Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Vote électronique
Anforderungen von Bund und Kantonen zu öffentlichen Intrusionstests

Gemäss Beschluss des Steuerungsausschusses Vote électronique vom 29. Oktober 2018 gelten für öffentliche Intrusionstests die folgenden Anforderungen:

1. Die Systemanbieter ermöglichen einen öffentlichen Intrusionstest für ihr System.

2. Er dauert mindestens 4 Wochen (Dauer eines Urnengangs).

3. Teilnehmende aus der ganzen Welt können das System testen.

4. Die Teilnehmenden müssen das System angreifen dürfen: Versuche müssen erlaubt sein, Stimmen zu manipulieren, abgegebene Stimmen zu lesen, das Stimmgeheimnis zu brechen, sowie Sicherheitsvorkehrungen ausser Kraft zu setzen oder zu umgehen, die die Stimmen und sicherheitsrelevante Daten schützen.

5. Teilnehmende dürfen ihre Erkenntnisse aus dem Test publizieren.

6. Die Systemdokumentation sowie der Quellcode müssen vorgängig auf dem Internet publiziert werden. (Dabei gelten die Bestimmungen gemäss VEleS Art. 7*a* f.) Als Testmaterial erhalten die Teilnehmenden eine hinreichende Zahl von Stimmrechtsausweisen. Diese können elektronisch zugestellt werden.

7. Die Rückmeldungen der Tester gehen bei einem von Bund und Kantonen bestimmten Dienstleister ein. Dieser bewertet die Rückmeldungen und nimmt zu ihnen sobald als möglich Stellung. Die Systemanbieter leisten dem Dienstleister dabei Unterstützung.

8. Als Voraussetzung für die Testteilnahme können die Systemanbieter Teilnahmeinteressierte verpflichten, sich zu einem Verhaltenskodex zu bekennen. Dieser könnte folgende Obliegenheiten umfassen:

    a. Unterlassen von Angriffen, die vom Test ausgeschlossen sind;
    b. Umgehende Meldung von gefundenen Mängeln;
    c. Zuwarten mit der Publikation der Beschreibung von gefundenen Mängeln, bis der Systemanbieter festgelegt hat, wie mit dem Mangel umzugehen ist.

9. Ausgeschlossen vom Test sind:

    a. Angriffe, die darauf abzielen, mit lastbasierten Angriffen die Stimmabgabe zu verunmöglichen (distributed Denial-of-service);
    b. Angriffe, die darauf abzielen, via gefälschte Nachrichten die Akteure dazu zu bringen, von den vorgesehenen Prozessen abzuweichen (Social-Engineering);
    c. Angriffe, die darauf abzielen, Stimmen zu manipulieren, sofern der Angriff mit Hilfe der individuellen Verifizierbarkeit erkannt werden kann.
    d. Angriffe, die darauf abzielen, Stimmen zu lesen, indem Malware auf die zur Stimmabgabe verwendeten Geräte verbreitet wird;
    e. Angriffe auf Dienstleistungen des Systemanbieters, die nicht mit E-Voting in Verbindung stehen;
    f. Angriffe auf das System zum elektronischen Versand der Stimmrechtsausweise.

10. Eine Einwilligung der Systemanbieter in den Test schützt die Teilnehmenden vor Strafverfolgung, sofern die Angriffe aus dem Test nicht ausgeschlossen sind.