E-Voting in der Schweiz – Herausforderungen und Schutzprinzipen

12

Christian Folini und Denis Morel

Zusammenfassung

Der Artikel erklärt, wie Wahl und Abstimmungen in der Schweiz praktisch ablaufen und wie E-Voting die bestehenden Stimmkanäle ergänzt. Dabei ist es wichtig festzustellen, dass der Begriff „E-Voting" in der Schweiz im Sinn des Abstimmens und Wählens von zu Hause aus, über das Internet, verwendet wird. Sogenannte Wahlmaschinen respektive Stimmcomputer im Wahllokal werden in der Schweiz keine eingesetzt. In über 200 Versuchen wurde E-Voting in der Schweiz geprüft, verfeinert und nach und nach immer höheren Sicherheitsanforderungen unterstellt. Grundlegende Konzepte wie die individuelle Verifizierbarkeit, die universelle Verifizierbarkeit sowie die Einführung von unabhängigen Kontrollgruppen bieten einen hohen Schutz vor der Manipulation von Stimmen. Die korrekte Umsetzung dieser Techniken und des zu Grunde liegenden E-Voting Protokolls muss jeweils in separaten Zertifizierungen überprüft werden. Die Implementierung, die Einführung und der Betrieb einer sicheren E-Voting Lösung stellen sehr hohe Anforderungen an das Know-How des Personals sowie die Maturität der Prozesse der beteiligten Organisationen. In der Schweiz erfüllen die Schweizerische Post und der Kanton Genf als Anbieter einer Lösung für die elektronische Stimmabgabe die an ein solches System gestellten Anforderungen.

C. Folini (✉)
netnea AG, Liebefeld, Schweiz
E-Mail: christian.folini@netnea.com

D. Morel
Post CH AG, Bern, Schweiz
E-Mail: denis.morel@post.ch

M. Bartsch, S. Frey (Hrsg.), *Cybersecurity Best Practices*,
https://doi.org/10.1007/978-3-658-21655-9_12

12.1 Einführung

Die Autoren dieses Artikels arbeiten seit mehreren Jahren für die Schweizerische Post im Bereich E-Voting. Denis Morel ist verantwortlich für den Geschäftsbereich und hat mit seinen Kollegen das System bis zum produktiven Einsatz aufgebaut. Christian Folini besetzte bei der Konzeption und dem Einsatz der Sicherheitselemente der Infrastruktur eine Schlüsselrolle. Die Autoren versuchen mit diesem Artikel, die Herausforderungen für die Sicherheit beim Einsatz eines E-Voting-Systems zu erläutern. Darüber hinaus wird beschrieben, wie die Schweiz diese Herausforderungen adressiert hat.

Der Artikel erklärt zunächst, wie Wahl und Abstimmungen in der Schweiz praktisch ablaufen und wie E-Voting die bestehenden Stimmkanäle ergänzt. Essentiell ist der Zusammenhang mit der brieflichen Stimmabgabe. Zudem ist es wichtig festzustellen, dass der Begriff „E-Voting“ in der Schweiz im Sinn des Abstimmens und Wählens von zu Hause aus, über das Internet, verwendet wird. Sogenannte Wahlmaschinen respektive Stimmcomputer im Wahllokal werden in der Schweiz keine eingesetzt.

Nach einer Erläuterung der wichtigsten Herausforderungen und Bedrohungen von E-Voting werden die Antwort der Schweiz in den gesetzlichen Anforderungen erklärt. Insbesondere das Konzept der vollständigen (individuellen und universellen) Verifizierbarkeit spielt hier eine grosse Rolle. Am Ende erklären die Autoren die wichtigsten Schutzprinzipien, die für den Einsatz eines E-Voting-Systems beachtet werden müssen.

12.2 Elektronische Stimmabgabe in der Schweiz

12.2.1 Allgemeine Besonderheiten des politischen Systems

Die Schweiz ist ein Bundesstaat mit drei Ebenen: Bund, Kantone und Gemeinden. Die Verfassung teilt die Kompetenzen der politischen Rechte zwischen Bund und Kantonen auf. Grundsätzlich trägt der Bund die Verantwortung, die Regeln durch gesetzliche Bestimmungen und Anforderungen an eidgenössische Wahlen und Abstimmungen zu definieren und zu überwachen. Die Kantone definieren die Regeln und die Aufteilung der Kompetenzen mit den Gemeinden für kantonale und kommunale Wahlen und Abstimmungen. Dazu kommt, dass der Bund die Kantone mit der Durchführung der Urnengänge auf sämtlichen drei Ebenen betraut. Der Bund fasst danach die Ergebnisse der Kantone für Abstimmungen auf Bundesebene zusammen.

Die Schweiz ist eine direkte Demokratie. Das bedeutet, dass die Schweiz ein Referendums- und ein Initiativrecht besitzt. Das Referendumsrecht erlaubt den Bürgern eine durch das Parlament verabschiedete Gesetzesänderung in Frage zu stellen. Dies geschieht durch eine Sammlung von Unterschriften. Wird das minimale Quorum von 50.000 Unterschriften erreicht, muss der Gesetzestext dem Stimmvolk zur Abstimmung vorgelegt werden. Das Initiativrecht erlaubt Bürgern, Änderungen in der Verfassung vorzuschlagen. Auch hier beginnt der Prozess mit einer Unterschriftensammlung (Quorum von 100.000

Unterschriften bei einer Wohnbevölkerung von 8 Millionen), darauf folgt die Beratung im Parlament und schliesslich die Volksabstimmung. Zu diesen beiden direktdemokratischen Abstimmungsmechanismen kommen alle vier Jahre die eidgenössischen Wahlen. Daneben werden auch kantonale und kommunale Wahlen und Abstimmungen durchgeführt. Das dermassen gestaltete politische System ruft einen Bürger durchschnittlich vier Mal pro Jahr an die Urne. Daraus ergibt sich eine sehr grosse Erfahrung mit Wahlen und Abstimmungen bei den dafür Verantwortlichen, aber auch bei den Stimmbürgern und Stimmbürgerinnen.

Für die praktische Umsetzung hat der Schweizer Bundesstaat in seiner 150-jährigen Geschichte verschiedene Elemente zum Einsatz gebracht. Zentral ist etwa das Stimmregister als Auszug des Einwohnerregisters. Beide Register werden von der Gemeinde gepflegt. Der Bürger erhält automatisch das Stimm- und Wahlrecht in seiner Wohngemeinde. Dazu kommen dieselben Rechte in seinem Kanton und für eidgenössische Wahlen und Abstimmungen. Das Stimmregister wird also laufend gepflegt.

Der primäre Stimmkanal ist die traditionelle „Wahlurne“. Sie steht den Bürgern am Abstimmungs- und Wahlsonntag offen. Die Schweizerische Post geniesst in der Bevölkerung ein hohes Vertrauen. Sie garantiert bei der Zustellung eine hohe Qualität und Zuverlässigkeit. Diese Voraussetzungen erlaubte es 1994 als zweiten Stimmkanal die briefliche Stimmabgabe landesweit einzuführen. Dazu füllt der Stimmbürger den Wahlzettel zu Hause aus und steckt ihn in einen Umschlag. Danach unterschreibt er den separaten Stimmrechtsausweis und legt ihn gemeinsam mit der verschlossenen Stimme in einen voradressierten Briefumschlag und bringt ihn zur Post. Je nach Kanton ist der Umschlag vorfrankiert oder der Stimmbürger muss das Porto selbst bezahlen. Bei der Auszählung werden zunächst die Stimmrechtsausweise überprüft und von den verschlossenen Umschlägen mit den Stimmen separiert. Letztere werden erst in einem zweiten Schritt geöffnet (Stimmgeheimnis).

Mit dem Einsatz der brieflichen Abstimmung [1] hat die Schweiz akzeptiert, dass der Bürger den Wahl- und Abstimmungsakt zu Hause in einem ungeschützten Umfeld durchführt. Heute stimmen mehr als 90 % der Bevölkerung brieflich ab. Die komfortable briefliche Stimmabgabe geniesst damit eine hohe Akzeptanz. Gewisse Schwächen (u. a. entzieht sich die Behandlung der eingehenden brieflichen Stimmen der direkten Kontrolle der Bürger) werden akzeptiert und der Stimmkanal wird nicht prinzipiell in Frage gestellt. Daran ändern auch ab und zu vorkommende Betrugsfälle auf lokaler Ebene nichts. Das heisst, die Auswirkungen der Vorfälle beschränken sich in aller Regel auf den kommunalen Rahmen und es ist sehr selten, dass ein Urnengang wiederholt werden muss. Auf nationale Ergebnisse haben die lokalen Unregelmässigkeiten keine Auswirkungen.

12.2.2 E-Voting in der Schweiz

Die Schweiz hat E-Voting (im Sinn des Abstimmens und Wählens über das Internet) 2003 im Gesetz zu den politischen Rechten versuchsweise eingeführt. Der erste Versuch fand

bei einer eidgenössischen Abstimmung im Kanton Genf statt. Bis heute sind über 200 Versuche durchgeführt worden. Sie waren alle erfolgreich. In 2014 hat das Parlament eine Gesetzesänderung verabschiedet, welche die Anforderungen an ein sicheres, modernes und überprüfbares System verankert. Dazu kommt die Idee der Beobachtbarkeit. Das bedeutet, dass der digitale Zählvorgang sichtbar werden muss und unter Aufsicht geschehen soll. Am Status der versuchsweisen Durchführung von elektronischen Urnengängen hat sich damit aber noch nichts geändert. Ergänzend hat der Bundesrat (die Schweizer Exekutive) im April 2017 bekannt gegeben, dass die elektronische Stimmabgabe in Zukunft als ordentlicher dritter Stimmkanal verankert werden soll.

Wie oben beschrieben sind die Schweizer Kantone mit der Durchführung von Wahlen und Abstimmungen betraut. Dies schliesst die Bundesebene mit ein und betrifft auch das E-Voting: Das bedeutet, dass jeder Kanton entscheiden kann, ob und wie er die elektronische Stimmabgabe einführen will. Er muss ein System auf dem Markt beschaffen und die Einführung sowie den Betrieb zusammen mit seinem Partner planen und organisieren. Heute gibt es zwei produktive E-Voting-Lösungen in der Schweiz: das System der Schweizerischen Post [2] (in Partnerschaft mit der spanischen Firma Scytl) und das System des Kantons Genf [3] (eine In-house Entwicklung, die der Kanton anderen Kantonen zur Verfügung stellt).

Als Voraussetzung für den Einsatz eines E-Voting-Systems für eidgenössische Wahlen und Abstimmungen müssen die Kantone die eidgenössischen technischen und organisatorischen Gesetzesanforderungen erfüllen. Die Bundeskanzlei – die für die Wahrung der politischen Rechte zuständige Bundesbehörde – führt einen Bewilligungsprozess durch. Am Ende des Prüfprozesses steht die Erlaubnis, das geprüfte E-Voting-System einzuführen.

Zunächst wurde E-Voting primär für Auslandschweizer eingesetzt. Aber mehrere Kantone haben E-Voting auch für Teile ihres Inland-Elektorats zugänglich gemacht (namentlich die Kantone Genf, Freiburg, Neuenburg, Basel-Stadt und St. Gallen). Prinzipiell gelten hierfür dieselben Anforderungen der Bundeskanzlei.

Das Stimmmaterial wird für alle drei Stimmkanäle nach wie vor per Brief in physikalischer Form zugestellt. Die Informationen vom Kanton an den Stimmbürger werden also nicht auf elektronischem Weg übermittelt. Wichtig ist ferner sicherzustellen, dass ein Bürger nur ein einziges Mal auf einem einzigen Stimmkanal abstimmen kann. Die Gemeinden und Wahlbüros setzen dazu eine Doppelstimmprüfung ein. Dabei werden die Nummern der physikalischen Stimmausweise mit den Nummern des digital eingesetzten Stimmmaterials verglichen. Damit stellen sie sicher, dass der Bürger nur einmal abgestimmt hat.

12.3 Prinzipielle Herausforderungen beim E-Voting

IT-Sicherheit beschäftigt sich mit Themen, die sich auf der sogenannten CIA-Triade abbilden lassen: Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit). Die Herausforderungen mit der Sicherheit von E-Voting passen idealtypisch auf dieses Modell.

Das Stimmgeheimnis lässt sich dem Thema Vertraulichkeit zuordnen. Ausschliesslich im Stimmregister registrierte Personen dürfen Stimmen abgeben und diese Stimmen sind vor Manipulationen zu schützen. Die Integrität der Stimmen muss also garantiert werden. Und schliesslich soll der Zugang zum elektronischen Stimmkanal für die gesamte Abstimmungsperiode verfügbar sein.

Eine grundsätzliche Herausforderung stellt auch der Browser des Stimmbürgers respektive der Stimmbürgerin dar. Diese Geräte unterstehen nicht der Kontrolle der Administration. Die grosse Verbreitung von Malware und die Anfälligkeit von Browsern für Infektionen bringen es mit sich, dass eine gewisse Zahl von Stimmen auf einem infizierten Gerät abgegeben werden. Auch diese Stimmen sind vor einer Manipulation zu schützen.

Neben den Problemen der IT-Sicherheit spielt die Bedienbarkeit und die Barrierefreiheit der E-Voting-Systeme eine grosse Rolle. Dabei muss darauf geachtet werden, dass die verschiedenen Unterstützungssysteme die Sicherheit des Gesamtsystems nicht schwächen.

12.4 Bedrohungen

E-Voting-Systeme unterliegen denselben Bedrohungen, denen auch andere Systeme der elektronischen Datenverarbeitung ausgesetzt sind. Die 2017 neu erschienene Zusammenstellung der OWASP Top Ten Application Security Risks [4] kann als einfacher Einstieg in diese technische Materie gewählt werden. Tatsächlich ist es aber nötig, sämtliche Bedrohungen mit einem sehr systematischen Ansatz zu erschliessen und in einem umfassenden Bedrohungsmodell (Threat Model) zu beschreiben. Dieses Modell der Applikation ergänzt und komplementiert die übrigen Architekturdokumente. E-Voting bringt es aber auch mit sich, dass das Bedrohungsmodell über die Technik hinaus erschlossen werden sollte. Eine Manipulation der Wahl respektive des Resultats erscheint als sehr grosse Bedrohung. Allein, bereits der Verdacht einer Manipulation bringt einen Vertrauensverlust in das Resultat mit sich und stellt deshalb bereits eine bedeutsame Bedrohung dar.

Wer kommt als Angreifer (Threat Actor) in Frage? Im Inland besitzen die Befürworter respektive die Gegner einer Vorlage potenziell ein Interesse an einer Manipulation. Da unterschiedliche politische Lager die zur Verfügung stehenden Wahlkanäle unterschiedlich annehmen und benützen werden, ergibt sich daraus ein weiteres Motiv für die Manipulation eines Wahlkanales respektive ein Angriff auf seine Verfügbarkeit. Auch international ist eine Beeinflussung einer Wahl ein mögliches Thema. Dabei kann die Manipulation des Resultats im Vordergrund stehen, oder aber ein Vertrauensverlust in ein Resultat provoziert werden, um Land und Gesellschaft zu destabilisieren. Handfester ist die Gefahr, die von einer finanziellen Erpressung ausgeht. Es erscheint schwer vorstellbar, dass jemand ein ganzes Land erpressen würde, aber diese Bedrohung sollte nicht vorschnell von der Hand gewiesen werden. Es ist ja auch bekannt, dass nicht alle Opfer von Ransomware gezielt angegriffen wurden. Bisweilen werden auch Fälle von Kollateralschäden publik, in denen Systeme quasi zufällig von Angriffen der organisierten Kriminalität betroffen wurden.

Unabhängig vom Standort sind E-Voting-Systeme prestigeträchtige Ziele für Sicherheitsforscher oder professionelle Angreifer, die sich Ruhm und Ehre erhoffen und weitgehend frei von finanziellen Motiven arbeiten. Weniger aus Erkenntnisinteresse, denn aus destruktiven Motiven dürften Anarchisten und Terroristen vorgehen, denen es einzig um die Störung oder Beeinträchtigung des elektronischen Wahlkanals und damit um eine Störung des demokratischen Prozesses geht. Zwar besteht diese Bedrohung auch bei den übrigen Wahlkanälen, aber die Zentralisierung der elektronischen Wahlurne und der Zugriff über das Internet potenziert die diesbezügliche Bedrohung.

Wo es nur um die Störung eines Wahlvorganges geht, rücken Denial of Service Angriffe ins Augenmerk. Hier geht es nicht um eine direkte Manipulation von Stimmen, sondern um das Unterbinden des Zugangs zur elektronischen Wahlurne. Denial of Service Angriffe werden heute im Internet als Dienstleistung für wenig Geld angeboten. Dabei hat es sich gezeigt, dass die Strafverfolgungsbehörden sich sehr schwer mit der Ahndung dieser Art von Verbrechen tun, da oft keinerlei verwertbare Spuren zum Auftraggeber des Angriffes zurückführen.

12.5 Rechtliche und regulatorische Grundlagen und Richtlinien

12.5.1 Regulation in der Schweiz

Das politische System der Schweiz mit seiner etablierten direkten Demokratie geniesst einen sehr guten Ruf. Die Beschäftigung mit der Ausgestaltung der demokratischen Prozesse und die praktische Umsetzung der durch die Verfassung garantierten demokratischen Rechte besitzt eine lange Tradition. Und auch E-Voting ist kein neues Thema. In über 200 Pilotwahlgängen wurden verschiedene Systeme getestet und die Verfahren und Richtlinien in mehreren Schritten optimiert.

Seit 2014 umfasst die Schweizer Gesetzgebung folgende Instrumente und legislative Elemente, die E-Voting betreffen:

- Das *Bundesgesetz über die politischen Rechte* definiert, dass E-Voting in der Schweiz als Versuch erlaubt ist und dass der Bundesrat für Bewilligung an einzelnen Kantonen zuständig ist.
- Die *Verordnung über die politischen Rechte* definiert die Grundregeln für die Bewilligung des Bundesrats und die prozentuale Grösse des Teils des Elektorats, für den ein Kanton ein E-Voting-System maximal einsetzen darf.
- Die *Verordnung der Bundeskanzlei über die elektronische Stimmabgabe* sowie die zugeordneten *Technischen und administrativen Anforderungen an die elektronische Stimmabgabe* definieren die einzelnen Anforderungen. Dabei unterscheiden sich die Anforderungen je nach dem prozentualen Anteil der zugelassenen Stimmbürger und Stimmbürgerinnen: Je grösser der Teil des zugelassenen Elektorats desto höher die Anforderungen.

Die Kantone, die E-Voting einführten, haben ihre Gesetze und Verordnungen leicht angepasst, damit E-Voting den Anforderungen der Bundeskanzlei genügen kann.

Die im Gesetz definierten prozentualen Limiten können wie folgt zusammengefasst werden:

- Einsatz für bis zu 30 % der Wahlberechtigten eines Kantons: das E-Voting-System erfüllt eine Liste von technischen und sicherheitsrelevanten Anforderungen (insb. BSI Common Criteria), das Hosting geschieht in der Schweiz.
- Einsatz für 30 % bis 50 % der Wahlberechtigten eines Kantons: Zusätzlich zu den Anforderungen an ein System für 30 % der Wahlberechtigten muss das System den Mechanismus der individuellen Verifizierbarkeit implementieren, das Hosting ist nach IS0 27001 zu zertifizieren und die Plattform ist nach den Anforderungen des Gesetzes zu zertifizieren. Das kryptographische Protokoll ist kryptographisch und semantisch zu beweisen.
- Einsatz für über 50 % der Wahlberechtigten: Zusätzlich zu den Anforderungen an ein System für 50 % der Wahlberechtigten muss das System den Mechanismus der universellen Verifizierbarkeit implementieren. Die Stimmabgabe muss End-to-End verschlüsselt erfolgen und die Plattform muss mehrere Kontrollkomponenten besitzen, die unabhängig voneinander betrieben werden.

Im schweizerischen Kontext ist es wichtig zu verstehen, dass die beiden Konzepte der individuellen und der universellen Verifizierbarkeit vom Gesetzgeber leicht anders definiert wurden als in der Wissenschaft gebräuchlich. Sie werden deshalb hier genauer beschrieben.

12.5.2 Individuelle Verifizierbarkeit

Im Schweizer Kontext ist die individuelle Verifizierbarkeit ein Weg, um die Anforderung des sogenannten „cast-as-intended“ zu implementieren. Die Wähler erhalten in ihrem (physikalischen) Stimmmaterial eine Liste von Kontrollcodes. Für jede Abstimmungsoption gibt es je einen solchen Code (jede Antwort, jeder Kandidat und jede Liste inkl. der leeren Antwort). Wenn der Wähler seine elektronische Abstimmung beendet, berechnet das System die Kontrollcodes der ausgewählten Optionen und zeigt sie auf dem Gerät des Wählers an. Der Wähler kann dann überprüfen, ob die angezeigten Codes denjenigen entsprechen, die er in seinen Stimmunterlagen erhalten hat. Der Wähler kann damit also überprüfen, ob seine Stimme korrekt übertragen und gespeichert wurde. Falls seine Stimme auf dem Weg der Übermittlung geändert worden wäre (Man-in-the-Middle) würde dies damit auffallen (Siehe [7]).

12.5.3 Universelle Verifizierbarkeit

Mit der universellen Verifizierbarkeit wird das E-Voting-System durch die kantonale Wahlkommission überprüfbar und beobachtbar. Zuerst muss das System durch ein verifizierbares kryptographisches Protokoll definiert werden. Das Protokoll heisst verifizierbar, weil es mathematische Beweise enthält, die erlauben, in jedem einzelnen Schritt zu beweisen, dass die Stimmen in der Urne nicht verändert wurden. Diese Beweise funktionieren selbst mit verschlüsselten Stimmen, also ohne die Stimmen und die Ergebnisse der Abstimmung zu kennen (Zero Knowledge Proof). Diese Beweise werden durch die Wahlkommission geprüft und validiert. Damit kann die Wahlkommission belegen, dass niemand die Urne gefälscht hat.

Zusätzlich sehen die Ausführungsbestimmungen der Schweizerischen Bundeskanzlei als Ergänzung zur universellen Verifizierbarkeit vier Kontrollkomponenten vor. Diese Kontrollkomponenten müssen die elektronische Urne und die Stimmabgabe überwachen. Sie sind unabhängig voneinander zu betreiben und garantieren damit einen zusätzlichen, vierfachen Schutz vor Manipulationen.

12.5.4 BSI Common Criteria

Die Anforderungen der Bundeskanzlei referenzieren direkt das Common Criteria Schutzprofil als Grundlage der Sicherheitsanforderungen an Online-Wahlprodukte (BSI-CC-PP-0037).

In der Einleitung des Dokumentes (siehe [8]) ist das Ziel des Schutzprofiles wie folgt definiert:

„Dieses Schutzprofil definiert einen Basissatz von Sicherheitsanforderungen, den jedes Online-Wahlprodukt zumindest erfüllen muss, um einige Arten von Vereinswahlen, Gremienwahlen, etwa in den Hochschulen, im Bildungs- und Forschungsbereich, und insbesondere nichtpolitische Wahlen mit geringem Angriffspotenzial sicher auszuführen."

Jedes E-Voting-System in der Schweiz muss die kompletten Anforderungen des Schutzprofils erfüllen, soweit sie mit den Gegebenheiten des schweizerischen politischen Systems vereinbar sind.

12.5.5 Zertifizierungen

Das Gesetz zu den politischen Rechten definiert, dass die Kantone und der Betreiber eines E-Voting-Systems ein Management System für Informationssicherheit (ISMS) im Einsatz haben müssen. Es muss konform zum ISO Standard 27001 aufgebaut und zertifiziert sein. Mit dem Management System wird sichergestellt, dass E-Voting sehr hoch in der Organisation verankert ist und dass die beschriebenen Prozesse aktiv gelebt werden. Dazu kommt, dass Entscheidungen auf einem Riskmanagement-System abgestützt werden müssen.

Zusätzlich zu einer Zertifizierung nach ISO 27001 müssen die Kantone und die Betreiber sich durch eine akkreditierte Zertifizierungsstelle prüfen lassen. Damit kann sichergestellt werden, dass das E-Voting-System und sein Betrieb im Detail konform zu den gesetzlichen Anforderungen des Bundes ist und bleibt. Der Scope der Zertifizierung umfasst die folgenden Teile:

- Prüfung des Protokolls: Validierung und Kontrolle der kryptographischen und semantischen Beweise des Protokolls.
- Prüfung der Funktionalitäten: Validierung der Erfüllung der funktionalen Anforderungen inkl. des Schutzprofils.
- Prüfung der Infrastruktur und des Betriebs: Validierung der Erfüllung der betrieblichen und organisatorischen Anforderungen.
- Prüfung der Kontrollkomponenten: Validierung der Erfüllung der Anforderungen für die universelle Verifizierbarkeit.
- Prüfung des Schutzes gegen Versuche in die Infrastruktur einzudringen: Validierung der Sicherheit des Systems, insbesondere. durch Penetrationstests.
- Prüfung der Druckerei: Validierung der Erfüllung der spezifischen Anforderungen an den Druck der Stimmrechtsausweise mit den Kontrollcodes.

12.6 Schutzprinzipien

Ohne moderne kryptographische Methoden wäre es nicht möglich, E-Voting-Systeme adäquat zu schützen. Die Fortschritte der letzten Jahrzehnte auf diesem Gebiet sind damit eine Voraussetzung für die Erfüllung der oben beschriebenen Schutzziele, namentlich Vertraulichkeit und Integrität der Stimmen. Die Public- / Private-Key-Verschlüsselung wie etwa die sogenannte ElGamal-Verschlüsselung ist ein zentrales Element, das in verschiedenen Teilen der Systeme eingesetzt werden kann.

Homomorphe Verschlüsselung erlaubt es, die Stimmen über mehrere Schritte zu anonymisieren, ohne dass die Stimme selbst verändert würde. Die Integrität der einzelnen Stimme wird durch die Verifizierbarkeit garantiert. Auch dahinter stehen kryptographischen Methoden.

Die maximale Sicherheitsstufe eines IT-Systems wird gemeinhin durch das schwächste Element vorgegeben. Die Einbindung der oben angesprochenen Kontrollgruppen hat das Ziel, hier eine höhere Schutzstufe zu etablieren. Der Schutz soll also nicht mehr länger durch das schwächste Element vorgegeben werden können. Vielmehr soll der höchste Schutz erhalten bleiben, solange wenigstens eine der Kontrollgruppen wie vorgegeben arbeitet. Es handelt sich dabei um eine Anwendung von byzantinischer Fehlertoleranz.

Ein wichtiges Grundprinzip beim Bau der E-Voting-Infrastruktur ist die Mandatory Access Control (MAC). Das heisst, jeder Systemzugriff und jede Veränderung von Einstellungen unterliegt einer Prüfung der Zugriffsberechtigungen. Die Berechtigungen selbst

werden unterteilt (Separation of Duties) und die Mächtigkeit der einzelnen Akteure und Systeme dadurch limitiert. Es werden immer nur die minimalen Zugriffsrechte, die nötig sind, um eine Arbeit verrichten zu können (Least Priviledge/Need to Have), ausgegeben. Beispielhaft hierfür ist die Aufteilung der Schlüssel zur Dechiffrierung der Wahlurne, die über den gesamten Wahlausschuss verteilt werden. Das bedeutet, dass ein einzelnes Mitglied der Wahlkommission die Urne nicht entschlüsseln kann. Die Betreiber der Wahlurne selbst wiederum besitzen keinen Anteil an diesen Schlüsseln und sind deshalb nicht in der Lage, die Stimmen selbst einzusehen.

Mandatory Access Control bedeutet in der Konsequenz auch eine Trennung der E-Voting-Systeme von anderen Systemen. Diese Separierung der Infrastruktur beim Betreiber stösst allerdings ab einem bestimmten Grad an wirtschaftliche Grenzen und lässt sich nicht mehr finanzieren, so dass bei der Trennung Kompromisse eingegangen werden müssen.

Die Infrastruktur ist durch mehrere Sicherheitsschichten zu schützen (Multi-Tier/Multilayer). Wesentliche Elemente stellen natürlich Netzwerk-Firewalls zwischen den Komponenten aber auch Web Application Firewalls (WAF) dar. Die Open Source WAF ModSecurity erlaubt dabei eine sehr granulare Kontrolle des Verkehrs. Ein Regelwerk wie das OWASP ModSecurity Core Rule Set sorgt für einen Grundschutz und weitere Regelsätze implementieren zusätzliche Schutzmassnahmen welche das MAC Modell respektive das Need-to-Have Prinzip unterstützen (Whitelisting von erlaubten Zugriffen).

Die Transparenz ist ein weiteres Grundprinzip, das die politische Akzeptanz von E-Voting-Systemen erhöhen kann. Die Transparenz bringt aber auch einen administrativen Mehraufwand mit sich, denn Informationen wollen richtig aufbereitet und für die interessierte Öffentlichkeit verständlich kommentiert werden. Die Sicherheit der implementierten E-Voting-Protokolle lässt sich kaum feststellen, solange nicht zumindest die Protokolle öffentlich gemacht und in der Forschungsgemeinschaft diskutiert werden. Bei der Frage der Offenlegung des Quellcodes sind die Interessen der Öffentlichkeit gegenüber den Schutzbedürfnissen des geistigen Eigentums zu prüfen. Die Frage der Transparenz stellt sich auch bei den Berichten zu Zertifizierungen und Penetration Tests, die gegebenenfalls zu publizieren sind. Private Sicherheitstester interessieren sich für E-Voting. Es bietet sich an, diesen die Beschäftigung mit dem E-Voting-System in einem regulierten Rahmen zu erlauben und dadurch öffentliche Penetration Tests zu ermöglichen. Dazu gehört es auch, einen Dialog mit diesen Forschern zu etablieren und auf ihre Befunde gegebenenfalls mit Anpassungen zu reagieren.

Disaster Toleranz und das weiter oben angesprochene Denial of Service Problem verlangen nach eigenen Lösungen. Ein Aufbau über mehrere Server-Standorte hinweg erscheint zwingend. Grosse Denial of Service Angriffe dürften die Infrastruktur dennoch überfordern. Ein Stück weit vermag ein Zusammengehen mit dem Internet Service Provider die Angriffe abzuschwächen, aber die grössten Angriffe werden die Netzwerkkapazität des Providers trotzdem übersteigen. Im Normalfall wird in diesem Moment die Unterstützung eines Content Delivery Networks respektive eines Anti DDoS Services gesucht.

Allerdings bedingen diese Massnahmen, dass man die SSL-/TLS-Schlüssel an den Schutzpartner übergibt, was im E-Voting-Kontext kaum denkbar ist. Das Ausschliessen von fremden IP-Adressen ist ebenfalls eine hilfreiche Massnahme (GeoIP), allerdings schneidet sie Stimmbürgerinnen und Stimmbürger im Ausland vom E-Voting ab, was dem Sinn und Zweck der Lösung zu widersprechen scheint. Effektiver erscheinen deshalb administrative Massnahmen wie die in der Schweiz bis dato favorisierte Schliessung des elektronischen Kanals 24 Stunden vor dem Schliessen des schriftlichen Abstimmungstermins. Das heisst, dass lokale Stimmbürger immer noch an der Urne abstimmen können. Ein DoS-Angriff auf den elektronischen Kanal wäre damit ärgerlich, würde die Stimmbürgerinnen und Stimmbürger aber nicht von einer Stimmabgabe abhalten. Auslandschweizer sind angehalten, ihre Stimme möglichst rasch nach Erhalt der Stimmunterlagen abzugeben.

12.7 Zusammenfassung

Die Schweiz hat ein gut etabliertes politisches System mit starken direktdemokratischen Elementen. Das Stimmvolk wird mehrmals pro Jahr an die Urne gerufen. Die sich daraus ergebende Routine im Umgang mit Abstimmungen und Wahlen sowie das breit akzeptierte briefliche Abstimmen bildet eine gute Voraussetzung zur Einführung der elektronischen Stimmabgabe über das Internet.

In über 200 Versuchen wurde E-Voting in der Schweiz geprüft, verfeinert und nach und nach immer höheren Sicherheitsanforderungen unterstellt. Grundlegende Konzepte wie die individuelle Verifizierbarkeit, die universelle Verifizierbarkeit sowie die Einführung von unabhängigen Kontrollgruppen bieten einen hohen Schutz vor der Manipulation von Stimmen. Die korrekte Umsetzung dieser Techniken und des zu Grunde liegenden E-Voting-Protokolls muss in separaten Zertifizierungen überprüft werden.

Die Implementierung, die Einführung und der Betrieb einer sicheren E-Voting-Lösung stellen sehr hohe Anforderungen an das Know-How des Personals sowie die Maturität der Prozesse der beteiligten Organisationen. In der Schweiz erfüllen die Schweizerische Post und der Kanton Genf als Anbieter einer Lösung für die elektronische Stimmabgabe die an ein solches System gestellten Anforderungen.

Literatur

1. Der Begriff „briefliche Abstimmung“ bedeutet in diesem Artikel, dass der Bürger per Brief abstimmen und wählen kann.
2. Siehe https://www.post.ch/evoting (am 24.12.2017 abgerufen).
3. Siehe https://www.ge.ch/vote-electronique/ (am 24.12.2017 abgerufen).
4. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, (am 24.12.2017 abgerufen).

Referenzen

1. Swiss Online Voting Protocol, R&D, Scytl Secure Electronic Voting (2016) https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol.pdf (am 24.12.2017 abgerufen)
2. Swiss Post E-Voting Protocol Explained, Scytl Secure Electronic Voting & Post CH Ltd (2016) https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol-explained.pdf (am 24.12.2017 abgerufen)
3. Distributed immutabilization of secure logs, Scytl Secure Electronic Voting & Post CH Ltd (2017) https://www.scytl.com/wp-content/uploads/2017/01/Distributed-Immutabilization-of-Secure-Logs_Scytl.pdf (am 24.12.2017 abgerufen)
4. A Secure E-Voting Infrastructure. Implementation by Swiss Post (2017), Second International Joint Conference on Electronic Voting E-Vote-ID 2017, TUT Press (am 24.12.2017 abgerufen)
5. Federal Ordinance on Political Rights, Swiss Federal Chancellery (2014) https://www.admin.ch/opc/de/classified-compilation/19780105/index.html (am 24.12.2017 abgerufen)
6. Federal Chancellery Ordinance on Electronic Voting (VEleS) , Swiss Federal Chancellery (2014) https://www.admin.ch/opc/en/classified-compilation/20132343/index.html (am 24.12.2017 abgerufen)
7. Technical and administrative requirements for electronic vote casting, Swiss Federal Chancellery (2014) https://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=en (am 24.12.2017 abgerufen)
8. Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte (BSI-CC-PP-0037) https://www.commoncriteriaportal.org/files/ppfiles/pp0037b.pdf (am 24.12.2017 abgerufen)