WHITEPAPER

Status Quo & Ausblick: Sicherheit bei POLYAS Online-Wahlen

POLYAS

Abstract

Die Corona-Pandemie und die dadurch beschleunigte Digitalisierung hat dazu geführt, dass elektronische Wahlen und Abstimmungen in den vergangenen Jahren stark zugenommen haben. Viele Abstimmungen auf Hauptversammlungen und Parteitagen, auf denen weitreichende Entscheidungen getroffen werden, finden inzwischen digital statt. Das Wahlgeheimnis darf dabei nicht verletzt werden, während gleichzeitig eine Manipulation am Wahlergebnis ausgeschlossen werden muss. Die fünf Wahlgrundsätze – nach denen Wahlen allgemein, unmittelbar, frei, gleich und geheim sein sollten, müssen stets eingehalten werden – unabhängig davon, ob die Stimmabgabe in Person, über den Postweg oder digital stattfindet.

POLYAS ist sich bewusst, dass es Kund:innen nicht ausreicht, allein auf die Integrität eines Online-Wahl-Anbieters zu vertrauen. Manipulationen müssen durch die Architektur des eingesetzten Systems ausgeschlossen werden können, die Stimmabgabe muss nachvollziehbar und überprüfbar sein, so wie auch das Wahlergebnis. In der IT-Welt spricht man von einer sogenannten “Ende-zu-Ende-Verifikation”. Um diese zu realisieren, hat POLYAS die Wahlsoftware CORE 3.0 entwickelt.

Im Folgenden soll unter Berücksichtigung verschiedenster Angriffsszenarien veranschaulicht werden, wie die Software funktioniert. Darüber hinaus wird unter Berücksichtigung aktueller wissenschaftlicher Erkenntnisse ein Ausblick auf die Trends – insbesondere in Hinblick auf die zusätzliche Sicherheit – bei Online-Wahlen gegeben.

Inhaltsverzeichnis

1 Einleitung

Die Corona-Pandemie hat viele Veränderungen mit sich gebracht. Einer der wichtigsten Nebeneffekte ist, dass die Digitalisierung der Arbeitswelt beschleunigt wurde. Das Arbeiten im Home Office hat stark zugenommen, Meetings und Veranstaltungen finden nun immer häufiger als Videokonferenz oder im hybriden Format statt. Und so ist auch der Bedarf an digitalen Abstimmungen und Wahlen deutlich gestiegen. Während in anderen Ländern bereits seit vielen Jahren wichtige Wahlen online durchgeführt werden (z. B. die Online-Parlamentswahl in Estland), wird nun auch der Ruf in Deutschland nach digitalen Stimmabgaben lauter. Fast zwei Drittel aller Deutschen sprechen sich laut einer repräsentativen BITKOM-Umfrage aus dem September 2021 dafür aus, dass künftig auch bei der Bundestagswahl digital abgestimmt werden kann[1]. Auch die Sozialwahl 2023, bei der die Sozialparlamente der Krankenkassen gewählt werden, wird digital stattfinden.[2]

Obwohl für den Einsatz von parlamentarischen Online-Wahlen noch ein weiter Weg vor uns liegt, sind die Vorteile nicht von der Hand zu weisen: Digitale Wahlen bieten Flexibilität, können zu einer höheren Wahlbeteiligung führen und haben darüber hinaus weitere Vorzüge wie etwa die Einsparung von Kosten. Auch der CO2-Verbrauch kann reduziert werden, wenn auf den postalischen Versand von Briefwahlunterlagen verzichtet wird.

Als Anbieter von Online-Wahlen ist POLYAS seit mehr als zwei Jahrzehnten Teil der zunehmenden Verbreitung digitaler Wahlsysteme. Im Sommer 1996 wurden die ersten Wahlen mit einer POLYAS-Software durchgeführt, die anschließend im Softwarehaus Micromata (bekannt z. B. durch das DHL-Tracking-Portal und die Online-Frankierung) weiterentwickelt wurde. 2012 erfolgte die Ausgründung des Unternehmens, und die POLYAS GmbH entstand. Mit unseren Systemen wählen zahlreiche Organisationen wie Kirchen, Vereine, Hochschulen, Kammern, Unternehmen, Verwertungsgesellschaften (z. B. Gema, VG Wort) und Parteien. Bedingt durch die Corona-Pandemie entschied sich auch die CDU, im Januar 2021 ihren ersten rein digitalen Bundesparteitag auszurichten. Die Wahl des neuen Parteivorsitzenden wurde dabei mit dem POLYAS Live Voting durchgeführt.

Online-Wahlen müssen eine besondere Herausforderung meistern, da das Wahlgeheimnis gewahrt und gleichzeitig Manipulation – durch Mechanismen zur Überprüfung der Wahl – ausgeschlossen werden muss. Die Server, auf denen das Online-Wahlsystem gehostet wird, müssen daher höchsten Sicherheitsansprüchen genügen, und selbstredend sollte nach dem durch die europäische Datenschutz-Grundverordnung (EU-DSGVO) vorgegebenen Prinzip der Datensparsamkeit gearbeitet werden. Aber das allein reicht nicht aus.

Auf der einen Seite muss die Architektur des Online-Wahlsystems selbst so gestaltet sein, dass eine Überprüfbarkeit ermöglicht wird – sowohl für den:die einzelne:n Wähler:in als auch für die Wahlleitung. In wissenschaftlichen Fachkreisen spricht man von Eligibilitäts-, individueller und universeller Verifikation, die man unter dem Schlagwort Ende-zu-Ende-Verifikation zusammenfast. Mit der individuellen

[1] Quelle: https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-sprechen-sich-fuer-Online-Wahlen-aus, letzter Abruf am 09.02.2022
[2] Quelle: https://www.soziale-selbstverwaltung.de/aktuelles-aus-der-selbstverwaltung/online-sozialwahlen-2023-ersatzkassen-stellen-sich-der-digitalen-herausforderung, letzter Abruf am 09.02.2022

Verifikation wird die korrekte Stimmabgabe (durch die wählende Person) überprüft. Die universelle Überprüfung aller Abläufe auf dem Wahlserver erfolgt durch die Wahlleitung. Und die Eligibilitäts-Verifikation (vom Englischen *eligibility verifiability = Wahlfähigkeit)* stellt sicher, dass ausschließlich Wahlberechtigte Stimmen zur Urne hinzufügen konnten. Mit dieser Methode wird die Stimmabgabe nachvollziehbar – eine Forderung an elektronische Wahlsysteme, die 2009 vom Bundesverfassungsgericht in einem Urteil zum Einsatz von Wahl-Computern formuliert wurde.[3] Neben der Ende-zu-Ende-Verifikation sind auch die Verteilung einzelner Komponenten des Online-Wahlsystems auf dritte Parteien, die Verwendung von Open-Source-Tools und Bulletin-Boards sowie der Einsatz kryptografischer Verfahren (z. B. der sogenannte Zero-Knowledge-Proof) essenzieller Bestandteil eines sicheren Online-Wahlsystems.

Auf der anderen Seite muss das System gegen unterschiedlichste Angriffsszenarien gewappnet sein. Um potenzielle Sicherheitslücken zu antizipieren, muss sich bei der Konstruktion des Online-Wahlsystems in die Situation möglicher Angreifer hineingedacht werden.

Für die Wahl des neuen Parteivorsitzenden der CDU im Januar 2021 kam beispielsweise der POLYAS CORE 3.0 zum Einsatz – eine Plattform, die unter Berücksichtigung der oben beschriebenen Anforderungen an eine Online-Wahlsoftware entwickelt wurde und stetig weiterentwickelt wird.

Im Folgenden soll die Funktionsweise des CORE 3.0 beschrieben werden. POLYAS verfügt noch über eine weitere, ältere Online-Wahlsoftware, den CORE 2.5. Dieser wurde erstmals 2016 nach dem internationale Common Criteria Schutzprofil BSI-CC-PP-0037-2008[4] vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. Im Sommer 2021 erfolgte die Rezertifizierung. Das Schutzprofil aus dem Jahr 2008 deckt den Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte ab. Eine Ende-zu-Ende-Verifikation ist jedoch nicht Teil der im Profil formulierten Anforderungen. Dies war einer der wesentlichen Gründe für die Entwicklung des CORE 3.0. Bisher gibt es kein aktuelleres Schutzprofil auf internationaler oder nationaler Ebene, es gibt jedoch in Fachkreisen bereits erste Gespräche dazu. Sobald ein Schutzprofil vorhanden sein sollte, wird sich POLYAS auch danach zertifizieren lassen.[5]

[3] Quelle: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-019.html, letzter Abruf 09.02.2022
[4] Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0037b_pdf.pdf?__blob=publicationFile&v=1, letzter Abruf am 09.02.2022
[5] Das BSI arbeitet bereits ein der Erstellung eines neuen Schutzprofils. Näheres dazu siehe S. 23

2 Aufbau des POLYAS CORE 3.0 Verifiable

2.1 Die drei Varianten des CORE 3.0

Bei POLYAS kommen unterschiedliche Varianten des CORE 3.0 zum Einsatz, denn nicht alle Wahlen haben das gleiche hohe Angriffspotenzial. Es handelt sich um den CORE 3.0 Base, den CORE 3.0 Live Voting sowie den CORE 3.0 Verifiable.
Bei Vereinswahlen etwa eignet sich der **CORE 3.0 Base**, der zwar nicht über individuelle Verifikation via Second-Device oder universelle Verifikation verfügt, aber so wie der CORE 3.0 Verifiable über eine Ende-zu-Ende-Verschlüsselung - von der Stimmabgabe bis zur Auszählung bleibt der Stimmzettel verschlüsselt.

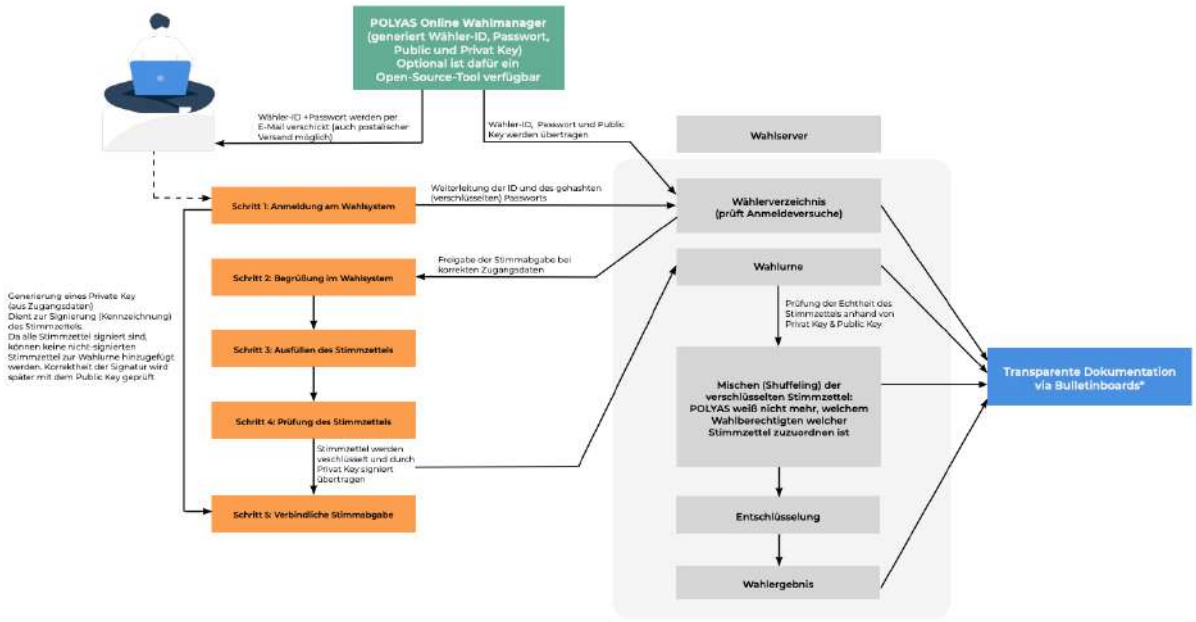

Abbildung 1: Schaubild CORE 3.0 Base

Auch werden die Vorgänge im Online-Wahlsystem wie im Fall des **CORE 3.0 Verifiable** ebenfalls auf Bulletin-Boards[6] dokumentiert.

[6] Näheres zu den Bulletin Boards siehe S. 15ff

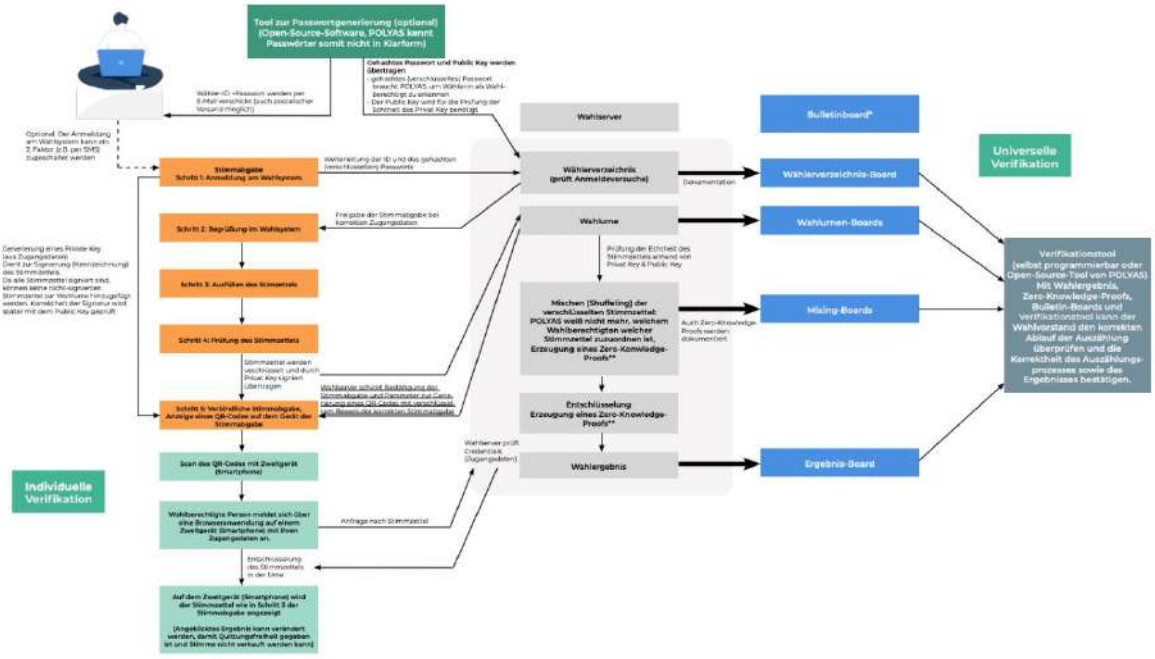

Abbildung 2: Schaubild CORE 3.0 Verifiable

Der **CORE 3.0 Live Voting** wird bei Abstimmungen auf Veranstaltungen eingesetzt. Die Anforderung an diesen CORE ist neben Sicherheit daher auch Schnelligkeit. Der CORE 3.0 Live Voting verfügt über eine Methode zur individuellen Verifikation, die allerdings nicht – wie im Fall des **CORE 3.0 Verifiable** – über einen Second Device (Zweitgerät, z. B. ein Smartphone) erfolgt. Stattdessen setzt POLYAS auf sogenannte Verifikations-Codes, bei denen den Stimmberechtigen nach ihrer Stimmabgabe ein Code angezeigt wird, den sie mit einer öffentlichen Liste abgleichen können, in der dem jeweiligen Code eine Wahlentscheidung zugeordnet ist.

Bei dieser Methode muss man – anders als bei der Verifikation via Second Device – darauf vertrauen, dass das Wahlgerät eindeutige (tatsächlich zufällige) Tracking-Codes generiert. Sobald dies geschehen ist und der Stimmzettel abgegeben wurde, können jedoch etwaige Manipulationen durch einen Abgleich des Inhalts mit der Wahlurne nach dem Auszählungsprozess erkannt werden. Das heißt, wenn der Stimmzettel aus der Auszählung entfernt oder verändert wird, kann der Wähler dies feststellen. Der CORE 3.0 Verifiable genügt höchsten Sicherheitsansprüchen und soll im Folgenden erläutert werden.

3 Passwortgenerierung und Anmeldung

3.1 Beschreibung

3.1.1 Wähler-ID und Passwortgenerierung

Die Anmeldung am POLYAS Online-Wahlsystem erfolgt standardmäßig über Wähler-ID und Passwort. Die Wähler-ID kann beispielsweise aus der E-Mail-Adresse der wahlberechtigten Person bestehen. Für eine datensparsame und

besonders sichere Wahl ist es aber genauso gut möglich, auf eine pseudonymisierte Wähler-ID zu setzen, bei der jeder wahlberechtigten Person vom Wahlveranstalter eine Zahlenfolge zugwiesen wird. So verbleiben die Klarnamen beim Wahlveranstalter.

Für die sicherste Variante der Passwortgenerierung kann sich der Wahlveranstalter für den Einsatz eines Open-Source-Tools zur Passwortgenerierung entscheiden. Das Tool wird nicht von POLYAS gehostet oder eingesetzt, sondern von einer dritten Partei. Die durch den Wahlveranstalter bestimmte Instanz generiert mit Hilfe des Open-Source-Tools die Passwörter für die Wahlberechtigten. Hierbei entstehen zwei Dateien:

- Eine Datei, welche die unverschlüsselten Passwörter der Wahlberechtigten enthält. Die Passwörter werden an die Wahlberechtigten verschickt. Das Passwort hat zwei Funktionen: Zum einen dient es als Anmeldekennwort im klassischen Sinne, das heißt: zur Autorisierung der wählenden Person am Wahlsystem. Zum anderen dient es als Private Key, um den Stimmzettel im Browser des Wahlberechtigten zu signieren. Sowohl Anmeldekennwort als auch Private Key werden vom ursprünglich generierten Passwort abgeleitet.
- Eine Datei, welche die gehashten (verschlüsselten) Passwörter für den Upload im POLYAS Online-Wahlsystem enthält. Zusätzlich beinhaltet die Datei die sogenannten Public Keys der Wahlberechtigten, welche später für die Verifikation des Wahlergebnisses genutzt werden. Mit diesen wird geprüft, ob die im Browser generierten Private Keys (Signaturen), die aus dem Passwort der Wahlberechtigten abgeleitet werden, korrekt waren und der Stimmzettel von der Person stammt, von der er stammen sollte.

3.1.2 Zwei-Faktor- Authentifizierung

Das Login vor der Stimmabgabe kann durch eine Zwei-Faktor-Authentifizierung zusätzlich abgesichert werden. Das bedeutet: Eine wahlberechtigte Person meldet sich mit Benutzername und Passwort an und erhält dann – wahlweise per SMS oder E-Mail – ein zeitlich begrenzt gültiges Passwort (den zweiten Faktor), mit dem sich der:die Wahlberechtigte anschließend für die Stimmabgabe anmelden kann.

3.1.3 Login zur Stimmabgabe

Loggt sich nun ein:e Wahlberechtigte:r mit seinem:ihrem Passwort und seiner:ihrer Wähler-ID im Online-Wahlsystem ein, werden ID und Passwort an das POLYAS Online-Wahlsystem weitergeleitet. Ist eine Zwei-Faktor-Authentifizierung vorgeschaltet, muss die wahlberechtigte Person zuvor noch das Passwort eingeben, das sie über den zweiten Faktor erhalten hat. Das POLYAS Online-Wahlsystem prüft auch dieses Passwort. Ist alles korrekt, wird der wahlberechtigten Person der bzw. die Stimmzettel angezeigt, die für sie bestimmt sind. Dies wird anhand der Wähler-ID erkannt.

3.2 Beispiele für Angriffsszenarien

3.2.1 Manipulation durch an der Wahlvorbereitung beteiligte Parteien

Szenario: Eine der Parteien, die für die Erstellung der Zugangsdaten zuständig ist, wird erpresst und gezwungen, die Zugangsdaten zur Wahl (Wähler-ID und Passwort) herauszugeben.

Lösung: Durch die Verteilung der Verantwortung bei der Erstellung der Zugangsdaten (Separation-of-Duty-Prinzip) kennt keine der beteiligten Parteien sowohl Passwort als auch die zugehörige Wähler-ID.

Der Wahlveranstalter kennt die Wähler-ID und weiß, welche Person mit der ID verknüpft ist und welche Stimmzettel sie sehen darf. Das Passwort kennt der Wahlveranstalter nicht, da dieses von einer dritten Partei generiert wird. Die dritte Partei, die das Passwort generiert, kennt die Wähler-IDs nicht.

Sofern die Unterlagen per Brief verschickt werden: Der Druckdienstleister kennt nur das Passwort in Klarform, nicht aber die Wähler-IDs.

POLYAS als Wahldienstleister erhält die Wähler-IDs vom Wahlveranstalter, die Passwörter liegen POLYAS aber nur in verschlüsselter Form vor.

3.2.2 Daten-Leak von Wähler-ID und Passwort

Szenario: Eine nicht-autorisierte Person gelangt in Besitz von Wähler-ID und Passwort einer wahlberechtigten Person.

Lösung: Selbst, wenn es einer nicht-autorisierten Partei gelänge, sowohl in den Besitz der Wähler-ID als auch des Passworts einer wahlberechtigten Person zu gelangen, müsste diese zusätzlich Zugriff auf den zweiten Faktor der angegriffenen Person (etwa deren Mobiltelefon) erhalten. Dadurch wird die Hürde für einen erfolgreichen Angriff erheblich erhöht.

3.2.3 Brute-Force-Angriffe

Szenario: Bei einem Brute-Force-Angriff handelt es sich um den Versuch, ein Passwort oder einen Benutzernamen per Trial-and-Error-Methode zu knacken.

Lösung: Die Brute-Force-Methode zur Erlangung von Passwörtern einer wahlberechtigen Person wird bei POLYAS unterbunden, indem Passwörter mit hoher Entropie (Informationsdichte) generiert und verwendet werden. Dies bedeutet schlicht, dass die Passwörter lang genug sind, um die Trial-and-Error-Methode

eines Brute-Force-Angriffes unwirksam zu machen. Der Schutz vor Brute-Force-Angriffen wird im Rahmen regelmäßiger Pentests überprüft[7].

4 Stimmabgabe

4.1 Beschreibung

Nach dem erfolgreichen Login einer wahlberechtigten Person wird in deren Client (Browser) aus dem Passwort ein Private Key generiert, welcher dazu dient, den Stimmzettel im Rahmen der finalen Stimmabgabe zu signieren. Die Signatur, die nur im CORE 3.0 Verifiable verwendet wird, ist notwendig, damit die Wahlurne erkennt, dass der eingehende Stimmzettel korrekt ist und von einer wahlberechtigten Person abgegeben wurde. Der:die Wählende füllt nun den digitalen Stimmzettel aus, kann die Auswahl noch einmal überprüfen und gibt die Stimme schließlich verbindlich ab.

Nicht nur das Signieren, auch das Verschlüsseln des Stimmzettels erfolgt clientseitig auf dem Gerät bzw. im Browser der wählenden Person mit dem sogenannten Election Public Key. Der Stimmzettel wird nur verschlüsselt und signiert transportiert und kommt auch nur verschlüsselt in der POLYAS Wahlurne an. Die Verschlüsselung im CORE 3.0 Verifiable erfolgt über die sogenannte ElGamal-Methode, während im CORE 3.0 BASE und im CORE 3.0 Live Voting das sogenannte Elliptic Curve Integrated Encryption Scheme (ECIES) genutzt wird. Der Transport der abgegebenen Stimmzettel erfolgt ausschließlich über eine TLS-Verbindung via Server-Zertifikat der D-Trust GmbH, einem Unternehmen der Bundesdruckerei-Gruppe. Erst nach dem Durchmischen der verschlüsselten Stimmzettel in der digitalen Wahlurne werden die Stimmzettel entschlüsselt.

Die Wahlberechtigten können ihre Stimme nur dann in die digitale Wahlurne legen, wenn ihre digitalen Stimmzettel korrekt signiert sind, also mit einem passenden Private Key versehen sind. Auf diesem Weg wird die Verifikation der Eligibilität (nur Wahlberechtigte können Stimmen zur Urne hinzufügen) gewährleistet. Zudem können die Signaturen auch im Zuge der universellen Verifikation mit den von dem Wahlveranstalter bestimmten Auditor:innen überprüft werden.

4.2 Beispiele für Angriffsszenarien

4.2.1 Ballot-Stuffing

Szenario: Unter Ballot Stuffing versteht man das Hinzufügen von Stimmen zur Wahlurne durch unbefugte Parteien. Wie bereits unter Punkt 3.2.1 erklärt, kann keine Partei, die an der Erstellung der Zugangsdaten beteilig ist, ungehindert Stimmzettel ausfüllen und zur Wahlurne hinzufügen. Was aber, wenn eine Partei versucht, der Wahlurne zusätzliche Stimmzettel hinzuzufügen?

[7] Mehr zu den Pentests siehe S. 20

Lösung: In der Wahlurne werden ausschließlich verschlüsselte Stimmzettel abgelegt, welche durch autorisierte Wahlberechtigte abgegeben wurden. Um zu verhindern, dass POLYAS oder eine andere unbefugte Partei Stimmzettel zur Wahlurne hinzufügen kann, wird jeder Stimmzettel durch den Private Key signiert, der von dem Passwort der:des Wahlberechtigten abgeleitet wurde.

Die Signatur des Stimmzettels wird während der Abgabe zunächst durch den Wahlserver überprüft, um sicherzustellen, dass der Stimmzettel durch eine wahlberechtigte Person abgegeben wurde. Dazu wird der Private Key, den POLYAS nicht kennt, mit dem Public Key abgeglichen. Die Public Keys erhält POLYAS, wie oben beschrieben, von jener Partei, die die Passwörter für die Stimmabgabe generiert. POLYAS oder eine andere Partei kann selbst keine Stimmzettel zum System hinzufügen, da dazu ein korrekt signierter Stimmzettel erzeugt werden müsste. Ein Stimmzettel, welcher nicht mit einem gültigen Private Key signiert ist, wird spätestens während der universellen Verifikation nach der Wahl von den Auditor:innen erkannt.

4.2.2 Manipulierter Stimmzettel

Szenario: Einem:r Angreifer:in gelingt es, den Browser einer wahlberechtigten Person so zu manipulieren, dass im Stimmzettel eine Wahlentscheidung gespeichert wird, die von dem:der Wähler:in nicht gewünscht war.

Lösung: Die wahlberechtigte Person kann nach der verbindlichen Stimmabgabe eine individuelle Verifikation mit einem Zweitgerät (z. B. einem Smartphone) vornehmen. Hier wird der wahlberechtigten Person ein Abbild ihres Stimmzettels angezeigt, der nun in der Wahlurne liegt. Sollte ein Angreifer den Stimmzettel manipuliert haben, würde die:der Wähler:in dies nun erkennen und könnte den Wahlveranstalter informieren. Wie genau die individuelle Verifikation funktioniert, wird in Kapitel 6 erklärt.

5 Wahlserver

Der Wahlserver ist das Kernelement des POLYAS Online-Wahlsystems CORE 3.0 Verifiable. Jeder eingehende Stimmzettel durchläuft einen ausgefeilten Prozess über verschiedene Instanzen des Wahlservers, an dessen Ende das Wahlergebnis einsehbar wird.

5.1 Beschreibung

5.1.1 Wählerverzeichnis

Das Wählerverzeichnis wird standardmäßig von POLYAS betrieben. Beim Wählerverzeichnis handelt es sich um ein Bulletin Board[8]. Das Wählerverzeichnis enthält keine Klartext-Zugangsdaten der Wahlberechtigten, sondern nur gehashte

[8] Näheres zu den Bulletin Boards siehe S. 15ff

(verschlüsselte) Werte. Die Daten (Wähler-ID, gehashtes Passwort, der Public Key zur Verifizierung des im Browser generierten Private Key und ggf. Informationen zur Wählergruppe), welche auf dem Wählerverzeichnisboard liegen, werden durch den Wahlveranstalter oder POLYAS im Online-Wahl-Manager – dem Tool, mit dem digitale Wahlprojekte bei POLYAS erstellt werden – hochgeladen und gepflegt. Das Wählerverzeichnis überprüft, ob Wähler-ID, Signatur durch den Private Key und Passwort korrekt sind, und ob der:die Wähler:in die Stimme noch nicht abgegeben hat. Außerdem gibt es den oder die Stimmzettel für die wahlberechtigte Person zur Abstimmung frei.

5.1.2 Wahlurne

Die Wahlurne wird durch POLYAS betrieben. Auch die digitale Wahlurne ist ein Bulletin Board. Hier werden die Stimmzettel abgelegt, bevor sie im nächsten Schritt mit Hilfe von sogenannten Mixnets durchmischt werden. Die Stimmzettel liegen nur verschlüsselt in der Wahlurne.

Bevor die Stimmzettel in die Wahlurne übertragen werden, prüft der Wahlserver, ob der Stimmzettel von einer wahlberechtigten Person stammt - also ob die Signatur durch den Private Key auf dem Stimmzettel mit dem Public Key der:des Wahlberechtigten übereinstimmt. Ist dies nicht der Fall, wird der Stimmzettel zurückgewiesen. War die Stimmabgabe erfolgreich, sendet der Wahlserver der:dem Wählenden eine Bestätigung über die erfolgreiche Stimmabgabe zurück.

Sobald die Wahlberechtigten ihre Stimme verbindlich abgegeben haben, werden sie im Wählerverzeichnis markiert und können sich nicht erneut zur Stimmabgabe anmelden.

5.1.3 Mixing-Prozess/Shuffling

POLYAS kennt nach dem Eingang der verschlüsselten Stimmzettel in die Wahlurne deren Inhalt nicht, weiß durch die Signatur aber, welcher Stimmzettel welcher wahlberechtigten Person zuzuordnen ist. Um das Wahlgeheimnis einzuhalten, werden die Stimmzettel nun in einem Mixing-Prozess durchmischt.

Dies erfolgt in verschiedenen Paketen: Bei einer gewissen Anzahl von eingegangenen Stimmzetteln wird ein Paket gebildet, das nach kryptografischen Shuffling-Methoden durchmischt wird. Die Anzahl berechnet sich aus der Anzahl (K) der Einträge im Wählerverzeichnis-Board. Liegen dementsprechend K Stimmzettel auf dem digitalen Wahlurnen Board, werden diese in Pakete verpackt und auf das Bulletin-Board verschoben, das die fertigen Stimmzettelpakete für das Shuffling enthält. Von dort aus werden sie gemischt. Nach dem Mischen werden die Stimmzettel erneut auf einem Bulletin Board abgelegt, bevor die Entschlüsselung und Auszählung der Stimmzettel erfolgt.

Die beim POLYAS CORE 3.0 Verifiable eingesetzte Shuffling-Methode wird als *Wikström Shuffle* bezeichnet, während beim POLYAS CORE 3.0 Base die *ONION-Shuffle*-Methode zum Einsatz kommt. Nur die *Wikström Shuffle*-Methode ist verifizierbar. Das Mischen der Stimmzettel nach diesem Verfahren erzeugt einen Zero-

Knowledge-Proof, mit welchem die Korrektheit der Operation mathematisch bewiesen werden kann, ohne das (Wahl-)Geheimnis zu verraten. Die Zero-Knowledge-Proofs werden für die universelle Verifikation des Wahlergebnisses benötigt und werden in Kapitel 7.3 erklärt. Wenn es bei einer Wahl Wählergruppen gibt, wird der Prozess des Mischens und Entschlüsselns für jede Wählergruppe einzeln durchgeführt.

5.1.4 Entschlüsselung der Stimmzettel

Standardmäßig besitzt POLYAS den Schlüssel und führt die Entschlüsselung der Stimmzettel. Der Plan von POLYAS ist es, dass der Schlüssel in naher Zukunft mit anderen Parteien geteilt werden kann. Die nach der ElGamal-Methode verschlüsselten Stimmzettel können dann nur entschlüsselt werden, wenn die anderen Parteien an der Entschlüsselung teilnehmen. Im Fall des CORE 3.0 Verifiable erzeugt auch das Entschlüsseln der Stimmzettel einen Zero-Knowledge-Proof.

5.1.5 Wahlergebnis

Auf dem Wahlergebnis-Board werden nach der Wahl die individuellen, entschlüsselten Stimmzettel veröffentlicht. Danach werden die Wahlergebnisse mit Hilfe eines Auszählungsmoduls ausgezählt und aggregiert, sodass sie für die Wahlleitung lesbar sind.

5.2 Angriffsszenario

5.2.1 Verrat des Wahlgeheimnisses

Szenario: Der Wahlanbieter (POLYAS) wird erpresst und soll die Wahlentscheidung eines prominenten Wählers verraten.

Lösung: Wenn der Schlüssel für die Entschlüsselung der Stimmzettel mit mehreren Parteien geteilt wird, kann eine einzelne Partei die Stimmzettel nicht in Klarform einsehen. Bei einem pseudonymisierten Wählerverzeichnis kennt POLYAS zudem die Klarnamen der Wahlberechtigten nicht.

5.2.2 Manipulation des Wahlergebnisses

Szenario: Der Wahlanbieter (POLYAS) wird erpresst und soll ein manipuliertes Wahlergebnis veröffentlichen.

Lösung: Um die Korrektheit aller Prozesse auf dem Wahlserver und des Wahlergebnisses nachzuweise, setzt POLYAS auf individuelle und universelle Verifikation sowie auf den Einsatz von Bulletin-Boards und Zero-Knowledge-Proofs. Mehr dazu lesen Sie in den nachfolgenden Kapiteln.

6 Individuelle Verifikation

6.1 Beschreibung

6.1.1 Überprüfung via Zweitgerät

Damit die Wahlberechtigten nach der Stimmabgabe überprüfen können, ob sich ihr korrekt ausgefüllter Stimmzettel in der digitalen Wahlurne befindet, nutzt POLYAS eine Überprüfungsmethode mittels einer Anwendung auf einem Zweitgerät. Diese Anwendung zur Überprüfung des Stimmzettels direkt nach Stimmabgabe wird durch POLYAS bereitgestellt und auch betrieben. Es besteht jedoch auch die Möglichkeit zur Nutzung einer Anwendung, die durch den Wahlveranstalter oder eine dritte Partei bereitgestellt und/oder betrieben wird.

Mit der individuellen Verifikation werden zwei Prinzipien beim Durchführen digitaler Wahlen eingehalten: *Cast as intended* und *Stored as cast*. *Cast as intended* bedeutet, dass der abgegebene, verschlüsselte Stimmzettel der wählenden Person bestimmte Wahlentscheidung enthält. Dies kann mit der Verifikation via Zweitgerät (Second Device, z. B. ein Smartphone) überprüft werden. *Stored as cast* bedeutet, dass die:der Wähler:in nachvollziehen kann, dass die Stimmzettel korrekt in der Urne gespeichert und nicht entfernt oder dort geändert wurden. Um dies sicherzustellen, erhält die wählende Person während der Verifikation eine Art Quittung (Receipt) über den abgegebenen Stimmzettel, mit dem die eigene Stimmabgabe aber nicht gegenüber Dritten bewiesen werden kann. Die individuelle Verifikation ist wesentlicher Bestandteil der Ende-zu-Ende-Verifikation.

6.1.2 Funktionsweise aus Sicht der Wählenden

Die Wahlurne schickt dem:der Wählenden eine signierte, maschinenlesbare Bestätigung über die Annahme der Stimmabgabe (Receipt). Die:der Wählende sieht auf dem Gerät, auf welchem die Stimme abgegeben wurde, einen QR-Code. Dieser enthält einen Teil des verschlüsselten Nachweises dafür, dass die entsprechende Stimme korrekt in der Wahlurne abgelegt wurde. Der zweite Teil des Nachweises wird vom Wahlserver unter Verwendung eines Zero-Knowlegde-Proofs bereitgestellt. Nur mit der Kombination dieser beiden Teilnachweise kann auf dem Zweitgerät (z. B. einem Mobiltelefon) der Klartext entschlüsselt werden.

Dazu scannt die stimmberechtigte Person den QR-Code mit ihrem Zweitgerät und authentifiziert sich anschließend über eine Web-App erneut am POLYAS Online-Wahlsystem. Hierfür gibt sie erneut Wähler-ID und Passwort ein. Nach erfolgreicher Authentifizierung in der Web-App wird nun der Nachweis über die Stimmabgabe entschlüsselt und der stimmberechtigten Person wird ein Abbild ihres Stimmzettels, der sich in der Wahlurne befindet, als lesbarer Klartext angezeigt.

Damit der angezeigte Stimmzettel nicht als Quittung für einen Stimmenkauf verwendet werden kann, ist dieser in der Ansicht in der Web-App veränderbar. Nachträgliche Änderungen haben jedoch keinen Einfluss auf den tatsächlich abgegebenen Stimmzettel in der Wahlurne.

6.2 Beispiele für Angriffsszenarien

6.2.1 Manipulation des Beweises durch den Wahlanbieter

Szenario: Der Wahlanbieter (POLYAS) wird erpresst und soll den Wahlberechtigten ihre Stimmzettel anzeigen, aber manipulierte Stimmzettel in der Urne ablegen.

Lösung: Die Web-App zur Verifikation des eigenen Stimmzettels kann von einem externen Anbieter gehostet und betrieben werden. Damit kann verhindert werden, dass der Wahlanbieter an der Anzeige des Stimmzettels Manipulationen vornimmt.

6.2.2 Ausschluss von Stimmenkauf

Szenario: Ein Angreifer versucht die individuelle Verifikation zu nutzen, um damit Stimmen von Wahlberechtigten zu kaufen.

Lösung: Die Wahlberechtigten haben keine Möglichkeit, ihre Stimmabgabe gegenüber Dritten zu beweisen, da das Abbild des Stimmzettels, der ihnen in der Web-App ihres Zweitgeräts angezeigt wird, veränderbar ist. Ein Screenshot der Anzeige wäre also kein Beweis der eigenen Stimmabgabe. Damit wäre der Versuch, die Stimme zu verkaufen, sinnlos.

7 Bulletin Boards und Zero-Knowledge-Proof

7.1 Beschreibung der Bulletin Boards

7.1.1 Bulletin Boards als fälschungssichere Protokolle

Um die Vorgänge bei der Durchführung einer Online-Wahl sicher zu dokumentieren und den Transfer von Daten sowie deren Verarbeitung transparent zu machen, nutzt POLYAS sogenannte Bulletin Boards. Diese digitalen Protokolle können nicht unbemerkt verändert werden und dienen als Basis für das universelle Verifikationsverfahren.

Ein Bulletin Board ist eine Art Datenbank-Tabelle, in der jedes Mal ein Hashwert angelegt wird, wenn ein neuer Eintrag erfolgt. Dazu wird aus dem vorherigen Hashwert und der neuen Information ein neuer Hashwert gebildet, sodass die Einträge auf dem Bulletin Board wie in einer Kette miteinander verzahnt werden. Sowohl die Informationen, die auf dem Bulletin Board abgelegt werden als auch der Hashwert, der über den Inhalt des Boards gebildet wird, werden signiert. Durch das Bilden immer neuer Hashwerte und das Signieren der Hashes und der Informationen auf dem Bulletin Board wird sichergestellt, dass zwar neue Inhalte hinzugefügt werden können, aber bestehende Inhalte nicht unbemerkt veränderbar oder löschbar sind. Sobald ein Bulletin Board versiegelt ist, können diesem keine neuen Informationen hinzugefügt werden.

7.1.1.1 Exkurs: Vergleich von Bulletin Boards und Blockchain

Immer wieder sorgte der Kurs der Kryptowährung Bitcoin in den letzten Jahren für Schlagzeilen. Dass Menschen bereit sind, in eine rein virtuelle Währung zu investieren, liegt an der Verschlüsselungstechnologie Blockchain. Sie garantiert, dass jede Krypto-Münze nur einmal existiert und der Besitz durch ein digitales Protokoll unstrittig ist. POLYAS nutzt mit den Bulletin Boards einer der Blockchain eng verwandte Technologie. Beide basieren auf demselben Mechanismus und haben eine fälschungssichere Dokumentation zum Ziel. Denn bei den Kryptografie-Methoden handelt es sich im Grunde um digitale Protokolle, deren einzelne Abschnitte durch mathematische Verfahren wie die Glieder einer Kette miteinander verzahnt sind. Die Einträge in diese Datenbank können daher nicht nachträglich geändert werden.

Der wesentliche Unterschied zwischen der Blockchain und den von POLYAS genutzten Bulletin Boards ist, dass die Blockchain dezentral (also auf einer Vielzahl von Servern) gehostet wird, während die Bulletin Boards zentraler gespeichert werden und ihr Inhalt den Auditor:innen nach der Wahl zur Verfügung gestellt wird. Bulletin Boards sind damit energieschonender, flexibel einsetzbar, schneller oder mit einem Wort: skalierbar. Skalierbarkeit bedeutet in der IT-Welt die Fähigkeit eines Systems zu wachsen, also einer steigenden Datenmenge Platz zu bieten, was insbesondere bei großen Wahlen und Abstimmungen gewährleistet werden muss.

7.2 Art der Bulletin Boards im POLYAS CORE 3.0 Verifiable

Bei einer Wahl mit dem POLYAS CORE 3.0 Verifiable kommen sieben verschiedene Bulletin Boards zum Einsatz. Jeder Schritt bzw. jede Instanz, die ein Stimmzettel durchläuft, wird von einem anderen Bulletin Board dokumentiert.

7.2.1 Wählerverzeichnis-Board

Die Daten auf dem Wählerverzeichnis-Board werden über den POLYAS Online-Wahlmanager (Wähler-ID, Wählergruppen etc.) bzw. durch das Passwort-Tool (Public Keys der Wahlberechtigten) generiert. Über das Wählerverzeichnis-Board lässt sich sicherstellen, dass die Zugangsdaten der Wahlberechtigten korrekt und integer erzeugt und auf dem Board abgelegt wurden. Sobald die Wahl im POLYAS Online-Wahlmanager versiegelt wird, lassen sich auch die Einträge auf dem Wählerverzeichnis-Board nicht mehr ändern.

7.2.2 Wahlschlüssel-Board

Der Wahlschlüssel dient zur Entschlüsselung der Stimmzettel und wird gemeinsam mit dem dazugehörigen Zero-Knowledge-Proof nach der ElGamal-Methode

generiert. Er wird auf dem Wahlschlüssel-Board noch vor der Wahl während des Initialisierungsprozesses abgelegt.

7.2.3 Wahlurnen-Boards

Die Stimmzettel werden, wie oben beschrieben, clientseitig verschlüsselt – also auf den Geräten der Wählenden – und dann in der Wahlurne abgelegt. Der Wahlserver gibt ausschließlich Stimmzettel an die Wahlurne weiter, die korrekt verschlüsselt und signiert sind und auch nur dann, wenn die wählende Person ihre Stimme noch nicht abgegeben hat.

Inkorrekte Stimmzettel hingegen werden nie an die Wahlurne weitergeleitet. Um Transparenz zu schaffen, hat POLYAS einen Vorbereitungsprozess für die Stimmzettel etabliert. Im Rahmen dieses Prozesses werden nicht korrekte Stimmzettel zunächst markiert und danach aussortiert. Die Wahlurne besteht somit aus zwei Boards: Auf dem einen werden alle korrekt signierten Stimmzettel abgelegt, auf dem anderen landen Stimmzettel, die nicht korrekt signiert worden sind.

Das Wahlurnen-Board wird versiegelt, wenn die Zeit der Stimmabgabe abgelaufen ist.

7.2.4 Mixing-Board

Die Stimmzettel werden, wie oben beschrieben, in Pakete einer festgelegten, sinnvollen Größe eingeteilt und innerhalb dieser Pakete durchgemischt. Die Größe richtet sich nach der Anzahl der Wahlberechtigten, die im Wählerverzeichnis-Board eingetragen sind. Das Mixing-Board enthält die zu mischenden Pakete, welche vom Wahlurnen-Board als korrekt weitergeleitet wurden und die Zero-Knowledge-Proofs[9], die die korrekt erfolgte Durchmischung beweisen.

7.2.5 Entschlüsselungs-Board

Die durchmischten Pakete werden nun entschlüsselt. Hierbei wird ebenfalls ein Zero-Knowledge-Proof erzeugt, welcher beweist, dass die Entschlüsselung korrekt durchgeführt wurde. Der Wahlschlüssel bleibt geheim.

Der POLYAS CORE 3.0 Verifiable überprüft standardmäßig alle System-Subkomponenten auf deren Korrektheit. Zur Wahrung des Wahlgeheimnisses erfolgt der Entschlüsselungsprozess erst dann, wenn alle vorherigen Prozesse auf den restlichen Bulletin Boards verifiziert wurden. Der Schlüssel zur Entschlüsselung der Stimmzettel wird also erst dann genutzt, wenn sichergestellt ist, dass der Ciphertext, der als Grundlage der Entschlüsselung dient, korrekt ist.

[9] Näheres zu den Zero-Knowledge-Proofs siehe S. 18

7.2.6 Ergebnis-Board

Das Ergebnis-Board enthält die individuellen, entschlüsselten Stimmzettel.

7.3 Beschreibung der Zero-Knowledge-Proofs

Beim Zero-Knowledge-Proof (auch als Zero-Knowledge-Protokoll bekannt) handelt es sich um ein kryptografisches Beweissystem, das einer Partei erlaubt, die anderen Parteien davon zu überzeugen, mit hoher Wahrscheinlichkeit ein Geheimnis zu kennen, ohne dieses dabei zu verraten. Bei POLYAS wird der Zero-Knowledge-Proof dafür genutzt, die universelle Verifikation zu ermöglichen. Sie werden beim Mischen und Entschlüsseln der verschlüsselten Stimmzettel erzeugt.

Mit den Zero-Knowledge-Proofs soll bewiesen werden, dass der gesamte Auszählungsprozess (Übernahme des Inhalts der Wahlurne und anschließendes Mischen und Entschlüsseln) korrekt durchgeführt wurde, und weder durch POLYAS noch durch externe Quellen Änderungen vorgenommen wurden. Also muss die Integrität der Urne bewiesen werden, ohne dass ihr Inhalt zu verraten wird.

Die Bedingungen des Verfahrens sind:

- Die Keys bleiben geheim und der Prozess bleibt unberührt
- Alle Klartexte in den verschlüsselten Stimmzetteln sind nach dem Mixen unverändert vorhanden
- Eine Zuordnung von Eingangsstimmzetteln zu Ausgangsstimmzetteln ist nicht mehr möglich

8 Universelle Verifikation

8.1 Beschreibung

Im Folgenden soll veranschaulicht werden, wie Bulletin Boards und Zero-Knowledge-Proofs zur universellen Verifikation genutzt werden.

Der Wahlveranstalter erhält von POLYAS ein sogenanntes Verifikations-Tool. Auch bei dieser Verifikation setzt POLYAS also auf das Prinzip *Separation of Duty*, also der Aufteilung von Verantwortung bei sicherheitsrelevanten Elementen der Online-Wahl. Das Tool kann von dem Wahlveranstalter selbständig installiert und ausgeführt werden, um die Wahlergebnisse nachzuvollziehen. Mit der Verifikation wird außerdem das von der internationalen Forschung formulierte Prinzip *Tallied as cast* eingehalten: Der:die Wähler:in kann nachvollziehen, dass alle Stimmen korrekt zum Wahlergebnis zusammengerechnet wurden. Die universelle Verifikation ist wesentlicher Bestandteil der Ende-zu-Ende-Verifikation.

Nach dem Ende der Auszählung erhält der Wahlveranstalter von POLYAS die Inhalte der öffentlichen Bulletin Boards, welche wiederum das Wahlergebnis, also

den Inhalt der Wahlurne (Stand bei Wahlende), sowie die Ergebnisse aller Zwischenschritte (inklusive der Zero-Knowledge-Proofs) enthalten.

Mit diesen Dateien sowie dem Verifikations-Tool kann der Wahlvorstand den korrekten Ablauf der Auszählung überprüfen sowie die Korrektheit des Auszählungsprozesses (und so auch des Ergebnisses, sofern die Inhalte der Stimmzettel korrekt sind) bestätigen.

Das Ziel des Verifikationsprozesses ist es, die Inhalte aller Bulletin Boards auf ihre korrekte Erzeugung hin zu überprüfen. Auf den Boards passiert dabei Folgendes:

- **Wählerverzeichnis-Board:** Dieses enthält die Liste der öffentlichen Zugangsdaten (Public Keys & Wähler-IDs) der Wahlberechtigten und kann von dem Wahlveranstalter nachträglich überprüft werden.
- **Wahlschlüssel-Board:** Die Verifikation besteht hierbei darin, zu überprüfen, ob der Zero-Knowledge-Proof, der die Richtigkeit des Wahlschlüssels beweist, korrekt durchgeführt wurde.
- **Wahlurnen-Board:** Das Verifikations-Tool prüft nach der Wahl, ob alle in der Wahlurne enthaltenen Stimmzettel korrekt erstellt und signiert wurden.
- **Mixing-Board:** Während der Verifikation wird anhand des beim Mixing entstandenen Zero-Knowledge-Proof überprüft, ob die Erzeugung der Pakete korrekt durchgeführt wurde.
- **Ergebnis-Board:** Dieses Board enthält alle legitim abgegebenen Stimmzettel sowie die Zero-Knowledge-Proofs der korrekten Entschlüsselung der Stimmzettel.

Die finale Auszählung der Wahlergebnisse erfolgt nur anhand des Ergebnis-Boards. Die Überprüfung dieses Schrittes besteht darin, die Wahlergebnisse auf der Basis des binären Codes nachzuzählen, um sicherzustellen, dass das zuvor festgestellte Ergebnis korrekt ist.

8.2 Beispiel für Angriffsszenarien

8.2.1 Manipulation der Verifikation durch Wahlanbieter

Szenario: Der Wahlanbieter (POLYAS) wird erpresst und soll die universelle Verifikation so manipulieren, dass sie als korrekt erscheint.

Lösung: Das Tool zur Verifikation wird von einer externen Stelle gehostet. Damit kann verhindert werden, dass der Wahlanbieter im Falle einer Erpressung die Anzeige des Stimmzettels manipuliert.

9 Generelle Sicherheitsmaßnahmen bei POLYAS

9.1 Penetrationstest

POLYAS führt mindestens einmal jährlich einen Penetrationstest, kurz Pentest, mit externen Prüfpartnern durch. Mit diesem Test wird im IT-Bereich die Sicherheit eines digitalen Systems geprüft. Die Tester gehen wie Angreifer vor und versuchen, in das System einzudringen. Auf diese Weise sollen die Schwachstellen in der IT-Infrastruktur ausfindig gemacht und schließlich beseitigt werden.

Bei POLYAS werden in einem mehrere Tage währenden Zeitraum alle sicherheitsrelevanten Komponenten in verschiedenen Nutzungsszenarien und User-Rollen überprüft. Die Prüfer testen alle Komponenten des Online-Wahlsystems sowie des Online-Wahlmanagers. Auf diese Weise können eventuelle Schwachstellen und Fehler des Systems schnell erkannt und beseitigt werden. Zuletzt[10] wurde POLYAS im Januar 2022 von der T-Systems überprüft, einer Tochterfirma der Telekom AG. Dabei konnten keine relevanten Schwachstellen entdeckt werden.

9.2 Hosting auf der Open Telekom Cloud

Auf Wunsch hostet POLYAS das Online-Wahlsystem auf den mehrfach zertifizierten Servern der Open Telekom Cloud (OTC). Für alle POLYAS Kund:innen mit gebuchtem Election Management ist das Hosting in Deutschland standardmäßig inklusive. Die Open Telekom Cloud wird von der T-Systems, einem Tochterunternehmen der Deutschen Telekom AG, in Deutschland betrieben. Die OTC bietet einen besonderen Schutz vor sogenannten DDoS-Attacken, bei der mit einer Vielzahl von automatisierten Anfragen an einen Server versucht wird, diesen abstürzen zu lassen. Der Zutritt zu den Servern, auf denen Ihre Daten gespeichert werden, ist gemäß ISO27001 nur befugten Personen möglich.

Darüber hinaus verfügt die OTC über zahlreiche Zertifikate[11], die eine datenschutzkonforme Verarbeitung und die Sicherheit der Datenspeicherung belegen:

- 27017 Zertifikat über Datensicherheitsmanagement (Dekra)
- ISO 27018 Zertifikat über Datenschutz-Management (Dekra)
- CSA STAR Zertifizierungsprogramm für Security Management System (TÜV)
- Geprüfter Cloud Service nach Anforderungskatalog „TÜV Trusted Cloud Se vice“ (TÜV)
- ISO 27001 Zertifikat über Informationssicherheitssystem (Dekra)
- ISO 20000 Zertifikat über Servicemanagementsystem (Dekra)
- ISO 9001 Zertifikat über Qualitätsmanagementsystem (Dekra)
- ISO 22301 Zertifikat über Business Continuity Management System (Dekra)
- ISO 14001 Zertifikat über Umweltmanagementsystem (Dekra)
- TCDP Version 1.0 Zertifikat über Datenschutzanforderung für die Auftragsdatenverarbeitung (Dekra)

[10] Stand: Januar 2022
[11] Quelle: https://www.t-systems.com/de/de/ueber-t-systems/zertifikate-t-systems

Ein kontinuierliches Monitoring überwacht die Wahl von der Versiegelung über den Wahlzeitraum bis hin zur Auszählung. Sofern es zu einer Störung im Ablauf der Wahl kommt, wird das POLYAS-Technik-Team automatisch informiert. Zu der Geschäftszeit von POLYAS werktags von 9.00 bis 17.00 Uhr analysiert das POLYAS Technik-Team umgehend den Fall und leitet situationsabhängig Maßnahmen ein. Zudem wird der Kunden-Support informiert. Kund:innen steht bei POLYAS eine Kontaktperson zur Seite, an die sie sich wenden können, sofern es beim Ablauf der Wahl zu technischen Problemen kommt. Auch während einer Störung ist sichergestellt, dass die Integrität und Konsistenz der Daten gewahrt bleibt. Sofern zusätzliche Support- und Handlungszeiten sowie Ansprechpartner:innen für kritische Wahlen benötigt werden, können diese bei POLYAS individuell hinzugebucht werden.

Die T-Systems überwacht ihre Systeme ebenfalls rund um die Uhr. Sollte es auf den Servern der Telekom zu Problemen kommen, greift das dortige Support-Team ein. Stellt POLYAS selbst ein Problem auf der OTC fest, steht POLYAS rund um die Uhr ein direkter Ansprechpartner bei T-Systems zur Verfügung.

9.3 Datenschutz

Als deutsches Unternehmen mit europäischen Server-Standorten erfüllt POLYAS vollumfänglich die deutschen und europäischen Gesetze und Datenschutz-Standards. Alle Vorgänge, bei denen es zur Verarbeitung personenbezogener Daten kommt, werden von uns gemäß den Vorgaben der DSGVO dokumentiert. Zudem haben wir für alle anfallenden Personendaten Löschkonzepte ausgearbeitet. Unsere Mitarbeiter:innen und Dienstleister haben sich dazu verpflichtet, sämtliche Datenschutz-Grundsätze einzuhalten.

POLYAS hat einen Auftragsverarbeitungsvertrag (AVV) speziell auf die Prozesse rund um die Online-Wahl erstellt. Mit dem Dokument werden die datenschutzrechtlichen Bedingungen abgedeckt. Der AVV steht in den AGBs auf der POLYAS Website unter https://www.polyas.de/agb zum Download zur Verfügung.

9.3.1 Zugriffsrechte auf die Wahldaten

Die Zugriffsrechte auf Daten zur Vorbereitung und Durchführung der Online-Wahl werden durch Kennwörter eingeschränkt, die ausschließlich den Wahlveranstaltern den Zugriff ermöglichen. Auch die POLYAS Election Manager:innen können nur im notwendigen Umfang auf die Daten zugreifen und verfügen nicht über alle Zugriffsrechte. Um nachvollziehen zu können, wer zu welchem Zeitpunkt auf die Daten zugegriffen oder diese verändert hat, fertigt POLYAS darüber hinaus Protokolle an, die dem Wahlveranstalter nach Abschluss der Wahl übergeben werden.

9.3.2 Verarbeitung personenbezogener Daten

Grundsätzlich gilt, dass POLYAS personenbezogene Daten ausschließlich nach den Weisungen des Verantwortlichen (Auftraggebers) verarbeitet. Je nach Konfiguration der Wahl müssen unterschiedliche Daten erhoben werden, um beispielsweise die Zugangsdaten zu versenden. Dementsprechend speichert POLYAS für die Wahldurchführung die Daten, die vom Wahlveranstalter im Wählerverzeichnis und Stimmzettel hochgeladen werden.

Diese Daten können beispielsweise sein:

- E-Mail-Adresse
- Name
- Adresse
- Mitgliedsnummer / Matrikelnummer / Mitarbeiternummer
- oder der Log-in-Name, den die Wahlberechtigten im Intranet des Wahlveranstalters verwenden und der ihnen zum Zweck der Pseudonymisierung zugewiesen wurde

9.3.3 Datenübermittlung

Wir versenden Kund:innenendaten ausschließlich über verschlüsselte Datennetze. Auch die Daten selbst sind verschlüsselt, um Manipulationen der Daten bei der Übertragung zu verhindern.

9.3.4 Speicherdauer und Rechte und Datenlöschung

POLYAS speichert personenbezogene Wähler:innendaten grundsätzlich nur so lange, wie es erforderlich ist, um vertragliche oder gesetzliche Pflichten einzuhalten. Danach werden die Daten unverzüglich gelöscht, es sei denn, POLYAS benötigt die Daten noch bis zum Ablauf der gesetzlichen Verjährungsfrist zu Beweiszwecken für zivilrechtliche Ansprüche oder wegen gesetzlicher Aufbewahrungspflichten.

Die Wahlleitung hat jederzeit das Recht, Auskunft über die Daten zu verlangen, die wir gespeichert haben. In diesem Fall stellt POLYAS eine Übersicht der gespeicherten Daten zur Verfügung und erläutert, wofür genau diese Daten benötigt werden.

Einzelne Wählende können die Löschung ihrer bei POLYAS gespeicherten Daten verlangen. Außerdem können diese die Verarbeitung ihrer Daten in bestimmten Fällen einschränken lassen. Auf Wunsch kann ein Löschdatum der Wähler:innendaten nach der Wahl mit der Wahlleitung vereinbart werden.

10 Ausblick

Auch wenn sich POLYAS mit CORE 3.0 Verifiable auf dem neuesten Stand der Technik befindet, wissen wir, dass es ein Stillstehen bei der Entwicklung von Sicherheitsmaßnahmen zum Schutz der Online-Wahl und des Wahlgeheimnisses nicht geben kann. Bereits jetzt zeichnen sich Themen ab, denen sich unserer Forschung und Entwicklung in den kommenden Monaten und Jahren widmen wird.

Noch dieses Jahr wird eine Anwendung live gehen, die es Wählenden möglich macht, sich mit dem neuen Personalausweis am POLYAS Online-Wahlsystem anzumelden. Dazu liest der:die Wählende mit dem eigenen Smartpohne per Ausweis-App2[12] den Personalausweis aus. Die Daten werden an die Bundesdruckerei weitergeleitet. POLYAS erhält von der Bundesdruckerei nur die Daten, die für einen Abgleich mit dem Wählerverzeichnis benötigt werden. Anhand des Abgleichs wird entschieden, ob die Person zur Stimmabgabe zugelassen wird.

Des Weiteren verfolgt POLYAS interessiert den Plan des Bundesamts für Sicherheit in der Informationstechnik (BSI), ein aktualisiertes Schutzprofil zur Sicherheit von Online-Wahlen zu erstellen. Das BSI hat bereits im Dezember 2021 einen ersten Ausblick darüber gegeben, welche kryptografischen Bausteine für eine sicherer Online-Wahl entscheidend sind.[13] Viele der genannten Anforderungen – wie zum Beispiel Signaturen, Zero-Knowledge-Proofs, Bulletin Boards und individuelle sowie universelle Verifikation – erfüllen wir schon heute. Selbstverständlich wird POLYAS eine Zertifizierung der Wahlsoftware CORE 3.0 in Betracht ziehen, sobald das neue Schutzprofil steht.

Eine andere Zertifizierung erfolgt hingegen schon dieses Jahr: die Zertifizierung nach dem weltweit anerkannten Standard ISO 27001. Sie hat das Ziel, die Wirksamkeit unseres Informationssicherheitsmanagementsystems (ISMS) objektiv und glaubwürdig nachweisbar zu machen. Der Schutz sämtlicher bei POLYAS verarbeitete Daten und die Integrität aller IT-Systeme werden im Zuge des Zertifizierungsprozesses analysiert und durch qualifizierte Maßnahmen sichergestellt.

Das POLYAS Research-Team verfolgt zudem genau die neuesten wissenschaftlichen Entwicklungen im Bereich der Quantencomputer. Diese neuartigen Rechner, die eine im Vergleich zu herkömmlichen Geräten ungleich größere Rechenleistung aufweisen, könnten eines Tages so leistungsstark sein, dass sie jedes Passwort entschlüsseln könnten, das bis heute als absolut sicher gilt. Eine solche Technologie würde sich selbstverständlich nicht allein auf Online-Wahlen auswirken, sondern auf jegliche digitale Datenverarbeitung weltweit. Allerdings gibt es auch heute schon Methoden, sich mit mathematischen Verfahren gegen die potenzielle Gefahr zu wappnen. Das Stichwort in diesem Kontext ist die sogenannte *everlasting privacy* (dauerhafter Datenschutz). Das bedeutet, dass die vom POLYAS Online-Wahlsystem veröffentlichten Daten, welche den Auditor:innen ausgehändigt und auf den Bulletin Boards veröffentlicht werden, es nicht ermöglichen, die einzelnen Stimmzettel mit den Wähler:innen in Verbindung zu bringen, selbst wenn man über die uneingeschränkte Rechenleistung eines Quantencomputers verfügt. Eine

[12] Mehr Informationen zur App: https://www.ausweisapp.bund.de/ausweisapp2/
[13] Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2021_02.pdf;jsessionid=A376023AB35672A704C6E28A63EC49BC.internet472?__blob=publicationFile&v=2, S.17f

einfache und für einige Wahlszenarien ausreichende Methode ist die Verwendung anonymisierter Wähler:innendaten. Es gibt jedoch auch kryptographische Techniken, die es POLYAS ermöglichen, *everlasting privacy* in das Online-Wahlsystem zu integrieren. POLYAS wird sich intensiv damit auseinandersetzen, wie diese Verfahren zur Sicherung der Online-Wahl und des Wahlgeheimnisses genutzt werden können.

Der in diesem Jahr bedeutendste Wendepunkt für das POLYAS Research-Team ist indes ein noch grundlegenderes Vorhaben: POLYAS wird damit beginnen, den Quellcode des Core 3.0 schrittweise öffentlich zu machen. Diese auch von Kritiker:innen der Online-Wahl als essenziell verstandene Maßnahme ist ein großer Schritt hin zum Prinzip der Transparenz, dem sich POLYAS seit seiner Gründung verpflichtet fühlt. Beginnen wird POLYAS mit dem Teil des Codes, der sich auf kryptografische Operationen bezieht, einschließlich des Codes für verifizierbares Shuffling der Stimmzettel. Mit einem offenen Quellcode können sich Expert:innen in aller Welt einen Eindruck von der Funktionsweise unserer Online-Wahlsoftware verschaffen und deren Validität überprüfen. Ein wichtiger Schritt hin zum Erreichen unserer Unternehmensvision einer fairen und nachhaltigen Welt, in der Partizipation für alle einfach und sicher ist.

11 Über POLYAS

POLYAS verändert die Art, wie Menschen wählen: Unsere digitale Plattform revolutioniert und vereinfacht die Organisation und Durchführung von Wahlen – von der Stimmabgabe bis zur Stimmauszählung. Das POLYAS Online-Wahlsystem ermöglicht das Wählen von überall, zu jeder Zeit, in Minutenschnelle.

Die Menschen haben bereits mit POLYAS gewählt, bevor sie Googlen konnten: Seit über 25 Jahren stellen wir unseren Kund:innen eine nachhaltige und transparente Lösung zur Verfügung. Dabei sind Sicherheit und Vertrauen unser Fundament, denn nur dadurch kann Partizipation für alle ermöglicht und die Demokratie weltweit gestärkt werden. Zehntausende Online-Wahlen, Nominierungen und Live Votings haben wir bereits erfolgreich durchgeführt. Millionen von Menschen haben ihre Stimme mit POLYAS abgegeben.

Unser Ziel ist Befähigung: Tausende Organisationen haben ihre Wahl bereits ohne unsere Hilfe im POLYAS Self-Service eingerichtet. Mit der sukzessiven Offenlegung unseres Quellcodes und der bewussten Aufgabentrennung in unserem starken Partnernetzwerk geben wir unseren Kund:innen die Kontrolle über uns und unser System. Bei Bedarf unterstützen unsere erfahrenen Wahlexpert:innen aber auch gerne bei der Durchführung von Wahlen.

Die POLYAS GmbH hat mehr als 60 Mitarbeiter:innen und Firmensitze in Kassel, Berlin und der Schweiz. Unsere „Best in Class“-Technologie und unsere langjährige Expertise schaffen Vertrauen. Deshalb sind wir stolz, über 100 Hochschulen, zahlreiche Genossenschaftsbanken, namhafte Vereine und Verbände, Unternehmen (wie die European Bank for Research & Development) und politische Parteien wie die CDU, SPD, FDP oder Bündnis 90/Die Grünen zu unseren Kund: innen zählen zu können.

Die Zukunft von Wahlen ist digital und POLYAS bereitet den Weg dorthin.

Weiterführende Links:

- Kontakt zu POLYAS
- Online-Wahlmanager kostenlos testen
- Blogpost-Serie “Mythen und Fakten zur Sicherheit von Online-Wahlen"

Pressekontakt: presse@polyas.de

POLYAS GmbH
Boxhagener Straße 18
10245 Berlin