



Parlamentarischer Vorstoss

Antwort des Regierungsrates

Vorstoss-Nr.: 308-2025
Vorstossart: Interpellation
Richtlinienmotion: ☐
Geschäftsnummer: 2025.GRPARL.1484

Eingereicht am: 24.11.2025

Fraktionsvorstoss: Nein
Vorstoss Ratsorgan: Nein
Eingereicht von: Daphinoff (Bern, Die Mitte) (Sprecher/in)
Roggli (Rüschegg Heubach, Die Mitte)
Rappa (Burgdorf, Die Mitte)
Gerber (Schüpfen, Die Mitte)

Weitere Unterschriften: 0

Dringlichkeit verlangt: Nein
Dringlichkeit gewährt:

RRB-Nr.: 621/2026 vom 03. Juni 2026
Direktion: Staatskanzlei
Klassifizierung: Nicht klassifiziert

Cybersicherheit und Integrität von Wahlen im Kanton Bern

Die fortschreitende Digitalisierung hat in den letzten Jahren auch die Durchführung von Wahlen und Abstimmungen im Kanton Bern zunehmend beeinflusst. Während diese Entwicklungen die Effizienz und den Zugang zu Wahlinformationen verbessern, ergeben sich auch neue Herausforderungen, insbesondere im Bereich der Cybersicherheit.

In Zeiten zunehmender Cyberbedrohungen ist die Sicherheit von Wahlen und Abstimmungen von grösster Bedeutung. Der Kanton Bern muss sicherstellen, dass alle Wahlprozesse – vom Einholen der Stimmen bis hin zur Bekanntgabe der Resultate – vor Angriffen, Manipulation und Desinformation geschützt sind. Ein transparentes, sicheres und faires Wahlsystem ist unerlässlich für das Vertrauen der Bevölkerung in die demokratischen Institutionen.

Angesichts der zunehmenden Digitalisierung der Wahlinfrastruktur und der wachsenden Bedrohungslage durch Cyberangriffe und digitale Desinformationskampagnen ist es entscheidend, dass der Kanton Bern vorausschauende Massnahmen trifft, um die Sicherheit der Wahlprozesse zu gewährleisten und den Schutz der Wählerdaten zu garantieren. In diesem Zusammenhang stellt sich die Frage, inwiefern der Kanton Bern auf die zunehmenden Risiken durch Cyberangriffe und digitale Manipulationen vorbereitet ist.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Wie wird die Sicherheit der digitalen Infrastruktur gewährleistet, die zur Erfassung und Übermittlung von Wahlergebnissen verwendet wird? Welche konkreten Massnahmen wurden bisher umgesetzt, um die Sicherheit dieser Infrastruktur vor Hackerangriffen oder anderen unbefugten Eingriffen zu schützen?

2. In welchem Umfang wird der Schutz sensibler Wahldaten (z. B. Wählerdaten, Stimmabgaben, Wahlergebnisse) auf kantonaler und kommunaler Ebene gewährleistet? Welche technischen und organisatorischen Vorkehrungen gibt es, um diese Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu schützen?
3. Wie stellt der Kanton sicher, dass Wahlen und Abstimmungen gegen digitale Desinformationskampagnen und gezielte Einflussnahme (z. B. durch Fake News oder Manipulation von sozialen Medien) geschützt sind? Welche Massnahmen werden ergriffen, um das Vertrauen der Bevölkerung in die Integrität der Wahlprozesse aufrechtzuerhalten?
4. Wie erfolgt die Sensibilisierung und Schulung von Gemeindeverwaltungen und Wahlbüros bezüglich der Cybersicherheitsrisiken im Kontext von Wahlen und Abstimmungen? Wird den Gemeinden eine zentrale Anlaufstelle oder Unterstützung durch den Kanton für IT-Sicherheitsfragen im Wahlprozess angeboten?
5. Inwieweit erfolgt eine Zusammenarbeit des Kantons Bern mit anderen Institutionen, wie dem Nationalen Zentrum für Cybersicherheit (NCSC), der Melde- und Analysestelle Informationssicherung (MELANI), anderen Kantonen oder Fachhochschulen (z. B. BFH, ETHL), um die Cybersicherheit im Wahlprozess zu stärken? Gibt es konkrete Kooperationen oder gemeinsame Initiativen zur Verbesserung der Wahlsicherheit?

Antwort des Regierungsrates

Der Kanton Bern setzt seit 2018 die Software BEWAS ein, um bei eidgenössischen, kantonalen und regionalen Urnengängen die Resultate zu ermitteln und zu publizieren. BEWAS ist eine Webapplikation der Bedag Informatik AG (Bedag). Die Bedag hat die Software entwickelt und erbringt für den Kanton Bern Pflege-, Wartungs-, Betriebs- und Supportleistungen. Rechtliche Grundlage für den Einsatz einer Informatikanwendung zur Ausmittlung von Abstimmungen und Wahlen bildet Artikel 53 Absatz 1 des Gesetzes über die politischen Rechte (PRG). Für BEWAS liegt ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) vor, das die Datenschutz- und Sicherheitsrisiken erfasst und bewertet.

Der Regierungsrat beantwortet die Fragen wie folgt:

1. *Wie wird die Sicherheit der digitalen Infrastruktur gewährleistet, die zur Erfassung und Übermittlung von Wahlergebnissen verwendet wird? Welche konkreten Massnahmen wurden bisher umgesetzt, um die Sicherheit dieser Infrastruktur vor Hackerangriffen oder anderen unbefugten Eingriffen zu schützen?*

Die Weisung über den Grundsatz für die Informations- und Cybersicherheit (ICSGW) regelt die Anforderungen an den Grundsatz für ICT-Mittel, Informationen und Personendaten der kantonalen Behörden. Das ISDS-Konzept beschreibt, welche weiteren Massnahmen zur Reduktion der Risiken auf ein akzeptables Mass ergriffen werden.

Die Infrastruktur der Bedag erfüllt diese Vorgaben vollumfänglich. Darüber hinaus betreibt die Bedag ein zertifiziertes Informationssicherheits-Management System (ISMS) nach ISO 27001:2022, ein zertifiziertes Business Continuity Management System nach ISO 22301:2019 sowie ein zertifiziertes Service Management-System nach ISO 20000:2018. Ergänzend bestehen zertifizierte Umwelt- (ISO 14001:2015) und Qualitäts-Management-Systeme (ISO 9001:2015).

Zusätzlich hat die Bedag ein umfassendes Sicherheitstest-Programm etabliert, bei dem u.a. auch BEWAS regelmässig von externen, unabhängigen Firmen überprüft wird. Die Ergebnisse dieser Prüfungen fliessen systematisch in allfällige Verbesserungs- und Korrekturmaassnahmen ein.

2. *In welchem Umfang wird der Schutz sensibler Wahldaten (z. B. Wählerdaten, Stimmabgaben, Wahlresultate) auf kantonaler und kommunaler Ebene gewährleistet? Welche technischen und organisatorischen Vorkehrungen gibt es, um diese Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu schützen?*

Zunächst ist festzuhalten, dass in BEWAS keine besonders schützenswerten Daten bearbeitet werden. Da der Stimmrechtsausweis bereits vor der Auszählung von den Stimm- bzw. Wahlzetteln getrennt wird, ist das Stimmgeheimnis jederzeit gewährleistet. Die Stimm- und Wahlzettel werden in den Gemeinden ohne technische Unterstützung des Kantons ausgezählt. Die Gemeinden können zur Ausmittlung eigene technische Hilfsmittel (z.B. Wahlzettelersfassungssoftware) einsetzen. Die Stimmausschüsse erfassen in BEWAS nur die ausgezählten Gemeinderesultate, die die Staatskanzlei anschliessend im Internet veröffentlicht. Die Stimmausschüsse können die kantonal publizierten Gemeindeergebnisse jederzeit mit den Gemeindeprotokollen vergleichen.

Sicherheitsaspekte haben beim Einsatz von digitalen Technologien grosse Bedeutung. Für BEWAS existiert, wie eingangs erwähnt, ein ISDS-Konzept. Für den Zugriff auf die Software durch Mitarbeitende in Gemeinden, Regierungsstatthalterämtern und der Staatskanzlei ist eine Zweifaktorenauthentifizierung notwendig. Nutzerinnen und Nutzer müssen sich mit ihrer E-Mailadresse, die vorgängig durch die zuständige Stelle (RSTA, STA) erfasst wurde, einem Passwort und einer einmal gültigen Transaktionsnummer anmelden. Vor jedem Urnengang aktualisieren die Staatskanzlei und die Regierungsstatthalterämter die Benutzerliste. Sämtliche Datenmanipulationen im System werden per Audit Logging festgehalten. Ebenso werden alle Login- und Account-Aktivitäten aufgezeichnet.

BEWAS wird über das Internet aufgerufen und im Rechenzentrum der Bedag betrieben. Es gibt keine direkten Schnittstellen zu anderen Netzen. Die Rechnerkapazitäten werden redundant in voneinander getrennten Maschinensälen aufgebaut und sowohl systemseitig wie applikationsseitig so konfiguriert, dass eine höchstmögliche Ausfallsicherheit besteht und die Skalierbarkeit garantiert werden kann. Die Datensicherung erfolgt täglich und vollautomatisch im Data Safe Rechenzentrum der Bedag in Le Noirmont. Weiter besteht ein Notfallkonzept und ein Service Level Agreement, das eine enge personelle Unterstützung durch die Fachkräfte der Bedag an den Wahl- und Abstimmungstagen gewährleistet.

3. *Wie stellt der Kanton sicher, dass Wahlen und Abstimmungen gegen digitale Desinformationskampagnen und gezielte Einflussnahme (z. B. durch Fake News oder Manipulation von sozialen Medien) geschützt sind? Welche Massnahmen werden ergriffen, um das Vertrauen der Bevölkerung in die Integrität der Wahlprozesse aufrechtzuerhalten?*

Desinformation ist die gezielte Verbreitung von Falschinformationen mit dem Ziel, die Gesellschaft, einzelne Gruppen oder Einzelpersonen im Sinne politischer oder wirtschaftlicher Interessen zu täuschen.¹ Desinformationskampagnen beschränken sich nicht nur auf den Kanton Bern. Von möglichen Beeinflussungsaktivitäten – zu deren Mittel die Desinformation gehört – ist die ganze Schweiz betroffen.

¹ Quelle: [Glossar des EDA](#) -> Desinformation

Vor dem Hintergrund zunehmender geopolitischer Spannungen ist mit einer Zunahme solcher Aktivitäten auch in der Schweiz zu rechnen. Der Bundesrat hat deshalb am 26. November 2025 eine interdepartementale Arbeitsgruppe gegen Beeinflussungsaktivitäten und Desinformation (IDAG) eingesetzt.² Ziel ist, die Arbeiten innerhalb der Bundesverwaltung zum Thema Beeinflussungsaktivitäten und Desinformation zu stärken, ein Lageverständnis zu erarbeiten und bei Bedarf den Entscheidungstragenden Massnahmen vorzuschlagen. Die IDAG wird vom Staatssekretariat für Sicherheitspolitik (SEPOS) geleitet und umfasst die von der Bedrohung meistbetroffenen Ämter. Unter anderem ist auch die für die politischen Rechte zuständige Bundeskanzlei eingebunden. Die Staatskanzlei steht diesbezüglich mit der Bundeskanzlei im Kontakt.

Der Regierungsrat begrüsst das Vorgehen des Bundes. Aufgrund der internationalen Dimension der Beeinflussungsaktivitäten ist es sachgerecht, wenn der Bund sich dem Thema annimmt. Der Kanton versucht, in seiner eigenen Kommunikation gegenüber der Öffentlichkeit vertrauensbildend zu wirken. Er nutzt seine offiziellen Kommunikationskanäle, um über Wahlen und Abstimmungen vorausschauend, transparent, offen und glaubwürdig zu informieren. Vor, während und nach einem Urnengang erhält die Öffentlichkeit aktuelle Informationen über Medienmitteilungen, Social-Media-Beiträge, die VoteInfo-App, das Amtsblatt sowie die Website des Kantons.

Die Abläufe und Verantwortlichkeiten sind bei Wahlen und Abstimmungen gesetzlich geregelt. Die Auszählung ist öffentlich und bei allen relevanten Vorgängen gilt für den Stimmausschuss das Vieraugenprinzip. Jede Person kann dem Regierungsrat Unregelmässigkeiten oder Mängel bei einer Wahl oder Abstimmung oder im Zusammenhang mit einem Volksbegehren anzeigen.

4. *Wie erfolgt die Sensibilisierung und Schulung von Gemeindeverwaltungen und Wahlbüros bezüglich der Cybersicherheitsrisiken im Kontext von Wahlen und Abstimmungen? Wird den Gemeinden eine zentrale Anlaufstelle oder Unterstützung durch den Kanton für IT-Sicherheitsfragen im Wahlprozess angeboten?*

Vor jeder Proporzwahl sind die Gemeinden verpflichtet, im Rahmen eines Praxistests die technischen Abläufe des Wahltages zu üben. Bei Majorzwahlen und Abstimmungen ist der Test freiwillig. Detaillierte Checklisten unterstützen die Gemeinden. Bei Fragen wenden sich die Gemeinden zuerst an ihr zuständiges Regierungsstatthalteramt. Je nach Bedarf unterstützt auch die Staatskanzlei oder die Bedag.

5. *Inwieweit erfolgt eine Zusammenarbeit des Kantons Bern mit anderen Institutionen, wie dem Nationalen Zentrum für Cybersicherheit (NCSC), der Melde- und Analysestelle Informationssicherung (MELANI), anderen Kantonen oder Fachhochschulen (z. B. BFH, ETHL), um die Cybersicherheit im Wahlprozess zu stärken? Gibt es konkrete Kooperationen oder gemeinsame Initiativen zur Verbesserung der Wahlsicherheit?*

Die Bedag tauscht sich periodisch auf mehreren Stufen mit nationalen wie internationalen Institutionen aus, um ihre Cybersicherheit zu stärken. Auch arbeitet sie eng und kooperativ mit dem Bundesamt für Cybersicherheit (BACS) zusammen.

² <https://www.news.admin.ch/de/newnsb/PhIsbTXMF5o3YiuqfGumj>

Der Regierungsrat unterstützt grundsätzlich weitere Digitalisierungsschritte im Bereich der politischen Rechte. Angesichts der bestehenden Risiken müssen hinsichtlich der technischen Sicherheit der Infrastruktur hohe Anforderungen gestellt werden, was sich auch auf die Kosten auswirkt. Der Regierungsrat wird daher weitere Digitalisierungsschritte vertieft und unter dem Aspekt der Sicherheit auch kritisch prüfen.

Verteiler

– Grosser Rat