Q&A

Öffentlicher Intrusionstest von Vote électronique

1. Darf der Bund Hackerangriffe finanziell entschädigen?

Die Schweizerische Post ist für die Entschädigungen für Meldungen von Sicherheitslücken zuständig. Sie legt die Höhe der Entschädigungen fest und zahlt diese aus. Der Bund und die Kantone leisten über den Schwerpunktplan von E-Government Schweiz einen Beitrag von CHF 250'000.- an die Durchführung des öffentlichen Intrusionstests.

2. Soll der öffentliche Intrusionstest beweisen, dass E-Voting nicht gehackt werden kann?

Nein. Der Intrusionstest hat zum Ziel, dass Schwachstellen aufgedeckt und wenn nötig behoben werden. Darüber hinaus ist es im Sinne der Transparenz, wenn sich möglichst viele unabhängige Fachpersonen im Bereich der E-Voting-Sicherheit auskennen. Der öffentliche Intrusionstest könnte für sie ein Anlass sein, sich mit E-Voting zu befassen.

3. Es liegt also in der Verantwortung von unabhängigen Fachpersonen, dass alle Schwachstellen aufgedeckt werden?

Nein. Der öffentliche Intrusionstest ist eine Sicherheitsmassnahme unter vielen. Jedes IT-System hat Schwachstellen, das wird bei E-Voting auch nach dem öffentlichen Intrusionstest der Fall sein. Entscheidend ist, dass keine Schwachstelle ein grösseres Risiko begründet. Schwachstellen müssen Sicherheitsmassnahmen gegenüber stehen, die hinreichend wirksam sind. Mit der vollständigen Verifizierbarkeit kennt E-Voting eine umfassende und besonders wirksame Sicherheitsmassnahme, die es für andere Dienstleistungen nicht gibt. Darüber hinaus werden die Systeme regelmässig von einer akkreditierten Stelle auditiert und zertifiziert.

4. Für die vollständige Verifizierbarkeit braucht es auch Computer. Gibt es auf diesen Computern denn keine Schwachstellen?

Vollständige Verifizierbarkeit bedeutet im Wesentlichen, dass die Manipulation einer einzelnen Komponente nicht ausreicht, um unbemerkt Stimmen zu fälschen. Wird eine einzelne Komponente manipuliert, stehen weitere Komponenten zur Verfügung, dank denen ein Fälschungsversuch entdeckt werden kann.

5. Wie schlimm muss die Schwachstelle sein, damit ihre Meldung entschädigt wird?

Der Schweregrad einer Schwachstelle ist dafür nicht massgeblich. Vielmehr ist entscheidend, dass sich die Teilnehmer beim Testen an die Spielregeln halten. Grundsätzlich sind alle Angriffe erlaubt und erwünscht, die mit Blick auf die Sicherheit der Stimmen einen Erkenntnisgewinn bringen könnten. Angriffe, die sich lediglich dazu eignen, bekannte Schwachstellen zu illustrieren, werden nicht entschädigt. Einige Angriffe sind sogar verboten, obwohl sie durchaus mit einem relevanten Risiko verknüpft sind. Um diese Risiken unter Kontrolle zu halten, stehen jedoch wirksamere Mittel zur Verfügung als der öffentliche Intrusionstest.

6. Welche Angriffe werden ausgeschlossen?

Zugelassen und entschädigt werden erfolgreiche Angriffe auf die E-Voting Infrastruktur der Post. Andere Organisationen (Kantone, Druckereien, weitere Dienstleistungen der Post) nehmen am öffentlichen Intrusionstest nicht teil, dementsprechend dürfen sie auch nicht angegriffen werden. Zudem sind lastbasierte Angriffe (distributed Denial-of-service) verboten, da sie im Rahmen eines öffentlichen Intrusionstests keine neuen Erkenntnisse bringen, auch anderweitig getestet werden können und ausserdem den Ablauf des Tests stören würden. Ebenfalls keine Entschädigungen werden für Angriffe auf die Benutzerplattformen der Stimmberechtigten ausgesprochen. Dasselbe gilt für jegliche Angriffe, die darauf abzielen, via gefälschte Nachrichten die Akteure dazu zu bringen, von den vorgesehenen Prozessen abzuweichen (Social-Engineering). Erfolgreiche Angriffe machen sich ein Fehlverhalten der Akteure zunutze, das im Rahmen eines öffentlichen Intrusionstests nicht realitätsgetreu simuliert werden kann. Dennoch: Das Brechen der individuellen Verifizierbarkeit (ein «Ja» wird abgegeben und ein «Nein» angezeigt), so dass die Stimmenden keine Möglichkeit haben die Manipulation festzustellen, wird entschädigt.

7. Lernen dank dem öffentlichen Intrusionstest nicht auch Angreifer, wie man E-Voting hacken könnte?

Eine Schwachstelle könnte statt den Veranstaltern einem potentiellen Angreifer gemeldet werden. Das ist unproblematisch, sofern die Veranstalter über die Schwachstelle ebenfalls Kenntnis erhalten und sie bei Bedarf beheben. Die von der Post in Aussicht gestellte Entschädigung bildet einen Anreiz, Schwachstellen (auch) den Veranstaltern zu melden. Darüber hinaus können illegale Versuche, Schwachstellen zu finden, auch unabhängig vom öffentlichen Intrusionstest vorgenommen werden. Der öffentliche Intrusionstest erlaubt es hingegen auch wohlmeinenden Akteuren, das System eingehend auf Schwachstellen zu untersuchen.

8. Weshalb wird E-Voting bereits angewendet, wenn das System noch keinem Intrusionstest unterzogen wurde?

Bei dem System, das nun für einen öffentlichen Intrusionstest zur Verfügung gestellt wird, handelt es sich um das erste System mit vollständiger Verifizierbarkeit. Die heute im Einsatz stehenden Systeme bieten noch keine vollständige, sondern die individuelle Verifizierbarkeit. Da die vollständige Verifizierbarkeit den breiteren Einsatz von E-Voting erlaubt, muss ein solches System noch höhere Sicherheitsanforderungen erfüllen. Diese umfassen unter anderem eine Zertifizierung sowie die Offenlegung des Quellcodes. Zusätzlich haben Bund und Kantone entschieden, dass vollständig verifizierbare Systeme vor dem Ersteinsatz einem öffentlichen Intrusionstest unterzogen werden müssen.