Das heikle Geschäft mit der Demokratie

Für die Schweizerische Post ist E-Voting ein Prestigeprojekt. Dabei setzt sie auf Technologie der spanischen Firma Scytl. Jetzt zeigen Republik-Recherchen: Der Marktführer für E-Voting hat EU-Gelder zweckentfremdet, Wahlen in den Sand gesetzt – und Sicherheitsprobleme bei der Stimmabgabe.

Von Adrienne Fichter, 31.01.2019

Eigentlich müsste sich die Schweizerische Post freuen. Nach dem Aus ihres Genfer Konkurrenten CHVote besitzt sie das E-Voting-Monopol im Land. Alle anderen Anbieter haben aufgegeben: weil sie die hohen Sicherheitskosten scheuen oder den Anforderungen des Bundes nicht standhalten.

Freuen müsste sich auch Scytl. Die spanische E-Voting-Firma ist der Branchenleader. Sie verkauft ihre Wahlsoftware an 42 Länder. Die Post ist einer ihrer wichtigsten Kunden.

Doch die Freude wird getrübt. Die Kritik am E-Voting wird lauter und lauter. Immer mehr Politikerinnen zweifeln an der Zuverlässigkeit des digitalen Wählens. Vergangenen Freitag präsentierten die Gegner gar eine Volksinitiative gegen das E-Voting. Mit einem Moratorium wollen sie die Wahltechnologie so lange verbieten lassen, bis nachgewiesen werden kann, dass die Stimmabgabe im Internet dieselben Sicherheitsstandards erfüllt wie jene der Urnenwahl.

Noch vor zehn Jahren herrschte Aufbruchstimmung beim Thema E-Voting. Davon ist im Wahljahr 2019 nur noch wenig zu spüren. Skepsis und Widerstand machen sich breit. Selbst die E-Voting-Promotoren werden nervös. Es steht viel auf dem Spiel – besonders für die Post. Das E-Voting ist ein Prestigeprojekt für den Staatskonzern. Er will damit zeigen, dass er beim digitalen Wandel mithalten kann.

Der Technologiepartner, auf den die Post beim Aufbruch in die digitale Zukunft der Demokratie setzt, ist allerdings nicht über alle Zweifel erhaben. 2014 hat Scytl regionale Wahlen in Ecuador derart vermasselt, dass alle eingescannten Wahlzettel am Scytl-Hauptsitz in Barcelona manuell ausgezählt werden mussten. Einige Scytl-Manager wurden deswegen sogar vorübergehend festgenommen. Das zeigen Recherchen der Republik.

Damit nicht genug: Das Unternehmen hält wichtige Informationen für die Überprüfung seines E-Voting-Systems zurück oder verlangt dafür saftige Lizenzen. Zudem setzte das Unternehmen sowohl Gelder aus Spaniens Staatskasse wie auch EU-Forschungsgelder für die Kundengewinnung ein, anstatt sie wie vorgeschrieben in die Weiterentwicklung zu investieren. Und dann ist da noch der Fall mit der unsicheren Stimmabgabe in Australien.

Was also ist vom Technologiepartner der Post zu halten?

Die Geschichte der Firma Scytl ist geprägt von Erfolgen, aber auch einigen Pannen. Es ist die Geschichte eines Unternehmens, das sich mehrfach neu erfunden hat – und für das die Schweiz schon sehr früh eine zentrale Rolle spielte.

Vor allem aber zeigt die Geschichte von Scytl, wie heikel es sein kann, wenn eine hoheitliche Staatsaufgabe wie der Wahlvorgang an eine private Firma ausgelagert wird.

Der Kanton Neuenburg als erster Kunde

Scytl wurde 2001 von Andreu Riera gegründet. Die Idee dafür hatte der Kryptografieexperte während der US-Präsidentschaftswahlen von 2000. Als damals die Stimmen in Florida nachgezählt werden mussten, dachte Riera, das müsse doch online viel effizienter ablaufen. «Wenn die wichtigste Demokratie der Welt einen Monat braucht, um zu bestimmen, wer gewonnen hat, und der Oberste Gerichtshof eine endgültige Entscheidung treffen muss, dann ist das traditionelle Wahlsystem eindeutig gescheitert», zitierte der frühere Scytl-CEO Pere Valles den 2006 verstorbenen Gründer Riera.

Der Wissenschaftler tüftelte seit den 1990er-Jahren an der Universitat Autònoma de Barcelona an kryptografischen Lösungen. Seit je beschäftigte ihn das Paradoxon einer E-Voting-Lösung: die Vereinbarkeit des Stimmgeheimnisses und der Verifizierung eines Wählers.

Die Kollegen seiner Forschungsgruppe nahm er gleich mit zu Scytl, sie waren die ersten Angestellten des Unternehmens.

Am Anfang harzte es. Die Wissenschaftler waren keine Verkäufer. Es war schwierig, den Regierungen eine derart komplexe Technologie zu erklären. Niemand wollte sich die Finger an elektronischen Wahlen verbrennen.

Scytl brauchte dringend einen ersten Kunden. Und fand ihn 2004 – im schweizerischen Neuenburg. Weshalb bot sich der Westschweizer Kanton damals als Versuchskaninchen an? Der Bund habe Pilotkantone für das E-Voting gesucht, sagt Neuenburgs Vizekanzler Pascal Fontana auf Anfrage der Republik. «Wir suchten die Firma mit dem besten Fachwissen in Sachen Sicherheit.» Die Wahl fiel auf Scytl.

Neuenburg wurde für das spanische Start-up zum Testfall. Und katapultierte die Firma in neue Höhen. Mit dieser ersten Referenz wuchs Scytl schlagartig.

Der Durchbruch gelang mit Florida

Nun floss das Geld. Mehrere Investoren dockten an. Unter anderem auch Vulcan Capital, der Fonds von Paul Allen, Co-Gründer von Microsoft. Dank den Finanzspritzen schaffte Scytl den Sprung von der akademischen Welt auf den freien Markt. Die Firma meldete 40 Patente an und stellte weltweit 600 Mitarbeiter ein. Bis vor ein paar Jahren war Scytl mit über 120 Millionen Euro Risikokapital das bestfinanzierte Start-up Spaniens.

Gründer Andreu Riera, der sich in der Forschungswelt wohler fühlte als in der Privatwirtschaft, überliess sein Baby dem neuen CEO Pere Valles und widmete sich neuen Forschungsideen. 2006 kam Riera bei einem Autounfall ums Leben. Er erlebte damit die wichtigste Wachstumsphase von Scytl nicht mehr – als der Firma 2008 der internationale Durchbruch gelang.

Es war das Jahr, in dem Facebook-König Barack Obama Millionen von Wählerinnen im Netz begeisterte. Und das Jahr, in dem das spanische E-Voting-Wunder seinen ersten amerikanischen Kunden gewann: Florida. Der US-Bundesstaat, der Andreu Riera zur Gründung von Scytl inspirierte.

«Florida wollte nicht mehr der letzte, sondern der erste Staat sein», erzählte CEO Valles später dem Businessmagazin «Informilo». Die Wahlbehörden suchten nach einer Technologie, mit deren Hilfe die in Afghanistan stationierten Soldaten abstimmen konnten. Die Auslandswähler wurden immer mehr zum wichtigsten Verkaufsargument für Scytl.

Die Nachfrage nach der Stimmabgabe via Internet wuchs. Aber nicht so schnell, wie dies Scytl-CEO Valles und seine Investoren gerne gehabt hätten. Politische Wahlen sind ein spezieller, volatiler Markt. Zu spüren bekam dies die Firma, als 2015 ein Vertrag über 30 Millionen Euro mit der Republik Kongo platzte. Der damalige Präsident des Landes hatte sich in letzter Sekunde gegen die Internetwahl entschieden.

24 Wahlprodukte im Angebot

Das spanische Unternehmen änderte aufgrund solcher Unwägbarkeiten schon sehr früh sein Geschäftsmodell. Es wurde zum Allrounder, einer Art Gemischtwarenladen für alle Arten des Wählens, online und traditionell. Neu boten die Spanier Software für Wahlmaschinen sowie Infrastruktur und Betreuung vor Ort an. Bis heute sind 24 verschiedene Wahlprodukte im Angebot, von der reinen Internetwahl bis zum Betrieb digitaler Urnen.

In den USA waren die Behörden zuerst skeptisch gegenüber *pitches* der spanischen Firma. Ausländischen Firmen, die Wahltechnologien verkauften, begegnete man grundsätzlich misstrauisch. Das änderte sich 2012, als Scytl den amerikanischen Konkurrenten SOE aufkaufte und Teams in den USA aufbaute. Von den 3200 US-Bezirksbehörden sind heute 1400 Scytl-Kunden.

In Fachmagazinen und an Internetkonferenzen rühmt sich die Firma, die Demokratien in Entwicklungsländern zu retten. Mit Werbevideos, die auf die Fehleranfälligkeit des Menschen verweisen. Und die präzise Schnelligkeit des Digitalen loben. Auf der Website des Unternehmens steht der Slogan: *We Power Democracy.*

Ex-CEO Pere Valles behauptete gerne, Wahlbetrug werde dank Scytl eingedämmt. An der NOAH-Konferenz in London im November 2015 erzählte er einem Reporter folgende Erfolgsgeschichte aus Afrika: «Drei Monate hatte es gedauert, bis die Stimmen der Wahlen 2010 in der Elfenbeinküste ausgezählt waren. 3000 Menschen sind gestorben, weil Präsident Laurent Gbagbo den Sieg des Herausforderers Alassane Ouattara wegen der langen Nachzählung nicht akzeptierte. Dank unserer Technologie konnten 2015 40 Prozent der Stimmen innerhalb von 24 Stunden ausgezählt werden. Ohne jeden Aufruhr.»

Trotz geplatzten Geschäften wie im Kongo wurden afrikanische Staaten wie die Elfenbeinküste zum besten Marketing für die spanische Firma. Immer wieder wiederholte Scytl ihre Werbebotschaft: Menschen sind fehlbar und nicht vertrauenswürdig, das Internet jedoch ist nicht korrumpierbar.

Verschlüsselung als Trumpf

Auch deswegen wurden Internetwahlen im vergangenen Jahrzehnt immer salonfähiger. Die Zahl der Scytl-Kunden wuchs seit 2012 stetig an. Doch damit wuchsen auch die Sicherheitsbedenken. Effizientes Abstimmen mit drei Klicks reichte nicht mehr als Verkaufsargument. Wählerinnen möchten darauf vertrauen können, dass ihre Stimmen auch digital sicher übermittelt und korrekt gezählt werden.

Kein Problem für Scytl, im Gegenteil: Genau auf diesem Feld triumphiert die Firma. Das Kryptografie-Know-how wurde dank ihrem Gründer Riera zum Asset des Unternehmens. Das manifestiert sich auch im Firmennamen. Scytl ist eine Ableitung von Skytale – dem Namen des ersten kryptografischen Werkzeuges, das je verwendet wurde: eine Pergamentrolle auf einem Zylinder. Die alten Griechen und Spartaner haben damit verschlüsselt kommuniziert.

Besonders stolz ist der E-Voting-Marktführer auf die technische Vereinbarkeit von Wahlgeheimnis und Authentifizierung. «Wir haben Verfahren entwickelt, mit der Wahlprüfer kontrollieren können, ob die abgegebenen Stimmen mit den eingetroffenen Stimmen übereinstimmen», so Valles im Jahr 2015. «Universelle Verifizierbarkeit» nennt man das im Fachjargon. Damit soll sichergestellt werden, dass die elektronisch abgegebenen und übermittelten Stimmen unterwegs nicht manipuliert werden können.

So weit, so gut. Gräbt man jedoch tiefer, tauchen viele Fragezeichen auf. Wie geht der Technologiepartner der Post …

1. … mit öffentlichen Geldern um?
2. … mit Pleiten und Pannen um?
3. … mit Sicherheitslücken um?

Und was bedeutet das alles für die E-Voting-Lösung der Post?

Wie Scytl mit Forschungsgeldern umgeht

Da ist die Sache mit dem Geld. Über den finanziellen Erfolg von Scytl ist nur wenig bekannt. Darüber spricht das spanische Unternehmen ungern. Die hohen Wachstumsraten und riesigen Finanzspritzen werden kommuniziert, Umsatzzahlen hingegen weist das Unternehmen keine aus.

Lange Zeit arbeitete das Start-up auf einen Börsengang hin. Ziel war es, 2017 am amerikanischen Nasdaq zu debütieren. Doch just in jenem Jahr liessen die Scytl-Manager die Börsenpläne fallen. Aus Gründen der Neutralität. «Bei einem so sensiblen Geschäftsfeld wie Wahltechnologie ist ein Börsengang in den USA politisch heikel», sagt Scytl-Sprecherin Gwendolyne Savoy.

Über die Investoren der Firma kursieren zahlreiche Gerüchte im Netz. Viele davon sind unhaltbar. Etwa, dass Scytl Verbindungen in die CIA unterhalte. Oder dass George Soros die Firma gekauft habe. Fest steht jedoch, dass Scytl hohe Summen aus der spanischen Staatskasse erhalten hat. Eigentlich handelte es sich dabei um Forschungsgelder. Doch die Firma setzte die Mittel in einigen Fällen anders ein als vorgeschrieben, wie Recherchen der Republik belegen.

Statt die Gelder in die Zusammenarbeit mit Universitäten zu stecken, stockte Scytl damit die Produktteams auf und entwickelte neue Prototypen für ihre Kunden. Ein Zuschuss über 1,5 Millionen Euro von Spaniens

Ministerium für Forschung und Industrie wurde gemäss einem internen Dokument, das der Republik vorliegt, unter anderem für eine «Produkte-Demo» für den Kanton Neuenburg eingesetzt. Und 900'000 Euro des EU-Förderungsfonds flossen in die Entwicklung von Softwaremodulen für ecuadorianische Wahlbehörden.

Im Dokument stehen Vermerke, wie der Mitteleinsatz gerechtfertigt werden soll. «Wir haben kreative Reports geschrieben», erinnert sich ein ehemaliger Projektmanager gegenüber der Republik. Spaniens öffentliche Förderer interessierte dies offenbar nicht. Oder sie waren mit den Erläuterungen von Scytl zufrieden – es gab keine Nachprüfungen. Scytl dementiert: «Die Gelder haben wir nur für Forschung und Entwicklung eingesetzt», sagt Sprecherin Gwendolyne Savoy.

Systemausfall in Ecuador

Da ist die Sache mit der Verlässlichkeit. Erfolgsgeschichten über Scytl sind viele zu hören, kaum bekannt sind die Pannen. Zum Beispiel jene bei den Regionalwahlen 2014 in Ecuador. Scytl hatte den Auftrag erhalten, für einige Regionen des lateinamerikanischen Staats die Wahlmaschinen zu betreiben.

Am Wahltag, dem 23. Februar, versagte die Technik auf mehreren Ebenen: Die Scytl-Software funktionierte in manchen Bezirken überhaupt nicht. Das Programm konnte einen grossen Teil der eingescannten Wahlpapiere nicht richtig lesen und korrekt interpretieren. Und einige Server fielen wegen der hohen Datenmenge komplett aus. In den Dschungelregionen, wo es nur schwaches Internet gab, war die Situation besonders dramatisch.

Gemäss einem Bericht der Union der Südamerikanischen Nationen (Unasur) «war das System nicht in der Lage, die Menge der eingescannten Informationen zu verarbeiten». IT-Blogger kritisierten später, dass das System vorher nicht ausreichend getestet worden sei. Scytl wiederum gab der schlechten Infrastruktur Ecuadors die Schuld.

Der nationale Wahlrat Ecuadors war empört und schickte das Scytl-Personal mitsamt den Wahlzetteln nach Barcelona. Am Hauptsitz der Firma hatten die Mitarbeiter 72 Stunden Zeit, die eingescannten Wahlzettel händisch auszuzählen. Als Pfand behielt Ecuadors Regierung mehrere Manager der Firma im Land zurück, unter anderem den zuständigen Projektleiter Osman Loaiza. Sie wurden vorübergehend festgehalten – wegen «Vertragsbruchs».

Im Hauptquartier wurden derweil alle Mitarbeitenden für die händische Aufzählung aufgeboten. Sie hätten während dieser Zeit auf Matratzen im Büro geschlafen, erinnert sich ein ehemaliger Entwickler. Doch es waren zu viele Wahlzettel. Scytl konnte erst nach einem Monat verkünden, wer in den ihnen zugeteilten Wahlbezirken gewonnen hatte. Die Zusammenarbeit wurde danach aufgelöst. Und die Scytl-Manager mussten sich vor Gericht verantworten.

Der Fall habe seltsamerweise international kaum Aufmerksamkeit erregt, sagen ehemalige Angestellte heute. Scytl bestreitet, dass die Wahlen in Ecuador in einem Debakel endeten. Man habe den Prozess «insgesamt verbessern können gegenüber den regionalen Wahlen 2009», sagt die Scytl-Sprecherin.

Schliesslich ist da noch die Sache mit der Sicherheit. Der heikelste Vorfall für Scytl geschah 2015 während der Parlamentswahlen im australischen

Bundesstaat New South Wales. Gewählt wurde dort mit der Scytl-Software iVote. Die Forscher Alex Halderman der University of Michigan und Vanessa Teague der University of Melbourne schauten sich das System genauer an und entdeckten eine gravierende Schwachstelle: Sie schafften es, die Verschlüsselung zwischen dem Browser des Wählers und dem E-Voting-System zu umgehen.

Hätten das Hacker mit bösen Absichten getan, so wäre es möglich gewesen, die Anonymität der Wählerin aufzuheben und die Stimme zu manipulieren.

Nun ist es nicht so, dass sich Scytl nach solchen Vorfällen verschanzt. Das Unternehmen reagierte auf die Kritik der Expertinnen. Relativ ausführlich, aber in der Position stets defensiv.

Denn da ist eine weitere Sache, die Fragen aufwirft.

Die Sache mit der Transparenz.

Fehlende Überprüfbarkeit

Zwar ist sich das Führungsteam von Scytl seines heiklen Geschäfts mit der Demokratie bewusst. Die Leute wissen, dass ihr Produkt durch Hackingattacken angreifbar ist. Deswegen holte Ex-CEO Pere Valles Wissenschaftlerinnen und Verschlüsselungsexperten in die Beiräte und bot Hand für Experten-Reviews.

Doch bei den wirklich relevanten Informationen bleibt man knausrig. Um Software kritisch zu überprüfen, bedarf es mehr als nur der Kenntnis des Quellcodes. Erst mit einer umfangreichen Dokumentation und Anleitung können Systeme aufgesetzt und getestet werden.

Genau diese Informationen gibt das spanische Unternehmen jedoch gemäss Informationen der Republik nicht heraus.

Entweder beantwortet die Firma entsprechende Anfragen damit, dass die Veröffentlichung ganzer Dokumentationen nicht zwingend mehr Sicherheit bedeuten würde. Auf Nachfrage des Technologiemagazins «Ars Technica» antwortete eine Scytl-Sprecherin 2016 flapsig: «Die Wähler kennen den Quellcode ihres Online-Bankings schliesslich auch nicht.»

Oder aber die Firma gibt in Stellungnahmen unumwunden zu, dass öffentliche Reviews ihr Geschäftsmodell gefährden würden. Weil die Konkurrenz damit kostenlos Zugriff auf das Kapital von Scytl erhielte – die Software und das über Jahre aufgebaute Know-how: «Bei einer öffentlichen Begutachtung hätte Scytl keine Kontrolle darüber, wer Zugriff auf unser geistiges Eigentum hat.» Also versuchen Scytl-Manager zu viel Transparenz möglichst zu vermeiden, wie veröffentlichte Forschungspapiere zeigen.

Forscher der Universität Berkeley wollten bereits 2008 Software der «Voting Kiosks» in Florida untersuchen, also der Wahlmaschinen, die zum Einsatz kommen. Doch ihnen fehlten dafür die entscheidenden Dokumente. Die Berkeley-Forscher konnten also weder testen, ob das System einwandfrei funktioniert, noch war es ihnen möglich, zu Testzwecken Angriffe darauf durchführen.

Das Debakel in Norwegen

Dasselbe Problem wiederholte sich drei Jahre später, als Norwegen 2011 beschloss, E-Voting einzuführen. Man setzte auf Scytl-Software. Um Vertrauen bei der norwegischen Bevölkerung zu gewinnen, publizierten die Behörden den Quellcode.

Doch das vorhandene Material war nicht nur unbrauchbar, es war sogar fehlerhaft. Eine Forschungsgruppe aus der Schweiz wies schliesslich die norwegische Regierung auf die Schwachstelle hin. Der «Haufen Code», den sie zur Einsicht erhalten hätten, habe nicht dazu getaugt, das System zum Laufen zu bringen, sagt Reto Koenig, Professor für Computerwissenschaften an der Berner Fachhochschule BFH, der damals das norwegische E-Voting-System untersuchte.

Die Gruppe um Koenig musste improvisieren. Und fand mit einfachen Programmen «einen Bug, der sich tief in der Kryptografie versteckt hatte». Diese Entdeckung warf kein gutes Licht auf den Pionier Norwegen, dessen E-Voting-System damals schon seit zwei Jahren im Einsatz war.

Andere Forscher kamen zu den gleichen Ergebnissen wie das Team aus der Schweiz. Reto Koenig und eine Forschungsdelegation der BFH wurden darauf nach Oslo eingeladen. Ihre Präsentation vor dem internationalen Gremium der OSZE-Wahlbeobachter zeigte Wirkung.

2013 schränkte Norwegen den E-Voting-Betrieb ein. Ein Jahr später wurde das E-Voting-Projekt ganz begraben. Wegen Ängsten aus der Bevölkerung. Und weil es einen politischen Wechsel gab. Dennoch stellt Scytl ihr Geschäft in Norwegen als Erfolgsgeschichte dar. Auf ihrer Website schreibt die Firma: «94 Prozent der Befragten schätzen unser Verfahren als sicher ein.»

Widersprüchliche Aussagen

Wie verträgt sich das Geschäftsgebaren von Scytl mit den hohen Sicherheits- und Transparenzanforderungen des Bundes?

Wie sicher wird das E-Voting-Angebot der Post?

Und was genau ist der Deal zwischen der Post und dem E-Voting-Riesen aus Spanien?

Seit Ende 2014 ist die Post Kundin von Scytl. Man habe sich für einen privaten Anbieter entschieden, «weil eine Eigenentwicklung zu teuer und risikohaft gewesen wäre», sagt ein Sprecher des Staatsbetriebs.

Für Scytl wiederum ist die Schweiz mit ihrer Staatsform der halbdirekten Demokratie einer der wichtigsten strategischen Märkte.

Zum Thema Transparenz und Überprüfbarkeit des Systems machte Scytl widersprüchliche Aussagen. An einer Fachkonferenz mit dem Titel «Swiss Cyber Storm» hielt Jordi Puiggalí, der langjährige technische Leiter von Scytl, 2017 ein Referat. Als ihn ein Teilnehmer fragte, ob Scytl bereit wäre, den Quellcode offenzulegen, antwortete Puiggalí zunächst ausweichend. Dann fügte er an: Eine Offenlegung, also die Scytl-Kernsoftware unter eine freie Lizenz zu stellen, komme für ihn nicht infrage.

Für die Bundeskanzlei gibt es in diesem Punkt jedoch keinen Spielraum für Verhandlungen. In Artikel 7b der Bundesverordnung über die elektronische Stimmabgabe (VEleS) steht: «Jeder und jede darf den Quellcode zu ideellen

Zwecken untersuchen, verändern, kompilieren und ausführen sowie dazu Studien verfassen und diese publizieren.»

Kurz: Alles ist erlaubt, ausser der kommerzielle Handel.

Jeder E-Voting-Anbieter muss sich auf diese Transparenzklausel einlassen. Und jeder, der das System testen will, soll seine Ergebnisse publik machen können, sagt Mirjam Hostettler, Projektleiterin Vote électronique bei der Bundeskanzlei. Das soll vertrauensbildend wirken. Der Begriff «Vertrauen» wird im erläuternden Bericht der Bundeskanzlei mehrfach genannt.

Die Verpflichtung zur Transparenz war auch eine Bedingung in der Ausschreibung der Post, in der Scytl das Rennen machte. «Für Scytl war von Anfang an klar, dass dieses Kriterium Bestandteil der Zusammenarbeit sein wird», bestätigt Sprecherin Gwendolyne Savoy gegenüber der Republik.

Sicher sicher

Zum Thema Sicherheit führt die Post gewichtige Argumente ins Feld, die Bedenken zerstreuen sollen. Anders als im bemerkenswerten Fall der unsicheren Stimmabgabe in Australien soll bei ihrem E-Voting-Angebot die Verifizierung der Stimmbürgerinnen nicht über SMS oder andere digitale Kanäle erfolgen, sondern analog – die Kantone versenden Prüfcodes zur Identifizierung und Verifikation per Briefpost (der Post).

Auch der Systemausfall der Scytl-Technologie in Ecuador ist nicht wirklich relevant für die Schweiz. Davon waren Wahlmaschinen betroffen – in der Schweiz geht es um die Stimmabgabe am Computer zu Hause. Ausserdem wird Scytl den Wahlvorgang in der Schweiz nicht hoheitlich ausführen. De facto soll der Betrieb des E-Voting-Systems bei der Post bleiben, Scytl selbst wird keinen Zugriff auf die Lösung haben, wie die Post bestätigt.

Derzeit lässt die Post ihr E-Voting-Angebot – also das System, das Protokoll, die Software und die Prozesse – von der KPMG, die als Zertifizierungsstelle beim Bund akkreditiert ist, prüfen. Ist die Zertifizierung geschafft, wird der Konzern eine Transparenzoffensive starten – mit der Aufforderung, ihr System zu hacken.

«Öffentliche Intrusionstests» nennt sich dies im Fachjargon. Durch die Offenlegung des Quellcodes, das Bereitstellen eines Testsystems und die Verlockung einer Hackerprämie wird alle Welt eingeladen, die Sicherheit ihres Produkts zu testen. Auch dies verlangt die Bundesverordnung.

Was beim Deal im Dunkeln bleibt

Der Test wird für die Schweizerische Post auch aus Imagegründen entscheidend sein. Denn der Konzern will auf jeden Fall den Eindruck vermeiden, dass die «digitale Demokratie» der Schweiz privatwirtschaftlich betrieben wird. Das E-Voting-System CHVote aus Genf, das 2019 wegen fehlender Zertifizierung nur eingeschränkt eingesetzt werden kann, ist offen und steuerfinanziert. Es ist auf Github abgelegt. Bürgerinnen können es auf dem eigenen Rechner installieren und auf Herz und Nieren prüfen.

Anders bei der Post mit ihrem Partner Scytl. Sie gewährte bisher nur einem kleinen Kreis von Auditoren Zugang zum System.

Im Dunkeln bleibt der Deal zwischen der Post und Scytl. Der spanische Anbieter betonte mehrfach, dass Transparenz ihren Preis habe. Eine Post-Sprecherin bestätigt auf Nachfrage der Republik zwar, man habe keine

Sonderlizenzen bezahlen müssen. Doch wie viel Geld die Post für die Technologie von Scytl bezahlt – darüber schweigt sich der staatsnahe Betrieb aus. Eine Interpellation von SVP-Nationalrat Claudio Zanetti zu diesem Thema ist hängig. Die einzige Zahl, die bisher bekannt ist, sind die 250'000-Franken, die Bund und Kantone für die Durchführung der Intrusionstests aufwenden.

Die Hacker sind bereit – und waren bislang erfolgreich

Die Kritiker werden trotz der vielen Vorkehrungen des Bundes und der Post nicht verstummen. Denn die Nerds haben ein Totschlagargument auf ihrer Seite: Wie können wir wissen, ob die bald zu testende Software am Wahltag im Oktober 2019 auch tatsächlich zum Einsatz kommt – oder eine andere?

«Selbst unter Idealbedingungen wäre das Vertrauensproblem nicht gelöst, da die Bürgerinnen nicht überprüfen können, ob der veröffentlichte Quellcode wirklich verwendet wird», sagt Hernani Marques vom Chaos Computer Club, einer der engagiertesten E-Voting-Kritiker.

Mirjam Hostettler von der Bundeskanzlei lässt dieses Argument nicht gelten: «Die Betreiber müssen bei Updates aufzeigen, welche Funktionen geändert haben. Sind es viele Funktionen, ist eine erneute Zertifizierung fällig.»

Womöglich können wir uns auf eine «Hacker-Show» gefasst machen. Denn Softwareentwickler Marques möchte mit seinen Kollegen das E-Voting-Angebot der Post simulieren und knacken. «Wir können vor laufender Kamera zeigen, wie die Systeme so unterwandert sein können, dass alles dem System nach sauber aufgeht, die Ergebnisse aber trotzdem nicht dem Wählerinnenwillen der an der Simulation beteiligten Gruppe entsprechen.»

Es wäre nicht das erste Mal, dass auf diese Weise E-Voting-Projekte gebodigt werden. Im Fall von Genf hackte 2013 ein Informatiker namens Sébastien Andrivet das System. Daraufhin wurde die individuelle Verifizierbarkeit eingeführt. Nachdem der Chaos Computer Club auch auf dieses System einen Hackerangriff durchführte, verkündete der Kanton Genf einige Wochen später, sein E-Voting-Angebot einzustellen.

Das Dilemma bleibt unlösbar

Deshalb zeigt sich SVP-Nationalrat Franz Grüter auch unbeeindruckt von der Transparenzoffensive der Post: «Unser Land ist nicht darauf vorbereitet, Cyber-Angriffe zu erkennen und abzuwehren.» Der Initiant der Initiative für ein Moratorium gegen E-Voting steht kurz davor, mit der Unterschriftensammlung zu starten. Das Abstimmungskomitee ist breit und bunt: Juso-Präsidentin Tamara Funiciello sitzt ebenso darin wie JSVP-Präsident Benjamin Fischer oder Balthasar Glättli, der Nationalrat der Grünen.

Noch ist eine grosse Mehrheit der Schweizer Bevölkerung gegenüber E-Voting positiv eingestellt. Die wenigsten interessieren sich für die technische Debatte. Laut der letzten Umfrage des Zentrums für Demokratie sei es den meisten egal, ob der Quellcode publiziert werde oder nicht, sagt Politologe Uwe Serdült.

Dennoch ist die Post nervös. Zwar muss sie vorerst noch nicht die Bevölkerung von ihrem Angebot überzeugen. Wohl aber die politischen Verant-

wortlichen in den Kantonen. Und diese mögen E-Voting immer weniger. Der Kanton Zürich überlegt sich einen Rückzug, Glarus hat sein Vorhaben beerdigt, und auch im Aargau sind die Politikerinnen skeptisch geworden. Derzeit sind nur Basel, Fribourg, Neuenburg und Thurgau E-Voting-Partner der Post.

Finden sich aufgrund der wachsenden Zweifel keine Abnehmer mehr, so ist das Projekt E-Voting gescheitert, bevor überhaupt das entsprechende Gesetz angepasst worden ist. Im Wahljahr 2019 würden die meisten Schweizer dann immer noch mit Stift und Papier abstimmen.

Und auch wenn die Überprüfungen und Tests des Post-Produkts einwandfrei sein sollten, zeigt der Fall Scytl ein Dilemma auf: Demokratisch gewählte Regierungen sind auf das Vertrauen ihrer Stimmbürger angewiesen und müssen transparent kommunizieren.

Eine private, profitorientierte Firma, die eine staatspolitisch zentrale Dienstleistung erbringt, möchte ihre Produkte an möglichst viele Kunden verkaufen und dabei Geschäftsgeheimnisse wahren.

Beide Interessen sind letztlich nicht miteinander vereinbar.