Aktueller Kommentar von SentinelOne vom 21.10.2020:

Schweizer Bericht über Schwachstellen in Wahl-Auswertungssoftware zeigt Verwundbarkeit auf

Morgan Wright, Chief Security Advisor bei SentinelOne <https://www.sentinelone.com/>

Das deutsche IT-Security Unternehmen AWARE7 GmbH, bekannt durch Penetrationstests, Live Hacking Shows und Seminare, beschreibt in einem aktuellen Blog Forschungsergebnisse <https://arxiv.org/abs/1906.07532> der ETH und der Universität Zürich in Bezug auf Sicherheitslücken in der Schweizer E-Voting Software. Letztlich ist es ein weiterer Beleg über die Probleme mit Wahl-Software. Bereits 2017 hatten Mitglieder des CCC Schwachstellen in einer ähnlichen Software in Deutschland, über die damals unter anderem der Spiegel <https://www.spiegel.de/consent-a-?targetUrl=https%3A%2F%2Fwww.spiegel.de%2Fnetzwelt%2Fnetzpolitik%2Fbundestagswahl-2017-hacker-zerlegen-wahl-software-pc-wahl-a-1166425.html> berichtete.

In Ländern mit freien Wahlen ist die Integrität der Stimmabgabe von größter Bedeutung. Selbst einen kleinen Teil der Wahlergebnisse in Zweifel zu ziehen, würde das Ergebnis und die Legitimität derjenigen, die gerade ins Amt gewählt wurden – manchmal nur mit sehr geringem Vorsprung – in Frage stellen. Die oft gehörte These, dass „Papierabstimmungen das Problem lösen“, ignoriert die Tatsache, dass Software und Netzwerksysteme seit langer Zeit zur Auszählung, Speicherung, Verarbeitung, Verbreitung und Überprüfung der Ergebnisse der Papierabstimmungen verwendet werden. Nationalstaaten mit einem geopolitischen Interesse oder kriminelle Organisationen mit einem Profitmotiv (z.B. Lösegeldforderungen) sind in der Lage, die vielfältigen Schwachstellen des gegenwärtigen Systems auszunutzen.

Um eine Störung des demokratischen Prozesses zu erreichen und Unsicherheit sowie Chaos zu stiften, muss ein Angreifer nicht jedes System oder jede Ebene des Verarbeitungsprozesses angreifen. Attacken auf nur ein bis zwei Schlüsselsysteme haben bereits das Potenzial, den gesamten Wahlprozess zu untergraben. Ein Angriff auf die Stimmabgabe wird höchstwahrscheinlich erst dann erfolgen, wenn die Wahl bereits im Gange ist.

Einfache Schritte können unternommen werden, um die Wahrscheinlichkeit der Störung einer Wahl und ihres Ablaufes so weit wie möglich zu verhindern. Letztlich ist es eine Untergrabung des Vertrauens in demokratische Grundprozesse, denen die Gesellschaft vertraut. Ein erster Schritt, der dazu beitragen kann dieses Vertrauen zu festigen, ist es sicherzustellen, dass die für Wahlen eingesetzte Software und die damit verbundenen Systeme gepatcht wurden. Die Änderung jedes Standardpassworts in ein starkes Passwort, gekoppelt mit einer Multi-Faktor-Authentifizierung, ist ein weiterer logischer Schritt. Viele Systeme weltweit, verwenden noch immer veraltete Sicherheitstechnologien, die entwickelt wurden, um Bedrohungen von gestern, nicht von heute und morgen abzuwehren. Bei den Wahlen geht es um die politischen Entscheidungen und Veränderungen der nächsten zwei Jahre, vier Jahre und eventuell sogar noch längere Zeiträume, deshalb ist es so wichtig diese Wahlprozesse vor fremden Eingriffen zu schützen.

Kontakt
Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580; sentinelone@kafka-kommunikation.de