Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

Mgmt Summary:

Eingetretene GAUs beim heutigen E-Voting lassen sich nicht managen, genauso wenig wie bei Atomkraftwerken. Wir können versuchen, genügend sichere Systeme zu bauen, die diesen Fall praktisch ausschliessen. Das bedeutet aber einen Neubeginn und das wird viel Geld kosten. Das Dokument zeigt auf, unter welchen Prämissen dies zu erfolgen hätte, damit ein solches Projekt bei Bevölkerung und Fachleuten ankäme.

Inhalt

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

Um diese Frage zu beantworten, muss man folgende Aspekte beachten:

1. Was verstehen wir überhaupt unter IT-Sicherheit bei E-Voting

Die Sicherheit ist ein zentrales Thema bei E-Voting. Das Gegenstück ist das Risiko. Es lohnt sich, die Begriffe etwas detaillierter anzuschauen.

1.1. Sicherheit ist das Gegenstück zu der Summe aller Risiken

Mathematische Grundformel: Um Sicherheit zu erreichen, müssen alle Risiken auf ein Minimum reduziert sein, dass man wirklich von „Restrisiko" reden kann. Ein einziges Risiko, dass dieser Formel nicht genügt, zerstört die Sicherheit. Das Problem ist, ob wir alle Risiken überhaupt erkennen. Dazu braucht es vertiefte Kenntnisse in allen Bereichen der IT. Einzelne Sicherheitselemente decken lediglich einzelne Risiken ab: Die Verschlüsselung mit SSL, sichere Passwörter, gute Kryptoalgorithmen, Popup –Blocker etc. etc. Die Risikofelder und damit auch die Risiken selbst nehmen mit der Anzahl der Mikro-Funktionen zu. Und diese wachsen und wachsen. Die IT Sicherheits-Industrie boomt deshalb auch. Aber wird die **Sicherheit** in der Zukunft **insgesamt** besser oder schlechter?

1.2. Eine genereller Anspruch an Sicherheit setzt eine entsprechende Konzeption voraus

Der Stimmbürger geht davon aus, dass sein gekauftes Endgerät genau die E-Voting Funktionen ausführt, die es soll und insofern sicher ist, als es niemals etwas Destruktives macht oder einem Dritten den gleichen Vorteil gewährt wie dem Käufer selbst. Dabei müsste doch unterdessen jedem klar sein, dass jedes, am offenen Internet angeschlossene Gerät diesem Anspruch niemals absolut genügen kann. Internet Eingriffe durch Cyberkriminalität könnten nur dann ausgeschlossen werden, wenn (1) *jede* der Kommunikationsbeziehungen einwandfrei verschlüsselt ist (2) der Absender *immer* eindeutig identifizierbar und (3) *vertrauenswürdig* ist. Dazu bräuchte es noch die üblichen Sicherheitsvorkehrungen.

Dass diese 3 Bedingungen jetzt und in Zukunft mit der aktuellen Konzeption E-Voting – basierend auf Main Stream-Technologie der untersten Preisklasse- nie eingehalten sind, scheint offensichtlich. Nicht auszuschliessen wäre jedoch, Sicherheit zu erreichen durch **geschlossene VPN-Netze und –Endgeräte** mit sicheren, eindeutigen Zugangsidentifikationen (z.B:SwissID) und gleichzeitiger, lückenloser Überwachung der Sicherheit[1]. Das führt dann direkt zur Frage, wieviel **Geld** wir bereit sind auszugeben für dieses Ziel der Digitalisierung der Demokratie.

1.3. Die vertrauenswürdige Sicherheit und die überprüfbare Mitwirkungspflicht

Die Sicherheit besteht nicht nur aus einer ausgeklügelten Technologie, sondern sie ist in den ganzheitlichen Einsatz eingebettet. Alle Prozessabläufe müssen ebenfalls einer definierten Sicherheitsdoktrin unterliegen. Und die Einhaltung derselben muss vertrauenswürdig, d.h. demokratisch überprüft und überwacht werden können.

[1] S. auch Ansatz „Sichere Lösung" https://www.noevoting.ch/public/downloadable/Sichere%20Lösung.pdf

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

Wer E-Banking macht, weiss, dass die Bank vom Kunden eine Mitwirkungspflicht verlangt. Er muss alles vermeiden, was an Risiken vermeidbar ist. Tut er dies nicht, oder gibt es Hinweise dafür, die er nicht entkräften kann, muss er den Schaden selbst tragen.

Und beim E-Voting? Die **Mitwirkungspflicht** des einzelnen Stimmbürgers bei der Individuellen Verifizierbarkeit ist zwar eine theoretische Pflicht, aber sie kann nicht überprüft werden. Aber anders als beim Fall des E-Banking trägt aber hier nicht der einzelne „Täter" den Schaden, sondern wir als Gesellschaft, und der Staat, der das Vertrauen seiner Bürger verliert. Wenn man diese Mitwirkungspflicht nicht überprüfen kann, so muss man auf sie verzichten. Dann muss aber die Gewährleistung der Sicherheit umso restriktiver überwacht werden können. Ist die Überwachung der Mitwirkungspflicht in der Zukunft realistischer als heute? Das ist eine unsicher zu beantwortende Frage, weil sie einzig von der gesellschaftlichen Entwicklung abhängt. Wenn **Überwachungen auf allen Gebieten** zur Norm werden, weil die Risiken für die kritischen Infrastrukturen nur so bekämpft werden können, so würde eine solche Lösung gut in die Zeit passen. Es gibt aber auch durchaus gegenteilige Bemühungen, gerade wenn es den einzelnen Bürger betrifft. Sollten die obsiegen, wird E-Voting mit dem heutigen Konzept nie genügend sicher werden, dass man dem Resultat absolut vertrauen kann.

1.4. Das Restrisiko ist kein reiner Zufallsprozess: Es gibt Gegner

Oft werden die Risiken der Cyberkriminalität insbesondere bei E-Voting als „Restrisiken" bezeichnet, die es ja immer hat („Es gibt keine 100%ige Sicherheit") und die man gefälligst vergessen sollte, weil man ja sonst gar nichts mehr unternehmen oder aufbauen kann. Auch wird mit dem Schlagwort des „positiven Denkens" oder dem Gespenst der „Angstmacherei" gearbeitet. Dabei wird vergessen, dass die Cyberkriminalität kein Zufallsprozess ist, den man statistisch in den Griff bekäme, weil man empirische Zahlen unterlegen könnte, die die Gefahr zahlenmässig vermeintlich genügend genau beschreiben.

Das Restrisiko bei E-Voting besteht in den Absichten von irgendwelchen **anonymen Mächten**, die unerkannt eingreifen können. Dass diese das können und oft auch wollen, ist in der letzten Zeit genügendem Masse bestätigt worden. Dafür gibt es in der Tat Statistiken. Diese Vorfälle der Vergangenheit sind natürlich nie genau auf unseren Fall des E-Voting CH abgestimmt, aber mit etwas flexiblem Denken kann man die gleiche Art der Kompetenzen und der kriminellen Energie auf unseren Fall anwenden und kommt auf das gleiche Resultat.
Es gibt keinen Grund anzunehmen, dass dieses Risiko in Zukunft kleiner würde. Im Gegenteil. Alle strategischen Studien inkl. die des NDB kommen auf den gleichen Schluss: Es wird schlimmer werden, die Aufwände gegen diese Risiken werden extrem steigen und dennoch keinen absoluten Schutz bieten. Im Schutze der Anonymität leisten sich vor allem Grossmächte und kriminelle Organisationen solche Operationen, welchen mit keinerlei diplomatischen Offensiven begegnet werden kann. Alles wird abgestritten, man kann ja nichts beweisen. Wir erinnern uns an das Handy von Frau Merkel. Glaubt jemand, dass dies ein einmaliger Ausrutscher eines einzelnen Geheimdienstmitarbeiters gewesen ist?

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

1.5. Das Risiko Management beim E-Voting gehört dazu

Die Frage bleibt, was passiert, wenn es passiert? Wie gehen wir mit dem Schadenfall um? Das gehört ebenfalls zur Konzeption der Sicherheit.

Da stellen wir fest, dass man offenbar bundesweit fest von der Annahme ausgeht, dass es nicht passiert. Nichts von Feststellungskriterienkatalog, Aktionsplan, Ressourcenbereitstellung, Schwellwerte für Entscheidungen. Genauso wie man für den Fall „Explodiertes Atomkraftwerk" Tabletten an die Bevölkerung zur Beruhigung verschickt hat, beschränkt sich das Risikomanagement „E-Voting" auf die **lapidare Feststellung**, „einige Leute werden es schon merken und dann gibt es eine Untersuchung". Womit dann effektiv gerechnet werden muss, steht in diesem Beitrag[2].

[2] S. auch Szenarien einer Manipulation in 4 Phasen
https://www.noevoting.ch/public/downloadable/arg_d/Szenario%20Manipulation.pdf

2. Was tut die IT Branche für die Sicherheit?

Das Vertrauen in die IT Branche kennt kaum Grenzen. Jeder einzelne User ist beeindruckt vom dynamischen Tempo der funktionellen Erneuerungen, der gigantischen Leistungsverbesserungen und das bei sinkenden Preisen. Keine andere Branche hat in den letzten Jahrzehnten so viel hervorgebracht. Es lohnt sich dennoch, die Grenzen dieser Entwicklung auszuloten.

2.1. Entwicklung der Sicherheitstechnik

Die rasante Entwicklung vor allem der Browser-Technologie hat einen grossen Teil des Erfolgspotentials der IT ausgemacht. Der User braucht kein spezielles (Client-Server) Programm mehr zum Zugriff auf eine Applikation, die er selber ebenfalls nicht immer auf dem eigenen Rechner installieren muss. Der Browser kann alles. Auf dem Browser installieren sich lokale kleine Programme, die alle möglichen beliebten Funktionalitäten des Benutzers implementieren. Mit vielen Schaltern kann man diese steuern, denn man weiss, genau dort kommen auch die Schadcodes am einfachsten hinein. Man kann restriktiver oder offener operieren. Ist man zu restriktiv, funktioniert die Applikation vielleicht nicht 100%ig, ist man zu offen, hat man weniger Schutz gegen Schadcode. Der Benutzer entscheidet selbst, meist für die sog. Standard-Einstellung, die gewährt durchschnittlich die beste Funktionalität mit dem wenigsten Ärger. Aber von “sicher“ kann keine Rede sein.

Natürlich muss der Browser immer wieder erneuert werden, denn neue Features verlangen neue Funktionalitäten. Aber der Browser macht das u.U. selbst, man hat nicht unbedingt etwas damit zu tun. Man verliert als User nur halt eben die Kontrolle völlig über die Sicherheit, denn im neuen Update sind zwar vielleicht einige alte Schwachstellen gefixt, aber garantiert auch wieder einige neue dabei. Das führt zur optimalen Zufriedenheit des Benutzers, denn um die alten hat er sich vielleicht gesorgt, die neuen kennt er ja (noch) nicht. Das heisst nichts weniger, dass nicht nur der normale User **keine Kontrolle** mehr hat, auch der **Fachmann** kann dieser Entwicklung nicht mehr im Detail folgen. Nur die allerwenigsten, hauptsächlich die Leute im Labor des Herstellers haben da noch eine Kontrolle. Die Frage ist einfach, kann man denen vertrauen und das auf alle Zeiten hinaus?

2.2. Anspruchshaltung des Kunden und die Absicherung des Lieferanten

Als Kunde will ich natürlich die Gewährleistung aller Neuerungen haben und der Lieferant garantiert mir alle Updates unter Umständen auch gratis. Was er mir nie garantiert, ist, dass irgendeine Version sicher oder ohne Fehler ist. Ich nehme das hin, weil ich gar keine Alternative dazu mehr habe. Ich mache den Haken unter die „AGB“ und kann die neue Version installieren. Das Lesen dieser langen AGB tut sich kaum jemand an. Dort **lehnt** der Lieferant jedwede **Verantwortung** für Probleme **ab**, die sich ergeben könnten durch die Installation. Ob diese Ablehnung aber jeweils mit dem nationalen Recht kompatibel ist, wird nur ganz selten untersucht und angesprochen.

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

2.3. Die Rechtslage wird in der EU strikter, aber wohl kaum durchsetzbar

Insbesondere in der Frage des Datenschutzes kommen Ansprüche des Users auf, die vom Gesetzgeber insbesondere in der EU neu gestützt werden sollen. Flugs haben alle Anbieter diese AGB entsprechend angepasst, dass der Text, den keiner liest, juristisch nicht angreifbar wäre, wenn es doch einer täte. Wie der Gesetzgeber das Recht durchsetzen will, bleibt oft im Dunkeln, und man hat den Verdacht, es geht hier nur um die Etikette. In Tat und Wahrheit hört man kaum von Anstrengungen, Verstösse zu verfolgen und zu ahnden. Zu aufwendig, langwierig und ohne Anreiz für den Kläger ist die Entdeckung eines Einzelfalles, den man ja haben müsste, um vor Gericht erfolgreich zu sein. Zudem ist die Verwicklung meist international und wenn schon die Regelung sehr **schwierig bis aussichtslos** ist, wie steht es dann um Beweisführung und Durchsetzung?

2.4. Interessenslage des Herstellers

Natürlich ist der Hersteller interessiert am Umsatz, d.h. auch an der Kundenzufriedenheit. Natürlich kann er sich nicht leisten, mit schlechter Qualität aufzufallen. Die Frage ist nur, ob die schlechte Qualität nur durch Fehlfunktionen auffällt, oder ob da nicht auch unsichtbare Fehlfunktionen die Sicherheit beeinträchtigen, d.h. Dritten mit irgendwelchen Tricks unerlaubte Zugänge verschaffen.

Man weiss, dass Informationen über solche Schwachstellen für teures Geld auch den Geheimdiensten verkauft werden können. Das Perfide daran heute ist, dass solche Operationen auch so zeitlich begrenzt sein können, dass der update, der diesen absichtlich eingebrachten Bug wieder fixt, schon in der Pipeline ist und unmittelbar nach der geplanten Operation erfolgt und von den Benutzern automatisch übernommen wird. Spuren eines solchen Falles sind vor ca. 4 Jahren aufgetreten (SSL). Natürlich würde man dies nie öffentlich zugeben und im Fall wo es auffliegt, wäre es immer die Tat eines Einzelnen oder eines Dritten. Der Ruf der Firma muss unter allen Umständen geschützt werden. Mit Sicherheit gibt es da auch Kräfte, die diese Art Korruption bekämpfen. Die Frage ist einfach, kann man darauf **vertrauen**, dass diese stets die Oberhand behalten und das auf alle Zeiten hinaus?

2.5. Die Sicherheitsindustrie boomt, die Nachfrage ist grösser als das Angebot

Diese obigen Tatsachen sind der Sicherheitsindustrie bekannt und sie produziert auf vollen Touren. Dutzende Antivirenhersteller verzeichnen Markt-Erfolge, sind dynamisch unterwegs und liefern immer wieder schnell Abwehr-Hilfsmittel gegen erkannte Bedrohungen. Die sog. „Zero-Day-Infections“ zeigen an, dass eine bekannte Schwachstelle innert weniger als einem Tag ausgenutzt werden muss, weil der dazugehörige Exploit ansonsten von der Erneuerung des Virenschutz bereits wieder erkannt wird.

2.6. Wo sind die Grenzen der Sicherheitsindustrie?

Nicht jeder Exploit ist jedem Hersteller von Antivirenprogrammen bekannt, und so gibt es immer wieder zusätzliche Lücken, die ausgenutzt werden können, je nachdem, welchem Hersteller man vertraut. Zu jeder noch nicht gefixten Schwachstelle kann auch jederzeit mit wenig Aufwand vom Kriminellen ein neuer Exploit gebaut werden, der wieder einen Tag Wirksamkeit hat. Zudem ist nicht jeder Fix, der publiziert wird, so gut, dass die Schwachstelle nicht doch noch irgendwie anders genutzt werden könnte.

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

Und jetzt kommt noch zu alledem hinzu, dass nicht alle Entdecker von Schwachstellen „Good Guys“ sind und die neuen Entdeckungen in die jährlich 10000 Fälle umfassenden NIST[3] Tabelle einfüllen. Man muss sehr wohl befürchten, dass es eine **Dunkelziffer von Schwachstellen** gibt, die zu einem Spezialpreis an Spezial-Organisationen verkauft werden. Die werden dann bei den Eingriffen verwendet, die jahrelang unerkannt bleiben, so wie jene der RUAG und des EDA.

[3] National Institute of Standards and Technology

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

3. Welche Rolle spielt dabei die Politik?

Die Einflussnahme der Politik in die Wirtschaft ist hierzulande geprägt von der Frage nach den Arbeitsplätzen, der Rahmenbedingungen des Staates und der regionalen Konkurrenz. In den Staaten, wo die Main-Stream-IT entwickelt wird, geht es auch und vor allem um Sicherheit und Machtansprüche. Die weltweite Cyberkriminalität ist dann oft auch nicht mehr einwandfrei davon zu trennen.

3.1. In den USA und bei anderen Grossmächten herrscht ein anderes Verständnis der Sicherheit

Das US-Verständnis der Sicherheit wird vor allem durch 9/11 geprägt. Damals wuchs die Einsicht, dass dem Terrorismus nur mit den modernsten Mitteln der Cyberattacken erfolgsversprechend begegnet werden kann. Alles was diesem Ziel widerspricht, wird bekämpft. Ja sogar, Einführung von sicherer Kryptologie in die USA wird verboten, weil sie nicht erlaubt, Kommunikation zu entschlüsseln, also diesem Sicherheitsziel widerspricht. Die Fähigkeit und der **Wille zur Auskundschaftung** macht auch nicht Halt vor befreundeten Nationen, wie wir seit Edward Snowden wissen. Man kann davon ausgehen, dass die Situation in Russland und China genau so ist und künftig darf erwartet werden, dass auch kleinere Staaten sich auf diesem Gebiet versuchen werden.

3.2. Fähigkeiten zum Angriff sind wesentlich billiger als die Sicherheit

Die Tatsache, dass der Angreifer eine einzige Schwachstelle finden muss, der Verteidiger aber alle Schwachstellen kennen und beseitigen muss, führt bei der strategischen Beurteilung eines optimalen Mitteleinsatzes direkt zur amerikanischen Haltung.

Daraus ist auch abzuleiten, dass die Verteidigung der Cyber-Sicherheit – insbesondere bei der Main-Stream-Technologie- viel teurer ist als der Aufbau einer Angriffsfähigkeit. Deshalb ist es sinnlos, zu meinen, mit etwas Aufwand in der Kryptologie bei E-Voting sei der **Preis für den Angreifer** zu hoch, so dass sich ein Angriff nicht lohne. Das gilt höchstens für den Schutz gegen Hobby-Hacker.

3.3. Die weltweite cyberkriminelle Szene

Die kriminelle Szene, die normalerweise keinen staatlichen Schutz geniesst, funktioniert grundsätzlich wie ein gewöhnlicher Wirtschaftszweig und erwirtschaftet mit Cyberattacken Milliarden über Geldwäsche und Erpressungen sowie illegalen Angeboten an Waffen oder „Dienstleistungen“. Das E-Voting bietet nun ein **neues Geschäftsfeld**, das sich natürlich noch entwickeln muss und auch einige Risiken birgt, womöglich aber bedeutend weniger Risiken als die übrigen Bereiche. Diese Szene arbeitet im sog. Dark-Net und geniesst so den Schutz der Nicht-Erkennung des Standortes. Nur aufwendige internationale polizeiliche Operationen mit gefälschten Kunden können ab und zu solche Täter entdecken und festnehmen. Solche kommen aber nur zustande, wenn die Täter Fehler begehen und die internationale Zusammenarbeit einwandfrei funktioniert, was sehr selten der Fall ist, weil die **Interessenslage** nicht immer eindeutig und kohärent ist. Da das Internet global ist, kann man sich als Krimineller auch in Gebiete zurückziehen, wo es kaum einen funktionsfähigen Staat gibt.

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

4. Wie viel Geld wollen wir für welche Sicherheit ausgeben?

Wenn wir die amerikanische Einsicht ignorieren oder ablehnen und versuchen, Sicherheit herzustellen und diese mit dem Rechtsstaat so weit wie möglich zu verteidigen, so stellt sich in erster Linie diese Frage.

4.1. Die Sicherheits-Industrie und deren Standards

Wenn der Fachmann Sicherheit an einem Objekt produzieren will, so orientiert er sich an den gängigen Standards, wie z.B. ISO 27001. Dort wird beschrieben, welche Massnahmen alle bekannten funktionellen Schwachstellen erfordern, um dem Standard zu genügen. Wenn man keine Massnahme ergreift, so muss man begründen, warum und beschreiben, welchen Einfluss das auf die Sicherheit des beschriebenen Objekts haben wird.

Da es Hunderte solche Vorschriften gibt, die man zu jedem Objekt anwenden muss, wird ein solches „Sicherheits-Konzept" genanntes Dokument rasch unübersichtlich und komplex. Wenn es aber gut gemacht ist, sind die Hauptrisiken explizit aufgelistet und ein Plan mitgegeben, wie diese einzeln bekämpft, eliminiert, minimiert oder getragen werden.

Dieses Dokument ist dann geheim, denn es bietet einem Angreifer eine optimale Vorlage. Geheim ist aber das Gegenteil von transparent und deshalb für E-Voting ungeeignet[4]. Das Aufzeigen der Risiken führt sofort zu unterschiedlichen Beurteilungen über die Tragbarkeit und damit zum Politikum. Kein Wunder, dass man versucht, die Herausgabe von solchen Dokumenten zu vermeiden[5]. Das Nicht-Aufzeigen ist aber entweder eine unprofessionelle Vorgehensweise oder ebenfalls **nicht transparent für den Bürger**. Was also tun?

4.2. Die objektive und die relative Sicht der Sicherheit

Objektiv gesehen, könnte man die Sicherheit am besten am Sicherheitskonzept messen. Welche Risiken sind wie gut abgedeckt, das kann ein Fachmann damit beurteilen. Besser wäre ein Gemisch von mehreren unterschiedlichen und vor allem unabhängigen Fachleuten, die sich einigen müssen. Schlecht ist es, wenn ein Vorgesetzter für das Zustandekommen des Projektes gleichermassen verantwortlich ist wie für die Sicherheit. Leider passiert genau das letztere in allen Unternehmen und auch in allen Ämtern der Verwaltung. Es hängt dann vom **Empfinden dieses Chefs** ab, ob er dem Gesamtresultat vertraut. Dabei kann er sich auf seine eigene Erfahrung sowie auf seine Einschätzung der Qualität seiner Mitarbeiter abstützen. Aber ist er so wirklich frei in seinem Entscheid? Gibt es in unserer Kultur ein Recht auf Scheitern? Fällt ein negativer Entscheid nicht als Tadel auf ihn selbst zurück? Können wir das in der Zukunft ändern?

Eine andere Sicht ist die relative Sicht. Man misst dabei den Aufwand und die Schadenfälle und stellt fest, inwiefern die Zunahme des ersteren zur Abnahme des zweiten führt. Dabei müsste man aber realistische Zahlen über beides haben. Beim **E-Banking** kann man das sehr wohl machen: Der Aufwand ist messbar und der Schaden auch. Es liegt einzig an der

[4] https://www.noevoting.ch/public/downloadable/arg_d/Transparenzanspruch.pdf
[5] https://www.noevoting.ch/public/downloadable/arg_d/Zugangsgesuch.htm

betreffenden Bank, ob sie qualitativ in der Lage ist, diese Messgrössen genügend genau zu messen. Aber sicher ist, dass es voll im Interesse der Bank liegt, diese Messgrössen zu kennen. Aber wie ist es beim **E-Voting**? Messgrössen auf der Kostenseite sind schon äusserst schwierig zu erheben[6], bei den Schadenfällen ist es geradezu unmöglich (s. Verweis von 1.5). Die Aussage, bei den bisherigen 200 Abstimmungen seien keine Schadenfälle bekannt geworden, ist ohne jeglichen Wert für die Beurteilung der Sicherheit oder die Beurteilung der künftigen Risiken[7]. Es liegt **nicht im Interesse der Verwaltung** aufzuzeigen, welche möglichen Ungereimtheiten diese Abstimmungen möglicherweise begleitet haben. Zweifel an Abstimmungen wären Gift für das Vertrauen in den Staat. Die Staatsräson spricht da eine klare Sprache.

4.3. Sichererer IT Betrieb kostet viel Geld

Der sog. sichere Betrieb in der Industrie und Verwaltung wird normalerweise gemäss objektiver Sicherbeurteilung (3.2) geführt und dokumentiert. Nicht zu vermeiden sind in der Realität meist folgende Differenzen zu der geplanten und dokumentierten Sicherheit: Ressourcenprobleme, Lieferprobleme, technische Probleme mit den Produkten, Budgetprobleme, suboptimale Besetzungen von Schlüsselpositionen.

Ob diese Probleme professionell ausreichend oder eher nur mit minimalem Aufwand gelöst werden, hängt nicht zuletzt von den finanziellen Möglichkeiten und den strategischen Sicherheitsansprüchen der Unternehmung oder des Amtes ab. Eine normale politische Kontrolle würde wohl die Folgen einer derartigen Misslichkeit normalerweise nicht beurteilen können. Sollte man aber, wie teilweise neu angedacht, ein **Cyber Security Zentrum** einrichten, welches fachmännisch genügend **ausressourciert** ist und **Kompetenzen** hat, könnte eine solche Kontrolle wirksam sein.

Und wie steht es konkret beim E-Voting? Die verschiedenen Kantone haben natürlich unterschiedliche Budgets und beurteilen den Kosten/Nutzen Faktor darum unterschiedlich. Schätzungen mit Vergleichen aus der Bundesverwaltung ergeben einen Gesamtaufwand für Bund und Kantone von ca. 80 - 160 Mio SFr. pro Jahr. Für den einzelnen Kanton dürfte eine 7 stellige Zahl resultieren. Die Kostenaufteilung zwischen Bund und Kantonen ist offenbar noch nicht geregelt. Dabei sind die 18jährigen Projektkosten noch gar nicht gerechnet. Das ergibt pro Abstimmung einen E-Zusatzaufwand von ca. 4-8 SFr. pro Stimmbürger. Wenn nur ¼ der Stimmbürger E-Voting machen, zahlen entweder die andern den Preis als Steuerzahler mit oder man müsste denen ca. 16-32 SFr. verrechnen, die es nutzen wollen. Vielleicht würde es dann gar niemand mehr nutzen wollen. Durch die Zurückhaltung mit Kostenangaben in der Verwaltung hat man den Eindruck, es interessiert sich in der Verwaltung kaum jemand für genaue, realistische Zahlen für E-Voting. Die Aussicht nach einem vermeintlichen Prestige-Gewinn scheint alle rationalen und wirtschaftlichen Überlegungen zu überstrahlen.

[6] Projekt- und Betriebskosten beim Bund und den Kantonen
[7] https://www.noevoting.ch/public/downloadable/SPK-Argumente.pdf

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

4.4. Wie sicher sind „sichere Systeme“?

Bei allen IT-Sicherheitsprojekten gibt es einige Schlüsselpositionen, welche eine besonders grosse Verantwortung für die Sicherheit tragen. So hat z.B. ein Administrator immer Zugang zu den Systemen, wenn auch nicht zwingend zu allen Daten. Damit könnte er Prozeduren manipulieren, selbst wenn er die einzelnen Daten nicht lesen kann[8]. Er kann es u.U. sogar unabsichtlich machen, wenn ein Dritter auf Lieferanten-Seite ihm z.B. Updates liefert, welche einen Schadcode oder eine Schwachstelle produzieren, mit dem nachher eine Manipulation ausgeführt wird. Je nachdem, wo Schlüsselcodes abgelegt werden, kann durch die Kopie solcher geheimer Schlüssel auch ein unerlaubter Zugriff auf Daten erfolgen. Alles ist möglich, wenn eine einzige Schwachstelle ausgenutzt wird. Das kann, aber das muss nicht unbedingt auffliegen.

Wie könnte man diesem Risiko begegnen? 2-3 Administratoren müssten sich jeweils gegenseitig überprüfen. Das gilt dann auch für alle anderen Schlüsselstellen: Redundante Besetzung von allen Schlüsselstellen, wie bei den Nuklear-Streitkräften mit dem roten Knopf.

Aber wird man das in der Verwaltung tun? Man wird vielleicht geheime Schlüssel an verschiedene Personen abgeben und sie verknüpfen. Das deckt dann wenigstens die direkte unberechtigte Entschlüsselungsgefahr ab. Für die meisten übrigen Risiken wird das wohl - ohne starken politischen Druck in dieser Richtung - als eine übertriebene Massnahme gesehen.

Was müsste man tun bei E-Voting? Es ist leicht erkennbar, dass die Sicherheitsansprüche hier den höchsten Anforderungen genügen müssten. Diese Anlage müsste personell, örtlich, und administrativ getrennt sein von allen anderen IT Anlagen und zudem die redundante Besetzung aller Schlüsselpositionen. Ohne starken politischen Druck in dieser Richtung kann man aber wohl auch hier nicht davon ausgehen, dass das so sein wird.

[8] Man denke an den ehemaligen Mitarbeiter des NDBs, der geheime Daten zum eigenen Vorteil verkauft hat und von der eigenen Organisation nicht entdeckt wurde.

Was sind die Zukunftsaussichten? Wird E-Voting sicherer werden?

5. Schlussfolgerungen

Wie gezeigt wurde, lassen sich eingetretene Risiken beim heutigen E-Voting nicht managen. Dies könnte zur Folgerung führen, dass wir halt genügend sichere Systeme bauen müssen, die diesen Fall praktisch ausschliessen. In diesem Fall kann man von folgenden einzuhaltenden Prämissen ausgehen:

- Die Systeme werden in der Zukunft auf keinen Fall „von selbst“ sicherer.
- Die heutige Konzeption muss durch eine völlig neue ersetzt werden („zurück auf Feld 1“). Hauptschwachstelle Benutzergerät muss ersetzt werden durch Spezialgerät.
- Es wird deutlich mehr Personal brauchen, vor allem bei der Gewährleistung der zentralen Sicherheit, was beim heutigen Fachkräftemangel ein Problem sein wird
- Es wird viel Geld in die Umsetzung der Sicherheit fliessen
- Eine vom Projekt und der übrigen Verwaltung unabhängige staatliche Stelle – kompetent in Cyberbedrohungen- beurteilt das Projekt mindestens in der Konzeptphase und den Betrieb einer solchen Anlage. Sie muss die Möglichkeit haben, den Betrieb teilweise oder ganz auszusetzen oder abzulehnen. Sie führt aber das Projekt nicht.
- Es muss Transparenz bei Sicherheit und Kosten sowie bei Vorfällen geschaffen werden, damit das Vertrauen der Bevölkerung und auch eine eigene Sicht des Kosten/Nutzenverhältnisses hergestellt werden kann.

Können diese Prämissen alle eingehalten werden, hat ein E-Voting in der Zukunft auch bei Fachleuten eine Akzeptanz-Chance. Mehrheitsfähig wäre es aber nur dann, wenn die Kosten-Nutzenfrage einigermassen eingeschätzt werden kann und zur Zufriedenheit ausfallen würde. Möglicherweise auch dann noch mit kantonal unterschiedlichen Entscheidungen.

Bleibt man auf dem Standpunkt: „Sicher ist es zwar nicht, aber wir machen ja auch E-Banking“, so wird der Graben in der Bevölkerung auch bestehen bleiben.