KANTON LUZERN

Regierungsrat

Luzern, 12. Januar 2021

ANTWORT AUF ANFRAGE A 388

Nummer: A 388
Protokoll-Nr.: 36
Eröffnet: 26.10.2020 / Justiz- und Sicherheitsdepartement

Anfrage Estermann Rahel und Mit. über die Sicherheitsstandards von Software im Bereich Wahlen und Abstimmungen

Vorbemerkungen:
Die Online-Zeitschrift «Republik» hat bereits im Vorfeld der Publikation vom 25. September 2020 die Dienststelle Informatik (DIIN) und die Abteilung Gemeinden zur Sesam-Applikation Wahlen befragt. Der Artikel erwähnt den Kanton Luzern an zwei Stellen. Zum einen wird Luzern als Sesam-Kunde aufgeführt, zum anderen als Beispiel für funktionierende Kontroll- und Verifikationsmechanismen, um Hacks zu vermeiden: «Dazu (*Anm. zu solchen Mechanismen*) zählen separat angefertigte – also nicht von der Software generierte – Protokolle. Solche werden etwa in Luzern erstellt». Gemeint sind hierbei die bei jeder Abstimmung oder Wahl erstellten Verbale der Urnenbüros in den Gemeinden, auf denen das Ergebnis der Abstimmungen oder Wahl verzeichnet wird. Verbale werden von allen gewählten Mitgliedern eines Urnenbüros unterzeichnet; damit beglaubigen sie die Richtigkeit der Angaben. Die Verbale werden per Post an die Abteilung Gemeinden gesandt, welche in einem zweiten Verifikationsschritt die in der Datenbank erfassten Gemeinderesultate mit jenen Resultaten der Verbale vergleicht. Zudem werden alle Resultate der Gemeinden schon am Abstimmungssonntag nach deren Übermittlung auf ihre Plausibilität hin überprüft. Danach erfolgt die Veröffentlichung der definitiven Abstimmungsresultate.

Zur Frage 1: Waren dem Kanton Luzern die von den Forschenden gefundenen Sicherheitslücken bewusst? Falls ja, seit wann, und was hat er dagegen unternommen?

Entgegen der Berichterstattung der «Republik» bestehen dank verschiedenen Massnahmen im Kanton Luzern keine Sicherheitslücken.

Für die von der Dienststelle Informatik (DIIN) betriebenen Server gelten hohe interne Sicherheitsrichtlinien. Ein Server wird daher nie mit Standardpasswörtern betrieben. Auch für den Datenbankserver der Wahlen-Applikation werden seit der Installation individuelle, komplexe Passwörter verwendet.

Zugriffe auf kantonale Systeme werden mittels einer Privileged Access Management-Lösung (PAM) verwaltet. Dieser privilegierte Zugriff schützt die Vertraulichkeit sensibler Daten und die Server-Infrastruktur. Sämtliche System- und Datenbankzugriffe werden protokolliert und können von den Sicherheitsverantwortlichen ausgewertet werden.

Weitere sicherheitstechnische Massnahmen sind daher nicht notwendig.

Zu Frage 2: Sind dem Kanton Luzern Fälle bekannt, in denen es aufgrund der Sicherheitslücken zu Fehleingaben kam oder die Lücken ausgenutzt wurden?

Nein, es sind keine Fälle bekannt. Neben den bereits erwähnten Verbalen, welche die einzelnen Urnenbüros der Gemeinden per Post dem Kanton zustellen, werden zusätzlich im Kanton Luzern bei der Entgegennahme der Resultate der Gemeinden am Abstimmungssonntag laufend Plausibilitätskontrollen sowie Stichproben durchgeführt, um eine hohe Verifikationsqualität zu erzielen.

Dieses systematische Vorgehen stellt sicher, dass Fehleingaben oder allfällige Manipulationen bei der Eingabe der Resultate in der Sesam-Applikation im Kanton Luzern auf jeden Fall entdeckt würden.

Zu Frage 3: Wie instruiert der Kanton die kommunalen Wahlbehörden für die Anwendung der Software und sensibilisiert sie für Sicherheit und Datenschutz? Ist die kantonale Dienststelle Informatik, der IT-Sicherheitsbeauftragte sowie die Datenschutzstelle einbezogen?

Die Software wird vor jeder Abstimmung in den Gemeinden und auch im Kanton auf ihre Funktionalität hin geprüft. Für das Erfassen der Abstimmungsresultate erhalten die Gemeinden vom Kanton persönliche Passwörter, die vor jeder Abstimmung neu nach dem Zufallsprinzip erstellt werden. Gesetzliche eidgenössische und kantonale Bestimmungen stellen sicher, dass bei Wahlen und Abstimmungen das Stimmgeheimnis gewahrt wird. Damit ist für das Urnenbüro nicht erkennbar, wer wie abgestimmt oder gewählt hat. Vor den Wahlen führt der Software-Entwickler Sesam separate Kurse für die Anwendung der Wahlen-Applikation durch, an der alle Informatik-Verantwortlichen der Gemeinden teilnehmen. Die Gemeinden sind im Rahmen ihrer Gemeindeautonomie selbst verantwortlich, ihre Mitarbeitenden für die Sicherheit und Datenschutz zu sensibilisieren.

Die DIIN bietet im Vorfeld von Abstimmungen technischen Support im Problemfall an. Auch am Abstimmungssonntag sind mehrere Personen der DIIN auf Pikett, um allenfalls unterstützen zu können. Bei der Organisation und Durchführung von Wahlen ist die DIIN von Beginn weg involviert.

Zu Frage 4: Hält es der Kanton für nötig, entsprechende Sicherheits- und Anwendungsstandards in einer Verordnung basierend auf dem Stimmrechtsgesetz festzuschreiben? Was würde sie beinhalten?

Wir sehen dazu keine Notwendigkeit, dies in einem Erlass festzuhalten. Zudem wäre es auch nicht geeignet, diese Regelungen generell-abstrakt in einer Verordnung festzuhalten. Die internen Abläufe und der mehrstufige Verifikationsprozess betreffen die operative Ebene und werden mit Weisungen und Checklisten im Managementsystem umgesetzt.

Für Abstimmungen besteht eine vollständige Betriebs- wie auch eine Prozessdokumentation, in welcher sämtliche Arbeitsschritte und Zuständigkeiten aller involvierten Stellen während einer Abstimmung erfasst sind.

Für Wahlen werden jeweils im Vorfeld Betriebs-, Sicherheits- und Notfallkonzepte erstellt, die für jede durchzuführende Wahl jeweils erneuert und überarbeitet werden.

Zu Frage 5: Jeder Softwareeinsatz bringt Sicherheitsrisiken mit sich, denen mit Schutzzielen begegnet werden muss. Wurden für den Einsatz der Software die Schutzziele definiert und die Informationen gemäss Informatiksicherheitsverordnung (SRL Nr. 26b) klassifiziert? Existiert ein Massnahmenplan zur Erreichung der Schutzziele?

Die Anwendung ist gemäss Informatiksicherheitsverordnung (SRL Nr. 26b) klassifiziert und die definierten Schutzziele werden eingehalten.

Zu Frage 6: Werden geeignete Schutzmassnahmen ergriffen, um unbefugten Zugriff, Missbrauch und Verfälschung der Informationen während des Datenaustausches über Organisationsgrenzen hinweg zu verhindern?

Die Datenübermittlung erfolgt ausschliesslich im kantonalen Netzwerk und nicht im öffentlichen Netz. Die Gemeinden haben sich in einem ersten Schritt via virtuelles privates Kommunikationsnetz (Citrix Gateway) ins kantonale Netz einzuwählen und anschliessend auch noch für die Nutzung der Abstimmungssoftware zu authentifizieren. Beide Zugriffe sind durch Benutzernamen und Passwörter geschützt. Bereits dadurch sind Zugriffe oder Manipulationen von Dritten praktisch ausgeschlossen. Ausserdem ist für die Software der Abstimmungen ein weiteres Passwort notwendig, das der Kanton vor jeder Abstimmung neu generiert und den Gemeinden zustellt. Zusätzlich werden die Resultate nach dem Abstimmungssonntag nochmals aufgrund der von den Gemeinden eingereichten Verbale kontrolliert. Unbefugter Zugriff, Missbrauch oder Verfälschung von Informationen sind daher entweder gar nicht möglich und würden für den unwahrscheinlichen Fall entdeckt.

Zu Frage 7: Arbeitet der Kanton in der Verbesserung und Weiterentwicklung von elektronischen Prozessen im Bereich Wahlen und Abstimmungen mit anderen Kantonen zusammen, welche die gleiche Software nutzen? Wie sieht diese Zusammenarbeit aus?

Der Kanton Luzern steht im dauernden Austausch sowohl mit dem Hersteller der Software wie auch mit anderen Kantonen, welche die Software im Einsatz haben. Aktuell wird die Software für Abstimmungen neu entwickelt. Als einzige Kantone sind Luzern und Basel-Landschaft eng in diesen grundlegenden Entwicklungsprozess eingebunden und stellen zusammen mit dem Hersteller die Funktionalität, die Qualität und die Sicherheit der Neuentwicklung sicher.

Zu Frage 8: Nach welchen Kriterien wählt und überprüft der Kanton Luzern die Software für die Ermittlung von Wahl- und Abstimmungsergebnissen, insbesondere hinsichtlich Sicherheit?

Mit einer Beschaffung werden Anforderungen an die Software aus verschiedenen Betrachtungswinkeln definiert. Nebst den Bereichen Funktionalität, Architektur, Interoperabilität, etc. sind Fragen zur Sicherheitsarchitektur selbstverständlich.

Zu Frage 9: Wird der Kanton bei zukünftigen Ausschreibungen für die Wahl- und Abstimmungssoftware die Offenlegung des Software-Quellcodes einfordern?

Dieser Entscheid muss bei der nächsten Beschaffung getroffen werden. Beim aktuellen Projekt der Neuentwicklung werden Sicherheitsreviews auf Quellcode-Ebene durchgeführt. Eine Offenlegung, wie beim E-Voting vom Bund aktuell diskutiert, ist bisher nicht vorgesehen.