Anlage 3:
Empfehlungen des BSI zur Übermittlung von vorläufigen Wahlergebnissen

Bei der Übermittlung der vorläufigen Wahlergebnisse von den Wahllokalen über die Gemeinden und Kreise bis zur Zusammenführung des vorläufigen Gesamtergebnisses besteht die Gefahr, dass Täter

- die Wahlergebnisse auf dem Übertragungsweg manipulieren
- unter Vortäuschung eines falschen Absenders gefälschte Wahlergebnisse einschleusen
- die Übermittlung unterbinden.

Daher ist es einerseits erforderlich, alternative Übermittlungsverfahren vorzuhalten (**Redundanz**) und andererseits die Unverfälschtheit (**Integrität**) und Echtheit (**Authentizität**) der vorläufigen Wahlergebnisse zu schützen.

Ein möglicher Ansatz zum Schutz der Integrität und Authentizität, der vom jeweils gewählten Übermittlungsverfahren unabhängig ist, ist die Nutzung eines **zweiten Kanals**. Typischerweise erfolgt dies wie folgt:

1. Der Absender sendet die Information auf dem ersten Kanal.
2. Der Empfänger sendet die empfangene Information auf dem zweiten Kanal zurück an den Absender.
3. Der Absender vergleicht beide Informationen und eskaliert den Vorgang bei Abweichungen.

Wie jede Sicherheitsmaßnahme ist auch die Nutzung eines zweiten Kanals nicht unüberwindbar, da die Angreifer auch beide Kanäle kontrollieren können. Sie erschwert aber den erfolgreichen Angriff, wenn die Kanäle unabhängig voneinander sind. Ein Beispiel für diesen Ansatz ist die Nutzung eines Portals zur Verifikation der gemeldeten Ergebnisse:

1. Der Absender meldet seine Wahlergebnisse per Telefon.
2. Der Empfänger stellt die empfangenen Ergebnisse auf einem Web-Portal ein.
3. Der Absender kontrolliert, ob seine gemeldeten Ergebnisse korrekt auf dem Web-Portal aufgeführt sind und eskaliert den Vorgang bei Abweichungen.

Abhängig vom jeweiligen Übermittlungsverfahren gibt es weitere Möglichkeiten, die Integrität und Authentizität der vorläufigen Wahlergebnisse zu schützen:

E-Mails können mit einer kryptografischen **Digitalen Signatur** versendet werden, die vom Empfänger überprüft werden kann. Dies setzt jedoch im Allgemeinen eine vorhandene Public-Key-Infrastruktur (PKI) voraus.

Bei einer telefonischen Übermittlung kann ein **Rückruf** an eine **vorab hinterlegte Telefonnummer** erfolgen. Darüber hinaus kann ein **individuelles Kennwort** abgefragt werden.