Ctrl-Alt-R

Gravierender Mangel am E-Voting-System der Post entdeckt

Von Andreas Moor, 12.03.2019, Update 10.45 Uhr

Das E-Voting-System der Post kommt nicht aus den Schlagzeilen: Auf die Zweifel am spanischen Technologiepartner Scytl folgte Kritik an der Art und Weise, wie der Quellcode des Systems veröffentlicht wurde. Zurzeit wird das System einem «öffentlichen Hackertest» unterzogen, während Fachleute aus aller Welt den Quellcode nach Schwachstellen durchsuchen.

Nun haben Experten um die kanadische Sicherheitsforscherin Sarah Jamie Lewis einen schweren Mangel an einer zentralen Komponente des Systems entdeckt. Dieser ermöglicht es einem Insider mit Zugriff auf das System, das Ergebnis einer Abstimmung zu manipulieren, ohne dass dies bei der Überprüfung entdeckt würde. Die Forscher betrachten den Fehler als so fundamental, dass «die Integrität des übrigen Codes infrage gestellt wird». Sarah Jamie Lewis: «Die Protokolle sind meiner Meinung nach mit fehlendem Verständnis der Kryptografie implementiert worden, kombiniert mit schlampiger Programmierung.»

Die Schwachstelle ist offenbar so gravierend, dass die Post heute Dienstag dazu Stellung genommen hat: «Internationale IT-Experten haben nun eine kritische Lücke im Quellcode gefunden und dies der Post gemeldet. Die Experten konnten aufzeigen, dass diese Lücke dazu genutzt werden könnte, um Stimmen zu manipulieren, ohne dass dies nachgewiesen werden könnte.» Im Klartext: Die universelle Verifizierbarkeit – ein vom Hersteller angepriesenes Kernstück der Software – ist also nicht gewährleistet. Auch die Bundeskanzlei reagiert und schreibt in einer Stellungnahme: «Die Bundeskanzlei hat die Post aufgefordert, ihre Sicherheitsprozesse zu überprüfen und anzupassen, damit solche Mängel verhindert werden können.»

Die Post sieht darin allerdings kein schwerwiegendes Problem: Um die Schwachstelle auszunützen, benötige man Zugriff auf die IT-Infrastruktur sowie «die Hilfe von mehreren Insidern mit Spezialwissen bei der Post oder den Kantonen». Dennoch habe man den Algorithmus korrigiert und werde die Änderungen demnächst veröffentlichen.

Sarah Jamie Lewis, Olivier Pereira und Vanessa Teague haben die Ergebnisse ihrer Untersuchung der Post gemeldet, sind jedoch nicht als Tester registriert. Deshalb können sie keine der von der Post ausgesetzten Prämien beanspruchen. «Wir glauben, die Leute haben ein Recht auf sichere Abstimmungen mit Systemen, die transparent sind und überprüft und verstanden werden können. Wir tun das nicht wegen des Geldes», sagt Sarah Jamie Lewis gegenüber der Republik.

Wie weiter? Zweifel am Prinzip der universellen Verifizierbarkeit stellen die Sicherheit eines Kernstücks des Systems infrage. Dass der Angreifer ein «Insider» sein muss mit Zugang zu den IT-Systemen der Post, weist auf ein grundsätzliches Problem des E-Votings mit einem zentralen System hin: Die Verantwortung ist auf eine kleine Anzahl Leute verteilt – damit steigt das Risiko einer Wahlfälschung.

Der entdeckte Mangel wirft auch ein Schlaglicht auf die Zertifizierung durch die KPMG: Die Prüffirma hat der Schweizer Post bescheinigt, dass sie alle Anforderungen für die universelle Verifizierbarkeit erfüllt. Der Öffentlichkeit werden die Prüfberichte bislang vorenthalten.