3.3. Variante «PROVEN» [L3]

Ganzheitliches Sicherheitskonzept E-Voting wird vorgängig öffentlich begutachtet und durch ausgewiesene Cyber-Experten grossmehrheitlich akzeptiert. Kantone erhalten konkrete Auflagen. Heutiger Testbetrieb wird bis zur Umsetzung eingestellt.

[1)]Der Bund kann Einschränkungen für die Nutzung von E-Voting erlassen.

[2)]Der Bund legt im Zeitraum von [18 Monaten] ein **ganzheitliches Sicherheit-Konzept** für die reguläre Einführung von E-Voting vor, bei dem zumindest [90%] der ***involvierten und interessierten*** Cyber-Fachexperten die Wirksamkeit der Massnahmen in Bezug auf eine absolute Vertrauenswürdigkeit des Wahlergebnisses attestieren.

[3)]Die Kantone kriegen Auflagen zur Beaufsichtigung, Überwachung und forensische Nachverfolgung bei Unregelmässigkeiten durch die zentrale Bundesstelle «Cyber Defence».

[4)]Diese Sicherungs-Massnahmen enthalten insbesondere auch die Sicherung der Nachvollziehbarkeit aller Eingriffe in das E-Voting System (inkl. Plattformen), Personensicherheitsüberprüfungen, Massnahmen gegen Social Engineering, ein Incident-Management, den Betrieb und die Sicherung der Druckzentren, welche die Codes ausstellen und die Errichtung eines Service-Zentrum für die Belange der Sicherung der Nutzer-Endgeräte.

[5)]Zuständigkeiten und Umfang der genannten Aufgaben werden öffentlich bekanntgegeben. Die Stellen sind verpflichtet, den Nachweis der Umsetzung zu erbringen. Alle Unregelmässigkeiten und deren Gegenmassnahmen sind jeweils zu veröffentlichen.

[6)]Das Konzept enthält auch die Kriterien über die An- oder Aberkennung der Wahl oder Abstimmung bei Auftauchen von Unregelmässigkeiten und Ergebnissen von forensischen Untersuchungen, sowie die mögliche Zeitverzögerung der Anerkennung durch solche Aktivitäten.

[7)]Der gegenwärtige Testbetrieb eingestellt und wird erst NACH der Umsetzung der konzipierten Massnahmen wieder aufgenommen.

[8)]Eine reguläre Einführung von E-Voting erfolgt, nachdem sich der neue Testbetrieb etabliert hat und die postulierten Ressourcen vorhanden und erfolgreich operativ sind.

[9)]Die Massnahmen werden periodisch von einem Fachgremium überprüft und falls nötig, verschärft. Das Fachgremium enthält zwingend auch unabhängige Cyber-Spezialisten.

[10)] Eine Betriebs-Vollkostenrechnung für E-Voting ist zu erstellen und zu veröffentlichen.

[11)]Wenn in der genannten Frist kein Papier zur Verfügung gestellt werden kann, das die genannten Bedingungen enthält, wird das Projekt E-Voting aufgegeben. Falls ja, ist das E-Voting in dieser Form per Volksabstimmung zu genehmigen.

Vorteile	Nachteile
Vertrauen unter Fachleuten kann am ehesten geschaffen werden, wenn über alle Schwachstellen und Gegenmassnahmen offen diskutiert wird. Evtl. stabilisieren sich damit auch die Mehrheitsverhältnisse in Volk und Parlament in Bezug auf die Akzeptanz oder Ablehnung von E-Voting.	Bei Offenlegung aller Schwachstellen und Gegenmassnahmen erhöht sich das Risiko für erfolgreiche Angriffe. Eine akzeptable Lösung wird sehr langwierig und sehr teuer werden. Ressourcenmangel droht. Die POST und die Kantone werden erhebliche Zusatzmittel vom Bund verlangen. Kantone verlieren ihre Autonomie. Die Transparenz der Vorgänge kann das Vertrauen auch erschüttern. Die Abhängigkeit von hochgradigen Spezialisten wird unumgänglich

Zuerst Sicherheit konzipieren und umsetzen und erst dann einführen!