stimmeingangs nicht nachvollzogen werden kann. [7]Die Wahlberechtigten müssen bis zur endgültigen Stimmabgabe die Möglichkeit haben, ihre Eingabe zu korrigieren oder die Wahl abzubrechen. [8]Ein Absenden der Stimme ist erst auf der Grundlage einer elektronischen Bestätigung durch den Wähler zu ermöglichen. [9]Die Übermittlung muss für den Wähler am Bildschirm erkennbar sein. [10]Mit dem Hinweis über die erfolgreiche Stimmabgabe gilt diese als vollzogen.“

[22] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862a_pdf.pdf;jsessionid=DB5161E6A1CA0FAD7A3149B21E62DCB0.internet082?__blob=publicationFile&v=1` (Stand: 23.08.2021)

Ein anderes Anmeldeverfahren kann grundsätzlich neue Schwachstellen mit sich bringen. Entsprechend kann dies nicht einfach ausgetauscht werden, ohne diese Änderung evaluieren und zertifizieren zu lassen. Konkret gilt die durchgeführte Zertifizierung entsprechend nicht mehr, wenn ein anderes Anmeldeverfahren zum Einsatz kommt. Eine neue Evaluierung und Zertifizierung wäre notwendig. Entsprechend ist es wahrscheinlich ein Versehen, dass hier in der Formulierung der Auflage gesagt wird „mit anderen Mechanismen (Smartcard, Biometrie, Single-Sign-On)“ und in der Klammer kein ‘usw.’ oder ein ‘insbesondere’ verwendet wurde.

Für die weiteren Ausführungen gehen wir dennoch davon aus, der Zertifizierungsreport bezieht sich wirklich nur auf die drei genannten Mechanismen. Im Folgenden gehen wir der Frage nach, ob die von Polyas gewählte Formulierung des ‘Secure Links’ nicht eine Form von Single-Sign-On ist. Hierzu ist es wichtig zu verstehen, was mit Single-Sign-On gemeint ist. Dies wird explizit in den Auflagen des Zertifizierungsreports ausgeschlossen: „[. . .] sind in der evaluierten Konfiguration nicht zulässig“. Der IT-Planungsrat[23] definiert Single-Sign-On wie folgt: „‚Single Log-In‘ bzw. ‚Single Account‘: Die Möglichkeit, sich mit nur einem Satz an Zugangsdaten in verschiedene geschützte Dienste einzuloggen bzw. gegenüber verschiedenen Diensten mit einem definierten Vertrauensniveau zu authentifizieren.“

Die Firma Polyas verwendet die Bezeichnung Secure Link. Es passiert aber genau das, was hier in der Erklärung von Single-Sign-On beschrieben wird: Der Secure-Link-Ansatz ermöglichst es Wähler*innen, sich mit nur einem Satz an Zugangsdaten (den Uni-Zugangsdaten) in verschiedenen Diensten – eben auch dem Online-Wahlsystem – einzuloggen.

Folgt man dieser Argumentation, ist das eingesetzte Online-Wahlsystem nicht zertifiziert.

4.2.2 Öffentlichkeitsgrundsatz

Im Folgenden diskutieren wir die vorgetragene Argumentation zum Öffentlichkeitsgrundsatz. Hier wurden zunächst Erläuterungen aus dem Urteil vom 30. Mai 2013 – 1 N 240/12 zitiert. Daraus leitet das Verwaltungsgericht Gera ab, dass „Mindestanforderungen zur Gewährleistung des Grundsatzes der Öffentlichkeit [. . .] die Kontrolle der Wahlhandlung durch den Wähler sowie die nachträgliche Überprüfung der Ergebnismitteilung dar[stellen]“. Dies bestätigt auch das Oberverwaltungsgericht Thüringen.

Die Kontrolle der Wahlhandlung durch die Wählenden ist bei dem eingesetzten System nicht möglich. Es bietet lediglich die Möglichkeit der nachträglichen Überprüfung der Ergebnismitteilung, bezogen auf ein Nachzählen von Stimmen (ohne, dass ersichtlich ist, dass diese Stimmen auch denen entsprechen, die von den Wähler*innen abgegeben wurden). Dies wurde vom Verwaltungsgericht Gera als ausreichend angesehen, da die „möglicherweise verbundene Einschränkung des Wahlgrundsatzes der Öffentlichkeit hinzunehmen“ ist.

Wir stellen zunächst einen Vergleich zur Papier-Wahl bzgl. dieses Grads der Öffentlichkeit her. Stellen Sie sich vor, Sie kandidieren bei einer Wahl, bei der ein externer Dienstleister beauftragt wird, Stimmen an nicht-öffentlichen Orten entgegenzunehmen, dann mit der Urne an einen geheimen Ort geht und Ihnen dann das Ergebnis präsentiert. Sie verlieren die Wahl, können das aber kaum glauben. Um Sie zu überzeugen, zeigt der externe Dienstleister Ihnen eine Urne mit Stimmen, die Sie selbst

[23] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/28_Sitzung/TOP06_Anlage1_SSO.pdf;jsessionid=B768543D5CA0C9F0A3226B4242FFE587.1_cid350?__blob=publicationFile&v=9 (Stand: 23.08.2021)

nachzählen können. Würden Sie darauf vertrauen, dass die in der Urne enthaltenen Stimmen auch wirklich die abgegebenen sind? Wie schwer ist es für den externen Dienstleister, die Stimmen auszutauschen? Würden Sie dies feststellen? Wären Sie jetzt davon überzeugt, dass Sie die Wahl verloren haben?

Im folgenden Abschnitt diskutieren wir die Kritikalität von Angriffen auf die unterschiedlichen Wahlkanäle, die möglich sind, wenn nur die Auszählung öffentlich ist. Hierdurch soll gezeigt werden, dass es bei Online-Wahlen besonders wichtig ist, dass alle Schritte der Stimmabgabe, der Stimmspeicherung und der Auszählung öffentlich sind, sprich, durch die Wähler*innen (unter Einhaltung des Wahlgeheimnisses) nachvollzogen werden können.

- Bei der Wahl im Wahllokal müssten die Wahlhelfer*innen gemeinsam korrupt agieren und die Urne bereits vor der Auszählung manipulieren (z. B., weil Stimmzettel ausgetauscht werden). Darüber hinaus könnten diese jeweils nur die Stimmen in einem oder in wenigen Wahllokalen manipulieren.
- Bei der Briefwahl müssten die Wahlhelfer*innen gemeinsam korrupt agieren und die Urne bereits vor der Auszählung manipulieren (z. B., weil Stimmzettel ausgetauscht werden). Ob so im großen Maße Manipulationen durchgeführt werden können, hängt vom Setting ab: d. h. (a) ob es nur ein Briefwahllokal oder wie bei Bundestagswahlen eine sehr große Anzahl an Briefwahllokalen gibt und (b) ob die Briefwahl nur auf Antrag möglich und der Hauptwahlkanal der im Wahllokal ist (und dadurch der Anteil der Briefwähler*innen gering ist).

  Darüber hinaus könnten Angestellte der Post Briefe entwenden. Allerdings könnten sie dies wegen des eingeschränkten Zuständigkeitsbereichs i. d. R. nur bei einigen wenigen Wähler*innen tun. Darüber hinaus könnte dies aufgedeckt werden, wenn Wähler*innen nachfragen, ob die Stimme angekommen ist.
- Bei einer Online-Wahl können Stimmen bzw. die Urne an verschiedenen Stellen im Prozess manipuliert werden: Zunächst kann dies bei der Abgabe auf dem Endgerät geschehen, dann bei der Übertragung und dann vor/während der Speicherung. Die Manipulation kann durch Cyberkriminelle oder den Anbieter des Wahlsystems (ggf. auch von Mitarbeiter*innen des Rechenzentrums, von dem das Wahlsystem betrieben wird) durchgeführt werden. Der Angriff kann von einem beliebigen Ort ausgeführt werden und dabei beliebig Stimmen verändern.

Nun stellt sich die Frage, wie man die unterschiedlichen Angriffe bewertet. In den beiden ersten Fällen (Papier-Wahl im Wahllokal und Briefwahl) müssen Wähler und Kandidaten den Wahlhelfer*innen vertrauen. Bei einem Online-Wahlsystem, wie dies an der Universität Jena eingesetzt wird, müssen Kandidat*innen und Wähler*innen darauf vertrauen, dass Cyberkriminelle kein großes Interesse an dem Ausgang der Wahl haben, sowie dass die Mitarbeiter*innen des Anbieters des Wahlsystems und des Rechenzentrums nicht korrupt sind. So besteht z. B. die Möglichkeit, dass Cyberkriminelle über Schwachstellen in der Infrastruktur oder dem Online-Wahlsystem selbst Manipulationen durchführen können. Dass solche Schwachstellen in der Realität durchaus existieren können, wird in Kapitel 6 am Beispiel von Online-Abstimmungen auf virtuellen Hauptversammlungen von Aktiengesellschaften gezeigt. Um das für Online-Wahlen notwendige Vertrauen auf ein entsprechendes Niveau zu heben, wäre es erforderlich, ein Ende-zu-Ende-verifizierbares Online-Wahlsystem einzusetzen,

Der Öffentlichkeitsgrundsatz hat das Ziel, die Ordnungsmäßigkeit und Nachvollziehbarkeit der Wahlvorgänge zu sichern. Wie die Ordnungsmäßigkeit gesichert wird, hängt vom Wahlkanal ab sowie von den zu adressierenden Ordnungsmäßigkeiten. Entsprechend kann argumentiert werden, dass eine Übertragung einer Maßnahme von

einem Wahlkanal auf einen weiteren nicht notwendigerweise ausreichend ist. Es sollte für jeden Wahlkanal neu geprüft werden, welche Maßnahmen sinnvoll und notwendig sind.

Das Thüringer Oberverwaltungsgericht untersucht die Forderung nach dem Öffentlichkeitsgrundsatz bezogen auf die Wahlordnung und kommt zu dem Ergebnis, dass die Möglichkeit der Kontrolle der eigenen Wahlhandlung und Stimmabgabe durch die Wähler*innen durch die Anforderungen in der Wahlordnung abgedeckt sind – konkret durch die folgenden Anforderungen: „Die Wahlberechtigten müssen bis zur endgültigen Stimmabgabe die Möglichkeit haben, ihre Eingabe zu korrigieren oder die Wahl abzubrechen.“ und „Die Übermittlung muss für den Wähler am Bildschirm erkennbar sein.“ Wie oben erwähnt können Angriffe an verschiedenen Stellen durchgeführt werden und sollten im Rahmen des Öffentlichkeitsgrundsatzes von Wähler*innen erkannt werden können: bei der Abgabe auf dem Endgerät, bei der Übertragung und dann vor/während der Speicherung. Aus unserer Sicht decken die beiden Anforderungen nur die Erkennung von Manipulationen bei der Übertragung ab. Um auch die anderen Manipulationen aufdecken zu können, ist es wichtig, Ende-zu-Ende-verifizierbare Wahlsysteme einzusetzen.

5 Online-Wahlen bei der Gesellschaft für Informatik (GI)

5.1 Beschreibung der Situation

„Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 kooperativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik.“[24]

Die GI führt ihre jährlichen Wahlen (Vorstands- und Präsidiumswahlen) seit 2004 online durch. Mitglieder können ihre Stimme auf Antrag auch per Briefwahl abgeben. Die Zugangsdaten zum Online-Wahlsystem bestehen aus der GI-Mitgliedsnummer und einem Passwort, welches den Wähler*innen per Post zugeschickt wird. Hierzu wurden unterschiedliche Systeme der Firma Polyas eingesetzt. Nachdem viele Jahre sogenannte Blackbox-Systeme der Firma Polyas zum Einsatz kamen, wurde 2018 entschieden, auf ein Ende-zu-Ende-verifizierbares System umzustellen[25], was jedoch bis heute nicht vollständig umgesetzt ist. Diese Umsetzung sollte in zwei Schritten erfolgen und sollte von einem losen Kreis aus interessierten Informatikern der GI begleitet werden: 2019 sollte auf einen anderen Kern aufgesetzt werden, da das Blackbox-System nicht erweiterbar ist, um Ende-zu-Ende-Verifizierung zu ermöglichen. 2020 sollte die individuelle Verifizierung angeboten werden. Die Schnittstellen zur Implementierung von Verifizierungstools durch Hochschulen wurden sowohl 2019 für die universelle Verifizierbarkeit als auch 2020 für die individuelle Verifizierbarkeit angekündigt. Die Umstellung 2019 erfolgte wie geplant. Das Karlsruher Institut für Technologie sowie die Universität Stuttgart hatten Tools implementiert, mit denen die universelle Verifizierung umgesetzt werden konnte. Diese wurden eingesetzt. Es wurde mit diesen Tools überprüft, dass alle Stimmen, die in der elektronischen Urne waren, korrekt ausgezählt wurden

[24] `https://gi.de/ueber-uns` (Stand: 23.08.2021)
[25] Siehe [3].

und dass nur Stimmen von Wahlberechtigten in der elektronischen Urne vorhanden waren. Nicht überprüft werden konnte in 2019, dass die Stimmen in der Urne auch dem Willen der Wähler*innen entsprochen hat. Dies Möglichkeit dies zu überprüfen (und damit die Umsetzung der individuellen Verifizierbarkeit) sollte 2020 umgesetzt werden. 2020 wurde die individuelle Verifizierbarkeit von der Firma Polyas nicht integriert.

5.2 Einordnung der Situation

Die folgenden Ausführungen zu den Online-Wahlen der Gesellschaft für Informatik basieren auf persönlichen Gesprächen mit Vertreterinnen und Vertretern der GI, u.a. mit Prof. Dr. Rüdiger Grimm, Mitglied des GI-Wahlausschuss. Die bei der GI bisher eingesetzten Systeme bergen eine Reihe von Risiken. Hierzu zählen u. a.:

1. Manipulationen durch den Anbieter Polyas können weder von der GI noch den Wähler*innen und Kandidat*innen erkannt werden.
2. Manipulationen durch den Betreiber der Rechenzentren oder durch Cyberkriminelle können nicht zuverlässig erkannt werden.
3. Schadsoftware auf den Endgeräten der Wähler*innen kann unbemerkt die Stimme verändern.

Die GI-Verantwortlichen kennen die Risiken der eingesetzten Systeme. Sie halten dies für die Vorstands- und Präsidiumswahlen der GI für vertretbar. Gründe hierfür sind u. a., dass man den Mitgliedern zutraut, ihre Endgeräte adäquat abzusichern; sowie dass davon ausgegangen wird, dass weder Kandidat*innen noch Externe ein Interesse daran haben, die Wahl zu manipulieren, da die Gewählten sich in erster Linie in besonderem Maße für den Verein engagieren und es sich um ehrenamtliche Positionen handelt. Nicht zuletzt hat man auch entschieden, dass man Polyas vertraut, keine Manipulationen vorzunehmen.

Es gab und gibt aber auch Kritiker – sowohl von Online-Wahlen im Allgemeinen als auch der eingesetzten Systeme. U. a. aus diesem Grund steht es allen Mitgliedern frei, Briefwahl zu beantragen.

Die GI ist sich bewusst, dass manche Wahlausrichter schauen, welche Systeme die GI einsetzt. Das Risiko der eingesetzten Systeme hängt allerdings nicht von dem vorhandenen Security-Hintergrundwissen der Wähler*innen ab. Daher ist es wichtig, dass jeder Wahlausrichter für die durchzuführende Wahl selbst entscheidet, ob die Risiken bzw. Angriffsmöglichkeiten, die das jeweilige Online-Wahlsystem mit sich bringt, für die eigene Wahl vertretbar sind oder nicht.

Das Risiko wird deutlich reduziert, wenn Ende-zu-Ende-verifizierbare Systeme eingesetzt werden. Nachdem international der Paradigmen-Wechsel zu Ende-zu-Ende-verifizierbaren Systemen vollzogen wurde, hat die GI entschieden, dass sie ebenfalls ein solches System einsetzen möchte. Ende-zu-Ende-verifizierbare Systeme können nicht allein von einem Online-Wahldienstleister umgesetzt werden, sondern es werden unabhängige Dritt-Dienstleister benötigt, die Tools zur Durchführung der Verifizierungsschritte bereitstellen. Diese Tools sind deutlich unaufwendiger umzusetzen als die Durchführung der eigentlichen Stimmabgabe und -auszählung. Dennoch müssen diese unabhängigen Dritten gefunden werden. Hier hat die GI einen Vorteil, da ausreichend Expertise bei den Mitgliedern gegeben ist, solche Tools zu implementieren.

Aufgrund des gewachsenen Vertrauens in die Firma Polyas wurde 2018 entschieden, der Firma die Möglichkeit zu geben, über zwei Jahre (2019/2020) ein Ende-zu-Ende-verifizierbares System anzubieten, welches für die Wahlen der GI geeignet ist. Der

Zeitraum wurde seitens der Firma Polyas leider nicht eingehalten. Die GI hofft, dass sie 2022 ein Ende-zu-Ende-verifizierbares Wahlsystem der Firma Polyas einsetzen kann.

6 Aktionärswahlen

6.1 Beschreibung der Situation

Die Corona-Pandemie war die Geburtsstunde der virtuellen Hauptversammlung (HV) von Aktiengesellschaften. Aufgrund der geltenden Reise- und Kontaktbeschränkungen wurde 2020 ein Großteil der HVs nicht mehr in Präsenz, sondern als digitale Abstimmung online über das Internet durchgeführt. Die erste rein virtuelle HV veranstaltete die Bayer AG für Kosten von rund 1 Million Euro am 28. April 2020[26]. An dieser Veranstaltung nahmen mehr als 5.000 stimmberechtigte Aktionäre teil. Die Grundlage für die Durchführung von virtuellen HVs ist das am 27. März 2020 vom Bundesrat im Eilverfahren verabschiedete Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht[27]. Seitdem hat sich die virtuelle HV schnell und in voller Breite als gesellschaftsrechtliches Kriseninstrument etabliert. Unlängst wurde das Gesetz bis Ende 2021 verlängert[28] und nach Ansicht der Länder-Justizminister soll die virtuelle HV dauerhaft eine gleichberechtigte Alternative zur Präsenz-HV werden[29].

Bei einer virtuellen HV werden von den Aktionären kritische Unternehmensentscheidungen (z. B. Entlastung von Vorstand und Aufsichtsrat, Gewinnverwendung und Kapitalmaßnahmen) in Form einer Online-Wahl getroffen. Zugleich werden in diesem Kontext sehr sensible personenbezogene Daten von den Anteilseignern verarbeitet. Deshalb bedienen sich die Aktiengesellschaften in aller Regel eines spezialisierten HV-Dienstleisters, welcher neben organisatorischer und rechtlicher Unterstützung auch ein *HV-Portal* zur praktischen Durchführung der virtuellen HV im Internet zur Verfügung stellt. Die Online-Wahl-Funktionalität ist hierbei immer ein wesentlicher Bestandteil.

In einer auf dem 17. Deutschen IT-Sicherheitskongress des BSI im Februar 2021 veröffentlichten empirischen Studie wurde die Sicherheit von acht HV-Portalen analysiert [10]. Insgesamt wurden im Zeitraum vom 28. April 2020 bis 31. Dezember 2020 in diesen HV-Portalen 584 virtuelle HVs deutscher Aktiengesellschaften durchgeführt. Im Ergebnis wiesen knapp 72 % der untersuchten virtuellen HVs kritische Schwachstellen auf, welche u. a. das unbemerkte Ändern der Stimmabgabe von Aktionären, die vollständige Übernahme des Aktionärs-Accounts durch den Angreifer, das gezielte Verhindern der Durchführung von virtuellen HVs oder das Auslesen der personenbezogenen Daten von Aktionären ermöglichten. Letztere Sicherheitslücke erlaubte es bei dem HV-Portal des Marktführers (über 160 virtuelle HVs waren potenziell betroffen), die personenbezogenen Daten (Name, Adresse, Geburtsdatum, etc.) aller Aktionäre, inkl. Abstimmungsverhalten und deren Anteilsbesitz, von allen durch den HV-Dienstleister durchgeführten HVs auszulesen. Von den gefundenen Sicherheitslücken waren u. a. auch virtuelle HVs von großen DAX- und MDAX-Konzernen betroffen. Insgesamt

[26] `https://www.juve.de/nachrichten/deals/2020/04/aktionaerstreffen-linklaters-mandantin-bayer-spart-mit-online-hv-25-millionen-euro` (Stand: 23.08.2021)

[27] `https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Corona-Pandemie.pdf` (Stand: 23.08.2021)

[28] `https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2020/102920_Virtuelle_Hauptversammlung.html` (Stand: 23.08.2021)

[29] `https://www.zeit.de/news/2021-06/17/justizminister-wollen-dauerhaft-virtuelle-hauptversammlung` (Stand: 23.08.2021)

konnten in sechs von acht untersuchten HV-Portalen über das Internet ausnutzbare Schwachstellen gefunden werden.

6.2 Einordnung der Situation

Die Ergebnisse der oben genannten Studie offenbarten deutliche Sicherheitsmängel bei nahezu allen untersuchten HV-Portalen. Es ist hervorzuheben, dass nur wohlbekannte und webbasierte Angriffe aus der OWASP-Top-10-Liste[30] in Betracht gezogen wurden. Die potenziellen Angreifer waren hierbei außenstehende Cyberkriminelle, die durch den Kauf von Aktien auch die Berechtigung zur Teilnahme an den virtuellen HVs erworben haben[31]. Das Nachrichtenportal Heise Online fand für den Sachverhalt klare Worte und spricht von „Anfängerfehlern“[32].

In Gesprächen mit den beteiligten HV-Dienstleistern wurde zudem klar, dass die Kunden bei der Entscheidung für einen Anbieter häufig nur anhand der gebotenen Funktionalität und des Preises entscheiden. Eine Risikobewertung inkl. Abschätzung und Test des notwendigen Sicherheitsniveaus findet dabei nur in seltenen Fällen statt. Dabei ist es aus Risikosicht ein großer Unterschied, ob bei einer HV eine Kampfabstimmung über den Unternehmensfortbestand ansteht, wie bei der Kapitalmaßnahme der Lufthansa AG im Herbst 2020, oder ob bei einer kleinen Aktiengesellschaft mit überschaubarem Aktionärskreis eine 'Standard'-Tagesordnung zur Abstimmung vorliegt. Häufig wissen die Aktiengesellschaften auch im Vorfeld, ob mit gezielten Störungen durch Aktivisten zu rechnen ist. Für Aktiengesellschaften wäre deshalb ein Katalog von Sicherheitsanforderungen wünschenswert, um das aus der Risikobewertung ermittelte notwendige Sicherheitsniveau bei dem HV-Dienstleister abzufragen bzw. mit deren Sicherheitsanforderungen und Annahmen abzugleichen.

Keine Ende-zu-Ende-Verifizierbarkeit Bei dieser Untersuchung wurden bezogen auf das Angreifermodell einige Angriffsvektoren nicht untersucht. So wurden keine Angriffe durch andere Akteure, z. B. (bösartige) Server-Administratoren, Wahlleiter oder die HV-Dienstleister selbst, in Betracht gezogen. Es gilt jedoch festzuhalten, dass weitergehende Methoden zur Umsetzung von Öffentlichkeit, Nachvollziehbarkeit und Überprüfbarkeit der individuellen Stimmabgabe sowie der Auszählung aller abgegebenen Stimmen, nach eigenen Recherchen, aktuell von keinem HV-Dienstleister angeboten werden.

So ist es zwischenzeitlich zwar möglich, sich in den meisten HV-Portalen einen Nachweis über die eigene Stimmabgabe als PDF-Datei erstellen zu lassen. Gegen am Wahlprozess beteiligte bösartige Akteure oder kompromittierte Endgeräte hilft dieses Dokument jedoch wenig. Zudem ist auch nicht klar, wie ein Notar die Unversehrtheit des Wahlsystems sicherstellen und die Abstimmungsergebnisse am Ende der virtuellen HV gegenüber Fehlern und Manipulationen überprüfen kann.

[30] Open Web Application Security Project (OWASP) `https://owasp.org/www-project-top-ten/` (Stand: 23.08.2021)

[31] Zur Teilnahme an einer HV reicht der Kauf einer Aktie aus. Die Kosten hierfür belaufen sich, je nach Höhe des Aktienkurses, auf weniger als 100 €.

[32] `https://www.heise.de/news/Virtuelle-Hauptversammlungen-mit-Anfaengerfehlern-5045689.html` (Stand: 23.08.2021)

7 BSI-Zertifizierung nach Common Criteria

7.1 Allgemeine Informationen zum Evaluations- und Zertifizierungsverfahren

Ähnlich wie in anderen sicherheitskritischen Bereichen unseres Lebens, zum Beispiel im Lebensmittel- und Gesundheitswesen, ist es auch in der Informationssicherheit empfehlenswert, die sicherheitsrelevanten Eigenschaften der jeweiligen IT-Produkte zu prüfen, bevor diese zugelassen bzw. eingesetzt werden. Ein Zulassungsverfahren besteht in der Regel aus zwei Schritten: der *Evaluierung* und der *Zertifizierung*.

Die *Evaluierung* umfasst die Prüfung und sicherheitstechnische Bewertung eines IT-Produktes (d. h. des Evaluierungsgegenstandes) gemäß wohldefinierter Sicherheitsanforderungen sowie Annahmen an die Einsatzumgebung und die Angreifermächtigkeit unter Anwendung einer wohldefinierten Prüfmethodik. Die Prüfstelle, die die Evaluierung durchführt, wird häufig vom Hersteller des IT-Produkts bezahlt.

Die *Zertifizierung* überwacht die Evaluierung und bestätigt die Ergebnisse der Evaluierung für einen genau festgelegten Konstruktions- bzw. Versionsstand des IT-Produktes. Es ist zu beachten, dass die Zertifizierung eines IT-Produktes von externen, unabhängigen und neutralen Prüfstellen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt wird.

Ein geänderter Konstruktions- bzw. Versionsstand führt zu einer Nachevaluierung, die sich ggf. nur auf die geänderten und sicherheitsrelevanten Bestandteile beschränkt, und zu einer Aktualisierung der Zertifizierung.

Um ein IT-Produkt bezüglich dessen Sicherheitseigenschaften zu evaluieren, ist es notwendig, den Evaluierungsgegenstand (das zu evaluierende und zertifizierende IT-Produkt), die Sicherheitsanforderungen und Annahmen (potenzielle Restrisiken) sowie die Evaluierungstiefe (legt die Prüfmethodik fest) klar zu definieren.

Ein international standardisierter Evaluierungsrahmen für die Sicherheit von IT-Produkten stellt der Common Critieria (CC) Standard[33] dar. Der Common Criteria Standard umfasst folgende wesentliche Konzepte:

- Evaluierungsgegenstand (EVG) / Target of Evaluation (ToE). Das ist das IT-Produkt oder der Teil davon, das bzw. der Gegenstand der Prüfung ist.
- Schutzprofil / Protection Profile (PP). Ein Dokument, welches Sicherheitsanforderungen für eine Klasse von IT-Produkten stellt, anhand derer ein IT-Produkt evaluiert werden kann.
- Sicherheitsziel / Security Target (ST). Ein Dokument, welches Sicherheitsanforderungen für ein spezifisches IT-Produkt stellt, anhand derer ein IT-Produkt evaluiert werden kann. Dies kann auf einem PP aufbauen, muss es aber nicht.
- Funktionale Sicherheitsanforderungen / Security Functional Requirements (SFRs). Ein Katalog einzelner Sicherheitsfunktionen, die von einem IT-Produkt bereitgestellt werden können.
- Vertrauenswürdigkeitsanforderungen / Security Assurance Requirements (SARs). Beschreibungen der Maßnahmen, die während der Entwicklung und der Evaluation des IT-Produkts ergriffen wurden bzw. werden, um die Einhaltung der funktionalen Sicherheitsanforderungen sicherzustellen.

[33] `https://www.commoncriteriaportal.org/` (Stand: 23.08.2021)

- Bewertung der Sicherheitsstufe / Evaluation Assurance Level (EAL). Eine numerische Bewertung, die die Tiefe und Genauigkeit der durchgeführten Evaluation beschreibt. Jede EAL entspricht einem Paket von Sicherheitsanforderungen (SARs, siehe oben). So kann die Prüftiefe zwischen EAL 1 (funktionell getestet) und EAL 7 (formal verifizierter Entwurf und getestet) liegen.

SFRs und SARs werden weiter in Klassen und Familien unterteilt und werden in Form eines einheitlichen Vokabulars bereitgestellt. Durch die Bereitstellung dieser Anforderungskataloge ist die Vergleichbarkeit von Produkten gegeben und ein standardisiertes Vorgehen bei der Prüfung sichergestellt.

Im Folgenden fokussieren wir uns auf das Konzept der Schutzprofile. Die Idee ist, dass Nutzer*innen zukünftiger IT-Produkte festlegen, welche Sicherheitsziele das IT-Produkt und welche Sicherheitsziele die Einsatzumgebung erfüllen sollen. Außerdem können sie so die Prüftiefe und damit die Evaluationsmethoden festlegen. Schutzprofile bestehen aus folgenden Abschnitten:

- Evaluierungsgegenstand (EVG),
- Definition des Sicherheitsproblems inkl. Bedrohungen und Annahmen an die Einsatzumgebung,
- Sicherheitsziele sowohl für den EVG als auch für die Einsatzumgebung (hierbei ist wichtig, dass die Aussagen aus einer Evaluation für den EVG nur gelten, wenn er in einer Umgebung eingesetzt wird, für die die Sicherheitsziele der Einsatzumgebung erfüllt sind),
- Sicherheitsanforderungen. Diese werden in zwei Kategorien unterteilt:
  - Funktionale Sicherheitsanforderungen (SFRs) und
  - Vertrauenswürdigkeitsanforderungen (SARs).

7.2 Beschreibung der Situation

7.2.1 Common Criteria Schutzprofil für Online-Wahlen

Es existiert bereits eine Reihe CC-konformer Schutzprofile im Kontext von elektronischen Wahlen. Budurushi et al. [5] bieten einen vergleichenden Überblick. Das Schutzprofil BSI-CC-PP-0037-2008 'Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte'[34] aus dem Jahr 2008 ist das einzige mit dem Fokus auf Online-Wahlen. Dieses Schutzprofil entspricht einer erweiterten CC-Evaluierungstiefe, nämlich EAL2+. Das Dokument startet mit folgendem Anwendungshinweis: „Die Erfüllung der in diesem Schutzprofil festgelegten Anforderungen reicht aus, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich und insbesondere nicht-politischen Wahlen mit geringem Angriffspotenzial sicher auszuführen. Zur sicheren Durchführung von Online-Wahlen mit höherem Angriffspotenzial, wie etwa Betriebsratswahlen oder parlamentarische Wahlen, sind weitere Sicherheitsanforderungen zu formulieren und mit nachweisbaren Maßnahmen durchzusetzen, um die Annahmen über die Anwendungsumgebungen, wie sie hier beschrieben sind, zu erfüllen [..].“[35]

[34] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0037b_pdf.pdf` (Stand: 23.08.2021)

[35] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0037b_pdf.pdf` (Stand: 23.08.2021)

7.2.2 Zertifizierung des POLYAS Core 2.2.3

Basierend auf diesem Schutzprofil wurde ein *Security Target*[36] von der Firma Micromata für das Online-Wahlprodukt POLYAS Core 2.2.3 entwickelt[37]. Das Security Target ist ein wichtiger Bestandteil der Evaluierung und konkretisiert das Schutzprofil für das konkrete IT-Produkt.

Anhand dieses *Security Target* wurde das POLYAS Core 2.2.3 von der DFKI GmbH evaluiert und vom BSI am 10. März 2016, mit einer Gültigkeit bis zum 9. März 2021, zertifiziert.[38]

Das Security Target von 2015 beinhaltet 15 Sicherheitsziele an die Einsatzumgebung (abgekürzt mit OE). Hierzu zählen u.a. [39]:

- „OE.Endgerät: Die Vertrauenswürdigkeit des Endgerätes liegt in der Verantwortung des Wählers, da der EVG nicht die Möglichkeit und die Berechtigung hat, das gesamte Endgerät nach Malware zu untersuchen und ggf. zu beseitigen. Der [...] EVG wird [...] von dem Wähler so [...] benutzt, dass das Endgerät den Vorgang der Stimmabgabe weder beobachten noch beeinflussen kann. Dazu gehört auch, dass der Wähler sein Endgerät nicht absichtlich für solche Zwecke manipuliert. Auf dem Endgerät wird vom Wähler Software eingesetzt, die in der Lage ist, den Stimmzettel korrekt anzuzeigen, die Eingaben des Wählers korrekt an den Wahlserver zu übertragen und die Stimme nach der Wahlhandlung zu löschen. Der Wähler muss sein Endgerät gemäß einer verfügbaren Handreichung in einem vertrauenswürdigen Zustand halten. In dieser Handreichung wird erläutert, wie der Wähler sein Betriebssystem mittels gängiger Anti-Viren und Personal-Firewall-Software auf einem ausreichenden Sicherheitsstandard halten kann.“
- „OE.Wahlserver: Der Wahlvorstand nimmt seine Verantwortung zur Sicherung des Wahlservers wahr, um auszuschließen, dass ein Netzwerkangreifer Zugriff auf den Server erhält. Die Umsetzung eines entsprechenden Sicherheitskonzeptes für die Netzwerkanbindung wird über Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen, erreicht. Der EVG soll neben den benötigten Ressourcen wie Datenbank und Application Server als einzige Anwendung auf dem Betriebssystem laufen (vgl. Abschnitt 1.3.4). Der Wahlserver selbst muss gegen unbefugten Zugriff mit ausreichend starken Nutzerpasswörtern/Zertifikaten gesichert sein.“
- „OE.ServerRaum: Ausschließlich der Wahlvorstand hat Zutritt und Zugang zum Wahlserver. Dies ist notwendig, um ausschließen zu können, dass der EVG verändert oder gar ausgetauscht wird. Solche Angriffe können vom EVG weder verhindert noch erkannt werden.“

[36] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862b_pdf.pdf` (Stand: 23.08.2021)

[37] Inzwischen existiert eine Re-Zertifizierung. Im Folgenden geht es um das bis 2021 eingesetzte Zertifikat und das entsprechende Security Target. Die Re-Zertifizierung erfolgt für POLYAS Core 2.5.0, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862V2a_pdf.pdf` (Stand: 23.08.2021)

[38] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862a_pdf.pdf` (Stand: 23.08.2021)

[39] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862b_pdf.pdf` (Stand: 23.08.2021)

- „OE.AuthentizitätServer: Der Wähler sowie der Wahlvorstand überprüfen anhand des eingesetzten SSL-Zertifikates, ob sie mit dem richtigen serverseitigen EVG kommunizieren.“

Das BSI-Zertifikat[40] beinhaltet in Kapitel 4 (Gültigkeit des Zertifikats)eine Reihe von Auflagen: „Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des IT-Produktes. Das IT-Produkt ist nur unter den folgenden Bedingungen konform zu den bestätigten Vertrauenswürdigkeitskomponenten:

- Alle Auflagen hinsichtlich der Generierung, der Konfiguration und dem Einsatz des EVG, die in diesem Report gestellt werden, werden beachtet.
- Das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.“

Weitere relevante Inhalte des Zertifizierungsreports sind:

- „Der EVG enthält keine kryptographischen Mechanismen. Folglich waren solche Mechanismen nicht Gegenstand der Evaluierung.“
- „Der Anwender des Produktes muss die Ergebnisse dieser Zertifizierung in seinem Risikomanagementprozess berücksichtigen. Um die Fortentwicklung der Angriffsmethoden und -techniken zu berücksichtigen, sollte er ein Zeitintervall definieren, in dem eine Neubewertung des EVG erforderlich ist und vom Inhaber dieses Zertifikates verlangt wird.“
- „Stehen nicht zertifizierte Aktualisierungen oder Patches zur Verfügung, sollte er den Inhaber dieses Zertifikates auffordern, für diese eine Re-Zertifizierung bereitzustellen.“

Schließlich sind auch folgende Auflagen und Hinweise erwähnt:

- „Eine ungewöhnliche Häufung von Stimmabgaben innerhalb kurzer Zeit, insbesondere kurz vor Beendigung der Phase Wahldurchführung kann als Indiz für einen möglichen Sicherheitsvorfall (Kompromittierung der Datenbank des Urnen EVG) interpretiert werden. Der Wahlvorstand wird auf seine Verantwortung für die Feststellung und Bewertung einer solchen ungewöhnlichen Häufung von Stimmabgaben hingewiesen.“
- „Für den Fall, dass der Entwickler/Hersteller zusätzliche Funktionen für einzelne Schritte der Wahlvorbereitung in die umgebende WWW-Applikation integriert, wird dem Entwickler/Hersteller auferlegt, den Wahlveranstalter auf seine Verantwortung für die Erhaltung der Sicherheit, insbesondere den Schutz der Vertraulichkeit von TANs, Passwörtern und Schlüsseln hinzuweisen, und geeignete technisch-organisatorische Maßnahmen für die Wahrnehmung dieser Verantwortung anzubieten.“

7.2.3 Unterschiede in den (Re-)Zertifizierungs-Dokumenten

Eine Prüfung des Security Targets zu POLYAS *2.5.0* und der entsprechende Zertifizierungsbericht unterscheiden sich inhaltlich nicht bzgl. der zitierten Stellen aus dem ursprünglichen Security Target und der ursprünglichen Zertifizierung.

[40] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/Reporte08/0862a_pdf.pdf` (Stand: 23.08.2021)

7.3 Einordnung der Situation

7.3.1 Erstellung des Schutzprofils vor dem Wahlgeräte-Urteil

Das Wahlgeräte-Urteil[41] von 2009 diskutiert ausführlich den Grundsatz der Öffentlichkeit: „Die Öffentlichkeit der Wahl ist Grundvoraussetzung für eine demokratische politische Willensbildung. Sie sichert die Ordnungsgemäßheit und Nachvollziehbarkeit der Wahlvorgänge und schafft damit eine wesentliche Voraussetzung für begründetes Vertrauen der Bürger in den korrekten Ablauf der Wahl. Die Staatsform der parlamentarischen Demokratie, in der die Herrschaft des Volkes durch Wahlen mediatisiert, also nicht dauernd unmittelbar ausgeübt wird, verlangt, dass der Akt der Übertragung der staatlichen Verantwortung auf die Parlamentarier einer besonderen öffentlichen Kontrolle unterliegt. Die grundsätzlich gebotene Öffentlichkeit im Wahlverfahren umfasst das Wahlvorschlagsverfahren, die Wahlhandlung (in Bezug auf die Stimmabgabe durchbrochen durch das Wahlgeheimnis) und die Ermittlung des Wahlergebnisses (vgl. BVerfG, Urteil des Zweiten Senats vom 3. Juli 2008 - 2 BvC 1/07, 7/07 -, NVwZ 2008, S. 991 <992> m.w.N.).“

Das Schutzprofil BSI-CC-PP-0037-2008 'Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte' wurde im Jahre 2008 vom BSI zertifiziert. Entsprechend ist es nicht überraschend, dass weder die Umsetzung des Öffentlichkeitsgrundsatzes in diesem Schutzprofil gefordert wird, noch Anforderungen an die Umsetzung dieses Grundsatzes gestellt werden. Es ist offen, ob auch ein System, welches den Öffentlichkeitsgrundsatz mittels Ende-zu-Ende-Verifizierbarkeit umsetzt, nach diesem Schutzprofil positiv evaluiert und zertifiziert werden kann. Falls nicht, sei darauf hingewiesen, dass Online-Wahlprodukte grundsätzlich nach Common Criteria auch ohne Verweis auf ein Schutzprofil evaluiert und zertifiziert werden können.

Die Tatsache, dass der Öffentlichkeitsgrundsatz im Schutzprofil BSI-CC-PP-0037-2008 keine Rolle spielt, sollte bei der Entscheidung, ob es ausreicht, dass ein Produkt nach diesem Schutzprofil evaluiert und zertifiziert ist, berücksichtigt werden. Ggf. ist es sinnvoll bzw. sogar erforderlich, das Ende-zu-Ende-Verifizierbarkeit eingebaut ist. Hinsichtlich des Erforderlichseins sei darauf verweisen, dass das BSI inzwischen in seinem Dokument 'Anforderungen an Produkte für virtuelle Versammlungen und Abstimmungen'[42] Verifizierbarkeit in 4.3.2 als Anforderung an *geheime* Wahlen und Abstimmungen benennt. Ebenfalls wird die Anforderung nach Verifizierbarkeit vom BSI in der Technischen Richtlinie 'BSI TR-03162 IT-sicherheitstechnische Anforderungen zur Durchführung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a Fünftes Buch Sozialgesetzbuch (Online-Wahl)' (Fassung: 10.05.2021) genannt – siehe hierzu auch Kapitel 8.

7.3.2 Basis-Anforderung und Disclaimer

Das Schutzprofil trägt den Titel 'Basis-Anforderungen' und beinhaltet anders als andere Schutzprofile einen Disclaimer für den allgemeinen Einsatzbereich. Vermutlich dient beides dazu, klarzustellen, dass ein Online-Wahlprodukt, welches nach dem Schutzprofil zertifiziert ist, nicht ausreicht, um unbedenklich jegliche Arten von Wahlen durchzuführen. Konkret wird darauf hingewiesen, dass nur Wahlen mit geringem Angriffs-

[41] `https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html` (Stand: 23.08.2021)

[42] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Anforderungen_Produkte_Abstimmungen_Versammlungen.pdf;jsessionid=0F210BA19D36B5DB5721FADA0AD83BEE.internet471?__blob=publicationFile&v=5` (Stand: 23.08.2021)

potenzial mit dem Schutzprofil adressiert werden. Darüber hinaus ist zu beachten, dass die Evaluierungstiefe mit EAL2+ auf einer Skala von 1-7 eher am unteren Ende angesiedelt ist.

Entsprechend wird auch seitens des BSI in dem Zertifizierungsbericht darauf hingewiesen, dass beim Risikomanagementprozess die Ergebnisse aus dem Zertifizierungsreport der Wahlveranstalter berücksichtigt werden sollen. Durch die Tatsache, dass es sich hier um Basis-Anforderungen und eine eher niedrige Evaluierungstiefe handelt, ist es um so wichtiger, dem Rat des BSI zu folgen und die Dokumente zu berücksichtigen, um eine informierte Entscheidung hinsichtlich der Aussagekraft eines Zertifikats nach dem Schutzprofil BSI-CC-PP-0037-2008 treffen zu können.

Das Schutzprofil wird vom BSI nicht mehr für die Zertifizierungen neuer Online-Wahl-Produkte eingesetzt. Aus diesem Grund ist das Schutzprofil im Archiv-Bereich des BSI zu finden. Inwieweit dies damit zu tun hat, dass die dort formulierten Basis-Anforderungen nicht mehr ausreichend sind, müsste das BSI beantworten.

Es ist daher nicht ausreichend, dass das potenziell einzusetzende Online-Wahlsystem nach diesem Schutzprofil vom BSI zertifiziert ist. Wahlausrichter können nur eine informierte Entscheidung treffen, wenn sie unter Einbezug von Security Target und dem Zertifizierungsbericht ein Verständnis für die möglichen Bedrohungen entwickeln und sich dadurch der potenziellen Risiken im konkreten Anwendungsfall bewusst sind.

7.3.3 Gültigkeit des Zertifikats

Das BSI-Zertifikat bzw. die Aussagen im BSI-Zertifizierungsbericht gelten nur für die angegebene Version des IT-Produktes und nur unter den dort genannten Bedingungen.

Dies gilt für alle nach den Common Criteria zertifizierte IT-Produkte und entsprechend auch für POLYAS Core 2.2.3. Daher ist es aus unserer Sicht unerlässlich, das Security Target und den Zertifizierungsbericht zu lesen, um dann individuell zu entscheiden, ob die Auflagen erfüllt sind und, wenn nicht, das hierdurch entstehende Risiko transparent zu kommunizieren und zu diskutieren. Insbesondere, wenn Entscheidungen anderer Wahlausrichter für ein bestimmtes zertifiziertes Wahlsystem übernommen werden sollen, ist es wichtig, danach zu fragen, wie diese Bewertung dort ausgefallen ist. Nur so kann sichergestellt werden, dass diese auch auf die eigene Wahl übertragen werden kann.

Schließlich bestätigt das Zertifikat die Sicherheitseigenschaften des IT-Produktes nur zum Zeitpunkt der Ausstellung. Dies erfolgte im Fall von POLYAS 2.2.3 im Jahr 2016. Dadurch, dass die Informationssicherheit aber sehr dynamisch ist und Angriffsmethoden im Laufe der Zeit sich fortentwickeln, ist es erforderlich, die Widerstandsfähigkeit des IT-Produktes regelmäßig überprüfen zu lassen. Entsprechend gilt es auch zu diskutieren, inwieweit eine Re-Zertifizierung angefordert werden sollte. Im konkreten Fall wurde POLYAS Core 2.5.0 im Jahr 2021 re-zertifiziert. Nach den Empfehlungen des BSI ist davon auszugehen, dass im Rahmen dieses Prozesses Angriffsmethoden bei der Evaluation berücksichtigt wurden – so es relevante gab. Inwieweit es diese gab, kann das BSI beantworten. An dieser Stelle sei darauf verwiesen, dass auch Aktualisierungen oder Patches dazu führen, dass das Zertifikat seine Gültigkeit verliert. Entsprechend gilt es insbesondere dann, wenn eine Wahlordnung ein Zertifikat verlangen sollte, zu klären, ob wirklich das zertifizierte IT-Produkt eingesetzt wird. Insbesondere, wenn dies nicht der Fall ist, sollte dies vor der Wahl bekannt sein und diskutiert werden.

7.3.4 Sicherheitsziele für die Einsatzumgebung

Das Schutzprofil und auch das Security Target (sowohl für POLYAS 2.2.3 als auch für 2.5.0) beinhalten eine Reihe von Annahmen an die Einsatzumgebung und entsprechend auch eine lange Liste an Sicherheitszielen für die Einsatzumgebung. Für all diese gilt es im Rahmen der informierten Entscheidung zu prüfen, ob diese bei der eigenen Wahl erreicht werden. Im Folgenden diskutieren wir die Sicherheitsziele für die Einsatzumgebung, deren Erreichung wir für besonders herausfordernd halten.

Beispielsweise ist zu prüfen, ob die Annahme, dass das Endgerät vertrauenswürdig ist (OE.Endgerät), erfüllt ist. In Anbetracht der steigenden Zahl an infizierten Geräten insbesondere im privaten Kontext ist es wichtig – zwecks informierter Entscheidung – zu diskutieren, wie wahrscheinlich es ist, dass dieses Ziel erreicht ist – sowohl im Hinblick auf das Wahlgeheimnis als auch im Hinblick auf die unbemerkte Veränderung der Stimme vor dem Versenden. Mit Bezug auf OE.Wahlserver sollte im Rahmen der informierten Entscheidungsfindung diskutiert werden, inwieweit das Ziel erreicht werden kann, dass der Wahlvorstand die Wahlserver so absichert, dass ausgeschlossen werden kann, dass ein Netzwerkangreifer Zugriff auf den Server erhält. Ähnlich gelagert wäre die Frage, ob es möglich ist sicherzustellen, dass nur der Wahlvorstand Zugriff und Zugang zum Wahlserver hat (OE.ServerRaum). Zuletzt sei erwähnt, dass auch die Erkennung von anderen Angriffen bei den Wähler*innen und dem Wahlvorstand liegt (z. B. OE.AuthentizitätServer, 'ungewöhnliche Häufung von Stimmabgaben'/'Schutz der Vertraulichkeit von TANs, Passwörtern und Schlüsseln' aus dem Zertifikatsbericht) und entsprechend auch hier zu beurteilen ist, ob dies realistisch ist.

An dieser Stelle sei erneut erwähnt, dass die Sicherheitsziele für das IT-Produkt nur erfüllt sind, wenn die Sicherheitsziele für die Einsatzumgebung erfüllt sind. Wenn das nicht der Fall ist, ist die Gesamtsituation neu zu bewerten.

7.3.5 Eignung von CC Schutzprofilen für Wahlen im Allgemeinen

Mit Hinblick auf eine mögliche Weiterentwicklung des jetzigen Schutzprofils sei der Leser auf den Beitrag 'Tauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland' [4] verwiesen.

8 Technische Richtlinie für die Sozialversicherungswahlen

Um die Wahlbeteiligung bei Sozialwahlen zu erhöhen, ist für 2023 geplant, einen Online-Wahlkanal anzubieten. Zu dem Ergebnis, dass dies grundsätzlich möglich ist, gibt es eine rechtswissenschaftliche Auseinandersetzung von Spiecker und Bretthauer [11]. Eine Technische Richtlinie (TR) wurde vom BSI (Fassung: 10.05.2021) veröffentlicht unter dem Titel 'BSI TR-03162 IT-sicherheitstech-nische Anforderungen zur Durch-führung einer Online-Wahl im Rahmen des Modellprojekts nach § 194a Fünftes Buch Sozialgesetzbuch (Online-Wahl)'[43]. Diese beschreibt Anforderungen für den Betrieb und die Nutzung von Anwendungen und IT-Systemen.

Die Richtlinie geht an vielen Stellen über die Definition von Anforderungen hinaus und beschreibt einen Vorschlag für ein Internet-Wahlsystem (siehe z. B. Abbildung 2, Seite 12 TR, Abbildung 3, Seite 15 TR, und Abbildung 6, Seite 29 TR), inkl.

[43] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03162/BSI-TR-03162.pdf` (Stand: 23.08.2021)

der Infrastruktur, der beteiligten Stellen und deren Kommunikation. Sie spezifiziert darüber hinaus verschiedene Prozesse (z. B. den Prozess des Testens der Software des Wahlsystems), Techniken (z. B. zur Überprüfung der Integrität der Stimme) und behandelt weitere Themen wie die Wähler*innenauthentifizierung.

8.1 Auseinandersetzung mit dem Dokument

Die Richtlinie in ihrem jetzigen Zustand enthält eine Reihe von unterschiedlichen Problemen, die wir in den folgenden Abschnitten aufzeigen und diskutieren.

8.1.1 Beschreibung von Ansätzen zur Umsetzung

Eine Technische Richtlinie ist idealerweise systemneutral. Ungewöhnlicherweise werden in der Technischen Richtlinie auch Umsetzungsbeispiele gegeben. Allerdings stellt dies teilweise eine Überspezifikation dar (siehe z. B. Kapitel 8.2.4). Darüber hinaus können die Vorschläge nicht einfach kombiniert werden, ohne Sicherheitsanforderungen zu verletzen (siehe auch Kapitel 8.2.3).

8.1.2 Angreifermodell

Sicherheitsanforderungen können nie uneingeschränkt erfüllt sein. Daher ist es wichtig, sich über das Angreifermodell (siehe auch Kapitel 2.1) bewusst zu sein, d. h. zu verstehen, welche Annahmen gelten müssen, damit die Sicherheitsanforderungen gegeben sind. Die Technische Richtlinie empfiehlt die Durchführung von Risikobewertungen (Abschnitt 2.1.1.3, Seite 9 TR). Es werden jedoch keine weiteren Hinweise zur Bewertung dieser Risiken gegeben. Es wäre notwendig eine Bedrohungsanalyse durchzuführen und so zu prüfen, welche Angriffe das System abwehren kann und welche Annahmen notwendig sind. Diese Annahmen sind dann zu bewerten, d. h. die Frage, wie realistisch diese sind, gilt es zu beantworten.

Darüber hinaus erwähnt die Technische Richtlinie zwar mehrere Bedrohungen (z. B. „unberechtigte Stimmabgabe“, „Softwareentwicklung (Backdoors)“), stellt diese aber nicht in den Kontext der im Text beschriebenen Online-Wahl-systeme. Die Richtlinie erklärt auch nicht, wie die Risiken im Zusammenhang mit diesen Bedrohungen reduziert werden können.

Außerdem werden u. a. die folgenden Bedrohungen nicht explizit erwähnt:

- Dem Angreifer gelingt es, das Wahlsystem zu kompromittieren (z. B. als böswilliger Insider oder als externer Angreifer, dem es gelingt, unbefugten Zugriff auf das System bzw. die Server zu erhalten). In diesem Kontext sind u. a. folgende Angriffe auf die in der TR beschriebenen Online-Wahlsysteme möglich:
  - Das Wahlsystem kann im Namen von Wähler*innen, die nicht an der Online-Wahl teilgenommen haben, unter Verwendung ihrer Wahlkennzeichen (WKZ) Stimmen hinzufügen. Dieser Angriff wäre nur schwer zu erkennen, z. B. nur von genau diesen Wähler*innen, wenn es eine systemunabhängige Möglichkeit gibt zu prüfen, ob man laut Wählerverzeichnis gewählt hat oder nicht.
  - Das Wahlsystem kann die abgegebenen Stimmen verändern, ohne entdeckt zu werden. Dies wäre sowohl auf dem Gerät der wählenden Person als auch auf dem Online-Wahlsystem serverseitig möglich. Die Richtlinie

schlägt zwar einige Schutzmaßnahmen vor, die es Wahlausrichtern, Kandidat*innen und Wähler*innen nicht oder nur sehr eingeschränkt ermöglichen, Wahlmanipulationen zu entdecken. So wird z. B. die Verteilung von Tracking-Codes an die Wähler*innen (beschrieben in Abschnitt 5.2 der TR) vorgeschlagen. Diese Maßnahme ermöglicht sogenannte Clash-Attacken [9], siehe auch Kapitel 3).

  - Das Wahlsystem kann das Wahlgeheimnis brechen. Dies wäre auf dem Endgerät der wählenden Person möglich, wenn dort Wähler*innen sich mit der eigenen Identität ausweisen und über das gleiche Interface die Stimme abgeben. Darüber hinaus kann das Online-Wahlsystem serverseitig die Reihenfolge, in der die Wähler*innen ihre Stimme abgegeben haben, zusammen mit ihren Identifikationsinformationen speichern. Wenn die entschlüsselten Stimmen am Ende der Wahl veröffentlicht werden, um eine bessere Verifizierbarkeit zu gewährleisten (wie in 5.2 der TR vorgeschlagen), kann das Wahlsystem diese Informationen nutzen, um das Wahlgeheimnis zu verletzen.
  - Wenn das Wahlsystem die Liste der WKZ der Wähler, die ihre Stimme online abgegeben haben, an die Entität, die die Briefwahl abwickelt, weiterleiten soll, übermittelt ein Angreifer die WKZ von Wählern, die ihre Stimme nicht online abgegeben haben, und verhindert so, dass diese wählen können. Falls diese Wähler nämlich beschließen, ihre Stimme per Briefwahl abzugeben, werden diese Stimmen nicht gezählt, da davon ausgegangen wird, dass die Wähler ihre Stimme bereits online abgegeben haben.

- Dem Angreifer gelingt es, das Endgerät, mit dem die wählende Person ihre Stimme abgibt, zu kompromittieren und entweder die Stimme zu verändern, bevor sie an das Wahlsystem übertragen wird, oder das Wahlgeheimnis zu verletzen, indem er den Stimmabgabeprozess technisch beobachtet und / oder protokolliert.

Es gibt mehrere Möglichkeiten, diesen und weiteren Angriffen zu begegnen, z. B. durch die explizite Festlegung, dass das Wahlsystem vollständig vertrauenswürdig sein muss, um die Sicherheit der Wahl zu gewährleisten, oder durch die Implementierung von entsprechenden Schutzmaßnahmen (z. B. die Anwendung eines Mixnet Shuffle vor der Entschlüsselung der Stimmen oder die Implementierung von Maßnahmen zum Schutz vor einem potenziell nicht vertrauenswürdigen Wahlgerät, siehe z. B. die Internet-Wahl in der Schweiz [1] oder der Einsatz von Code-Voting [7]). In jedem Fall zeigen diese Angriffe jedoch, wie wichtig es ist, das Angreifermodell für die Wahl zu definieren, damit transparent ist, welche Bedrohungen durch das System abgewehrt werden und welche Annahmen notwendig sind, damit die Sicherheitsanforderung erfüllt sind. Dies stellt die Basis für die Risikobewertung dar.

8.1.3 Unpräzise oder inkorrekte Aussagen

Darüber hinaus enthält die Richtlinie mehrere Aussagen, die unpräzise oder irreführend sind. Im Folgenden diskutieren wir beispielhaft solche Aussagen:

Homomorphe Verschlüsselung Diese Methode zur Sicherstellung des Wahlgeheimnisses wird in der Richtlinie erwähnt und sie ist in der Tat in modernen Wahlsystemen weit verbreitet. Die Richtlinie macht jedoch mehrere irreführende bzw. widersprüchliche Aussagen im Kontext der Beschreibung dieser Methode:

- Die Richtlinie erwähnt 'homomorphe Verschlüsselung' ohne weitere Spezifikation. Es gibt zwar vollständig homomorphe Verschlüsselungen (z. B. Verschlüsselungsverfahren, die sowohl Addition als auch Multiplikation auf Ciphertexten ermöglichen und dieselben Operationen auf den verschlüsselten Klartexten beibehalten werden), aber sie sind derzeit nicht sehr effizient und werden daher in der Praxis selten eingesetzt. Insbesondere werden diese im Kontext von Online-Wahlen nicht eingesetzt. Entsprechend ist davon auszugehen, dass hier sogenannte semi-homomorphe Verschlüsselungen gemeint sind. Semi-homomorphe Verschlüsselung bedeutet, dass man z. B. die verschlüsselten Ciphertexte multipliziert und dadurch die verschlüsselte Summe der Klartexte erhält. Semi-homomorphe Verschlüsselungsverfahren sind in modernen Online-Wahlsystemen weit verbreitet.
- Die Richtlinie besagt, dass alle Stimmen vor der Auszählung entschlüsselt werden müssen (Seite 34 der TR, „Zur Ermittlung der Wahlergebnisse MÜSSEN die elektronischen Stimmen zuerst entschlüsselt werden."). Dies ist nicht der Fall, wenn die homomorphe Addition verwendet wird – ihr Hauptvorteil ist nämlich, dass es nicht notwendig ist, einzelne Stimmen zu entschlüsseln. Vielmehr genügt es, stattdessen die Summe aller abgegebenen Stimmen zu berechnen, diese Summe zu entschlüsseln und das so erhaltene Ergebnis zu veröffentlichen. Die Richtlinie erwähnt dies zwar später (Seite 34 TR, „Wird eine homomorphe Verschlüsselung genutzt, ermöglicht diese die Auszählung der Stimmen, ohne dass einzelne Stimmen entschlüsselt werden müssen."). Allerdings steht diese Aussage zu der vorherigen 'MÜSSEN'-Anforderung der TR im Widerspruch.
- Die Richtlinie besagt, dass der private Schlüssel der Online-Wahlleitung nach der Entschlüsselung der Stimmen veröffentlicht werden kann, um eine bessere Transparenz zu gewährleisten („Optional: privater Schlüssel zum Entschlüsseln wird zur Nachvollziehbarkeit nach Ermittlung des Wahlergebnisses veröffentlicht"). Ein solcher Ansatz könnte sehr gefährlich für das Wahlgeheimnis sein: Das Online-Wahlsystem kennt für jeden Wähler die verschlüsselte Stimme. Es kann den veröffentlichten privaten Schlüssel dann aber nach der Wahl auch nutzen, um jede einzelne Stimme zu entschlüsseln und so zu sehen, wer wie gewählt hat. Eine relativ einfache Möglichkeit, dieses Problem zu vermeiden und gleichzeitig die Verifizierbarkeit (d. h. die Möglichkeit, Manipulationen bei der Entschlüsselung und Auszählung zu erkennen) zu gewährleisten, ist die Verwendung von sogenannten Zero-Knowledge-Beweisen. Mit diesen kryptographischen Beweisen kann die Korrektheit der Entschlüsselung nachgewiesen werden, ohne den privaten Schlüssel zu veröffentlichen. Es handelt sich hierbei um eine Technik, die in modernen Online-Wahlsystemen weit verbreitet ist, aber in der Richtlinie nicht erwähnt wird. Mit weiteren bekannten Techniken wie Secret Sharing und/oder verteilter Schlüsselgenerierung kann man darüber hinaus vermeiden, dass einer einzelnen Person der Online-Wahlleitung vertraut werden muss. Diese Techniken sind erforderlich, um einen angemessenen Schutz des Wahlgeheimnisses zu erreichen.

Methoden zur Verifizierbarkeit Die Richtlinie widmet einen eigenen Abschnitt dem Thema Nachvollziehbarkeit, d. h. Funktionalität, die entweder die Wähler*innen oder Dritte anwenden können, um die Integrität des Wahlergebnisses zu verifizieren. Die drei genannten Ausprägungen (Seite 34/35 TR) sind genau genommen nicht nebeneinander zu sehen. Die drei genannten Aspekte sollten alle gleichzeitig adressiert

werden.

Die TR nennt beispielhaft technische Möglichkeiten zur Umsetzung dieser drei Aspekte (Seite 35 TR). Die Richtlinie geht nicht darauf ein, wie diese Techniken kombiniert werden sollten. Da die genannten unterschiedlichen Techniken verschiedene potenzielle Angriffspunkte adressieren, wäre eine Kombination dieser Techniken in der Tat erforderlich. Die genannten Techniken sind allerdings entweder technisch inkompatibel oder führen zu neuen Bedrohungen, die im Rahmen der Risikobewertung berücksichtigt werden müssten. Im Folgenden diskutieren wir beispielhaft Probleme mit den in der TR genannten Techniken:

1. „Nach Ende der Wahl kann eine Tabelle mit allen unverschlüsselten Stimmen auf einem Bulletin Board veröffentlicht werden, ohne dass hier eine Zuordnung durch die wählende Person zur eigenen Stimme möglich ist." – Hierbei wäre es notwendig, die Stimmen zu anonymisieren. Andernfalls wäre ein manipuliertes Online-Wahlsystem in der Lage, den Zeitstempel der abgegebenen Stimme oder die Reihenfolge, in der die Stimmen abgegeben wurden, mit den Identitäten der Wähler*innen zu verknüpfen und somit das Wahlgeheimnis zu verletzen. Wenn die verschlüsselten Stimmen zusammen mit den Signaturen veröffentlicht werden, siehe 2. und 4. dieser Auflistung, könnte sogar die Öffentlichkeit das Wahlgeheimnis für alle Wähler*innen brechen, wenn die Stimmen nicht zunächst anonymisiert werden. Um die Stimmen zu anonymisieren, kann ein verifizierbares Mixnetz verwendet [2] werden. Außerdem kann die Veröffentlichung aller Stimmen im Klartext zu sogenannten italienischen Angriffen führen [44][6].
2. „Nachdem die Online-Stimme verschlüsselt wurde und bevor diese in die elektronische Wahlurne übertragen wird, muss der wählenden Person der verschlüsselte Eintrag angezeigt werden, sodass dieser von der wählenden Person abgespeichert werden kann. Dazu muss die elektronische Wahlurne mit den verschlüsselten Online-Stimmen entweder während oder nach der Wahl an einer zentralen Stelle (Bulletin Board) veröffentlicht werden." – Wie im vorherigen Absatz beschrieben, müssen die Stimmen insbesondere dann anonymisiert werden, wenn die verschlüsselten Stimmen veröffentlicht werden und Wähler*innen zugeordnet werden können.
3. „Die elektronische Wählerstimme kann seitens des Browsers signiert werden. Anhand dieser Signatur kann nach Ende der Wahl geprüft werden, ob diese mit der abgegebenen Stimme richtig gespeichert wurde." – Zunächst ist festzustellen, dass in der TR nicht gesagt wird, was es bedeutet, dass seitens des Browsers signiert wird. Wir gehen zunächst davon aus, dass gemeint ist, dass die Stimme zunächst verschlüsselt und dann mit dem privaten Schlüssel der wählenden Person signiert wird. Dies ist durchaus in modernen Online-Wahlsystemen üblich. Die hier beschriebene technische Möglichkeit würde dann aber davon ausgehen, dass die Identität der wählenden Person für jede verschlüsselte Stimme mindestens dem Online-Wahlsystem bekannt ist. Das ist zwar an sich kein Problem, steht aber ggf. im Widerspruch zu der Anforderung aus der TR, dass die abgegebenen Stimmen nicht mit den Identitäten der Wähler*innen verknüpft werden

[44] Solche Angriffe werden eingesetzt, um Wähler*innen zu zwingen, ihre Stimme auf eine bestimmte Art und Weise abzugeben. Hierbei weist der Angreifer die wählende Person an, einen Stimmzettel abzugeben, der wahrscheinlich einzigartig ist (z. B. ein bestimmtes Muster von Stimmen in komplexen Stimmzetteln). Das Vorhandensein eines solchen Stimmzettels unter den ausgezählten Stimmen kann als Beweis dafür verwendet werden, dass die wählende Person die Anweisungen befolgt hat.

sollen: „Die elektronische Wählerstimme, welche an die Wahlurne übertragen wird, DARF NICHT Daten enthalten, welche Rückschlüsse auf die WKZ oder auf die Identität des Wahlberechtigten erlauben.“,

4. „Bevor die Online-Stimme in die elektronische Wahlurne übertragen wird, muss dieser eine einmalige Zufallszahl (zusammen mit dem Online-Stimmzettel generiert und angezeigt) zugeordnet werden. Diese Zufallszahl muss dem Wähler angezeigt werden, sodass er diese abspeichern kann. Am Ende der Wahl kann die elektronische Wahlurne mit den entschlüsselten Online-Stimmen und zugehörigen Zufallszahlen an einer zentralen Stelle (Bulletin Board) veröffentlicht wird.“. – Der Vorschlag spezifiziert nicht, wer die Zufallszahl (auch Tracking-Code genannt) wie generiert. Da diese der wählenden Person angezeigt wird, gehen wir davon aus, dass diese vom Online-Wahlsystem erzeugt wird. Dann schützt dieser Ansatz allerdings nicht vor den sogenannten Clash-Attacken [9]. Ein manipuliertes Online-Wahlsystem kann nämlich jeder wählenden Person, die für Kandidat A gestimmt hat, dieselbe Zahl geben, aber nur eine dieser Stimmen in der Wahlurne speichern; als Ergebnis würde jede wählende Person glauben, dass ihre Stimme für A gezählt wurde, da er sie neben der ihm zugewiesenen Zahl finden kann, jedoch wird nur eine Stimme für A in die Auszählung aufgenommen. Die anderen für A abgegebenen Stimmen können unbemerkt verändert werden (siehe auch Kapitel 3). Dieses Problem kann bis zu einem gewissen Grad vermieden werden, wenn die wählende Person auch eine Zufallszahl angeben soll. Dies birgt die Herausforderung, dass zum Schutz des Wahlgeheimnisses sichergestellt werden muss, dass Wähler keine Zahlen verwenden, die sie identifizieren, z. B. ihr Geburtsdatum.

8.1.4 Detaillierungsgrad variiert

Die Richtlinie ist in ihrem Detaillierungsgrad etwas uneinheitlich, was es erschwert, die Zielgruppe, die die Richtlinie adressiert, einzuschätzen. So bewegen sich einige Vorschläge auf einem sehr abstrakten Niveau, während andere sehr detailliert beschrieben sind.

Nicht spezifisch genug Die Richtlinie macht nur sehr begrenzte Angaben zu den vom System erfassten Daten. Insbesondere werden an mehreren Stellen Daten aufgeführt, die ‘mindestens’ protokolliert werden müssen, siehe z. B. Abschnitt 2.4 der TR. Die Richtlinie geht jedoch nicht auf datenschutzrechtliche Aspekte ein. Insbesondere das Konzept der Datenminimierung und der Datenschutz-Folgenabschätzung (s. Art. 35 DSGVO[45] (Stand: 23.08.2021)), das im Idealfall dazu führen sollte, dass die Entwickler und Administratoren des Wahlsystems sorgfältig abwägen, welche Daten für die spezifizierten Funktionen (z. B. Überwachung von unberechtigten Zugriffen) tatsächlich notwendig sind und welche Daten nicht erhoben werden sollten. Darüber hinaus werden Fragen des Schutzes personenbezogener Daten (dazu gehört auch die Überlegung, welche der gesammelten Daten tatsächlich als personenbezogene Daten angesehen werden können) nicht erwähnt. Weitere datenschutzrechtliche Fragen ergeben sich bei der Betrachtung der personenbezogenen Daten der Wähler*innen, auf die der Online-Dienstleister Zugriff hat. All diese Themen werden nicht diskutiert.

Weitere Beispiele der Richtlinie, die einer genaueren Erläuterung bedürfen, sind:

[45] https://dsgvo-gesetz.de/art-35-dsgvo/

- Was sind die 'Prüf- und Ergebnisprotokolle', die während der Wahl erstellt werden müssen (Seite 16 TR)?
- Was ist mit 'doppelter Entschlüsselung' gemeint („Mit privatem Schlüssel der Wahlleitung [Optional: doppelt entschlüsseln]“, Seite 18 TR)?
- Was sollte in den Wahlunterlagen enthalten sein, die den Wähler*innen zugesandt werden, insbesondere in Bezug auf Anweisungen zum Schutz ihrer PCs vor Cyberangriffen (Seite 24 TR)? Während die Richtlinie erwähnt, dass die notwendigen Informationen auf den BSI-Webseiten zu finden sind, ist unklar, welche Inhalte ausgewählt werden müssen (die Richtlinie gibt einige Beispiele an, wobei jedoch unklar ist, ob die Aufzählung als erschöpfend zu verstehen ist), in welcher Form diese Inhalte für die Wähler*innen aufbereitet werden müssen (z. B. als gedrucktes Material oder als Link zur Webseite), und was zu tun ist, wenn die Inhalte geändert werden.

Überspezifiziert Die Richtlinie beschreibt einige der Mechanismen sehr detailliert, sodass sich die Frage stellt, ob die vorgeschlagenen Techniken immer so verwendet werden sollten, wie sie beschrieben sind, oder ob Anpassungen vorgenommen werden können und das Online-Wahlsystem dennoch TR-konform sein kann. Die folgenden Beispiele veranschaulichen überspezifizierte Passagen:

- Die Richtlinie schlägt vor, die elektronische Wahlurne getrennt vom Wählerverzeichnis zu speichern („Die elektronische Wahlurne MUSS getrennt vom Wählerverzeichnis Online und der WKZ-Liste Online Stimmabgabe gespeichert werden.“). Diese Methode ist zwar an sich nicht unbedingt problematisch, entspricht aber nicht dem Stand der Technik, bei dem die abgegebenen verschlüsselten Stimmen zusammen mit der entsprechenden Identität der wählenden Person (entweder personenidentifizierend oder pseudonymisiert) gespeichert werden.

  Durch diese Anforderungen werden viele Techniken zur Umsetzung der Verifizierbarkeit (d. h. Techniken, die es der wählenden Person ermöglichen zu überprüfen, ob ihre Stimme tatsächlich als abgegebene Stimme registriert wurde, und es Dritten ermöglichen, zu überprüfen, ob alle abgegebenen Stimmen legitimen Wähler*innen zugeordnet werden können und nicht vom System hinzugefügt wurden) ausgeschlossen. Außerdem würde das Fehlen der Verbindung zwischen der wählenden Person und der abgegebenen verschlüsselten Stimme keine Aktualisierung der Stimme ermöglichen (sogenanntes Vote-Updating, wie dies z.B. im estnischen System möglich ist). Gleichzeitig ist das Vote-Updating eine einfache Technik, um Stimmenkauf und Wahlzwang zu adressieren.
- Die Richtlinie besagt ebenfalls, dass die Identitäten der Wähler*innen an das Online-Wahlsystem übertragen werden müssen („Das WVO und die WKZ werden innerhalb des Informationsverbundes Krankenkasse erstellt und müssen in das Online-Wahlsystem (Informationsverbund Online-Wahl) übertragen werden.“, Seite 13 TR). Insbesondere vor dem Hintergrund der bereits diskutierten datenschutzrechtlichen Problematik stellt sich die Frage, warum nicht stattdessen Pseudonyme verwendet werden können, sodass die Erhebung personenbezogener Daten im Auftrag des Wahlsystemanbieters minimiert wird. In diesem Fall müsste die Authentifizierung durch die Krankenkassen erfolgen (und nicht, wie in der Richtlinie vorgeschlagen, vollständig an den Wahlsystemanbieter delegiert werden). Denkbar ist, dass dies für die Krankenkassen nicht umsetzbar ist. Dennoch sollte die Option diskutiert werden.

Nicht adressiert Darüber hinaus werden mehrere Themen, die für die Durchführung von Online-Wahlen relevant sind, nicht erwähnt. Hierzu zählen u. a. folgende Themen:

- Benutzbarkeit und Barrierefreiheit: Diese beiden Eigenschaften sind entscheidend, um sicherzustellen, dass die Wähler*innen in der Lage sind, das vorgeschlagene System zu benutzen. Darüber hinaus wirkt sich ein Mangel an Benutzbarkeit negativ auf die Sicherheit aus, wenn z. B. die Verifizierungsverfahren zu komplex sind, sodass weder Wähler*innen noch Dritte die notwendigen Prüfungen durchführen können, um sicherzustellen, dass die Wahl nicht manipuliert wird.
- Verschiedene Sonderfälle, die auftreten können und entsprechend adressiert werden sollten, werden in der TR nicht behandelt, z. B.:
  - Was ist, wenn Wähler*innen behaupten, ihre Wahlunterlagen seien nicht angekommen? Sollen neue generiert werden (inkl. evtl. Generierung eines neuen WKZ)? Falls diese Materialien Zugangsdaten der wählenden Person enthielten, sollten diese Zugangsdaten ungültig gemacht werden?
  - Was ist, wenn die wählende Person behauptet, dass sie die Integrität ihrer abgegebenen Stimme nicht überprüfen kann (z. B. wenn sie ihren Tracking-Code nicht finden kann oder wenn die Stimme neben diesem Code nicht übereinstimmt)? Gibt es eine Möglichkeit, ihre Behauptung zu validieren? Gibt es eine Möglichkeit für die wählende Person, Unregelmäßigkeiten zu melden, ohne ihr eigenes Wahlgeheimnis zu brechen? Dies führt zum Problem der Rechenschaftspflichtigkeit (Accountability) [8].

8.2 Empfehlung

Die Idee, eine Richtlinie für die Durchführung von Online-Wahlen vorzuschlagen, ist zeitgemäß und wertvoll. In Anbetracht der oben dargelegten Probleme empfehlen wir jedoch eine Aktualisierung der Richtlinie, die u. a. die oben genannten Anmerkungen präzisiert und weitere Verweise auf wissenschaftliche Publikationen und Berichte zu unterschiedlichen Ansätzen und bekannten Sicherheitsproblemen aufnimmt.

9 Fazit

Abschließend möchten wir zunächst einige Fragen auflisten, die vor der Einführung von Online-Wahlen beantwortet werden sollten:

- Unter welchem Angreifermodell und unter welchen Annahmen an das Benutzer*innenverhalten erfüllt das System die Wahlrechtsgrundsätze? Muss den Endgeräten (sprich z. B. Smartphones oder Laptops), von denen aus die Stimme abgegeben wird, vertraut werden – oder können diese unbemerkt die Stimme verändern und das Wahlgeheimnis brechen? Wie realistisch sind derartige Manipulationen im konkreten Fall (als Basis für Risikobewertung)? Kann das Risiko durch organisatorische Maßnahmen reduziert werden?
- Können Manipulationen durch Cyberangriffe, Betreiber und Wahlausrichter zuverlässig erkannt werden oder muss darauf vertraut werden, dass alle ehrlich sind und Cyberangriffe nicht durchgeführt werden?

- Worauf beruhen die Informationen zu den Sicherheitseigenschaften und dem Angreifermodell bzw. den Annahmen?
- Welche Aussagen zur Sicherheit werden im Zertifizierungsbericht von wem auf welcher Grundlage getroffen? Wie sind die dort genannten Auflagen zu bewerten? Wie genau wird die Erfüllung der Sicherheitsanforderungen evaluiert?

Abschließend sei darauf hingewiesen, dass viele Forschungsergebnisse zur Sicherheit von Online-Wahlen existieren. Diese Forschung umfasst u. a. zahlreiche kryptographische Wahlprotokolle zur Gestaltung verschiedener Wahlformen sowie zur Benutzbarkeit der Verifizierungstechniken. Darüber hinaus setzen andere Länder wie die Schweiz und Estland bereits verifizierbare Online-Wahlsysteme ein.

Literatur

[1] Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) (July 1st 2018). `https://www.fedlex.admin.ch/eli/cc/2013/859/de`, 2018.

[2] Stephanie Bayer and Jens Groth. Efficient Zero-Knowledge Argument for Correctness of a Shuffle. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 263–280. Springer, 2012.

[3] Bernhard Beckert, Achim Brelle, Rüdiger Grimm, Nicolas Huber, Michael Kirsten, Ralf Küsters, Jörn Müller-Quade, Maximilian Noppel, Kai Reinhard, Jonas Schwab, Rebecca Schwerdt, Tomasz Truderung, Melanie Volkamer, and Cornelia Winter. GI Elections with POLYAS: a Road to End-to-End Verifiable Elections. In *Fourth International Joint Conference on Electronic Voting (E-Vote-ID 2019), 1-4 October 2019, Lochau / Bregenz, Austria - Proceedings. Ed.: M. Volkamer; B. Beckert*, page 293–294. Gesellschaft für Informatik (GI), 2019.

[4] Johannes Buchmann, Stephan Neumann, and Melanie Volkamer. Tauglichkeit von Common Criteria-Schutzprofilen für Internetwahlen in Deutschland. *Datenschutz und Datensicherheit*, 38(2):98–102, 2014.

[5] Jurlind Budurushi, Stephan Neumann, Genc Shala, and Melanie Volkamer. Entwicklung eines Common Criteria Schutzprofils für elektronische Wahlgeräte mit Paper Audit Trail. In Eric Schneider Erhard Plödereder, Lars Grunske and Dominik Ull, editors, *INF14 - Workshop: Elektronische Wahlen: Unterstützung der Wahlprozesse mittels Technik*, volume 232 of *Lecture Notes in Informatics (LNI)*, pages 1415–1426. Gesellschaft für Informatik e.V. (GI), Köllen Druck+Verlag GmbH, Bonn, September 2014.

[6] Roberto Di Cosmo. On Privacy and Anonymity in Electronic and Non-Electronic Voting: the Ballot-As-Signature Attack. 2007.

[7] Jörg Helbach and Jörg Schwenk. Secure Internet Voting with Code Sheets. In *International Conference on E-Voting and Identity*, pages 166–177. Springer, 2007.

[8] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Accountability: Definition and Relationship to Verifiability. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS 2010)*, pages 526–535. ACM Press, 2010.

[9] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Clash Attacks on the Verifiability of E-Voting Systems. In *2012 IEEE Symposium on Security and Privacy*, pages 395–409. IEEE, 2012.

[10] Andreas Mayer. Virtuelle Hauptversammlungen: Ein sicherer Ersatz für Präsenzveranstaltungen? In *Deutschland. Digital. Sicher. – 30 Jahre BSI*, Tagungsband zum 17. Deutschen IT-Sicherheitskongress, pages 233–248, Ingelheim, February 2021. Secumedia Verlags GmbH.

[11] Indra Spiecker and Sebastian Bretthauer. Die rechtliche Zulässigkeit einer Online-Wahl zur Sozialwahl. `https://www.vdek.com/magazin/ausgaben/2019-04/onlinewahl_rechtlichezulaessigkeit.html` (Stand: 23.08.2021), 2019.