

Grundschutzkataloge der Bundesanstalt für Sicherheit in der Informationstechnik

Die Grundschutzkataloge (GK) der Bundesanstalt für Sicherheit in der Informationstechnik stellen Basisanforderungen an den Umgang mit Computersystemen zusammen, die einen Grundschutz zum Ziel haben. Der Grundschutzkatalog stellt einen guten Überblick über den allgemeinen Stand der Technik dar. Im Folgenden wird eine Auswahl der Anforderungen in den GK zusammengestellt und mit den Anforderungen nach der BWahlGV verglichen.

1. Einsatz kryptographischer Methoden

Die Richtlinien für die Bauart von Wahlgeräten stellen keine konkreten Anforderungen, mit denen die Integrität der Software und der Stimmen gewährleistet werden kann. Die BSI-Grundschutzkataloge erwähnen zu diesem Bereich etwa, dass bei der Auswahl eines geeigneten kryptographischen Verfahrens zunächst die Anforderungen an die Vertraulichkeit und Authentizität zu definieren seien. Das BSI spricht auch ausdrückliche Empfehlungen für bestimmte Hash-Verfahren aus (GK, M 2.164) Bei besonderen Anforderungen an die Vertraulichkeit oder Integrität von in Datenbanken gespeicherten Informationen seien diese zu verschlüsseln (GK, M 4.72). Beim Einsatz von Kryptomodulen seien diese durch geeignete physikalische Sicherheitsmaßnahmen vor unautorisiertem Zugriff auf die Modulinhalte zu sichern (GK, M4.87). Bei der Überprüfung von Software auf ihre Authentizität seien geeignete kryptographische Methoden zu verwenden (GK, M 4.107).

Entsprechend den fehlenden Vorgaben der BWahlGV wird die Software der eingesetzten Wahlgeräte durch ungeeignete Prüfsummen authentifiziert, wird ein Austausch der Software durch unbefugte Dritte nicht durch konstruktive Maßnahmen verhindert und werden die abgegebenen Stimmen nicht durch kryptographische Verschlüsselung vor einer Veränderung geschützt.

2. Kontrolle des Zugangs

Die Grundschutzkataloge fordern, bei IT-Systemen müsse sichergestellt werden, dass nur autorisierte Personen das IT-System benutzen können. Hierfür seien geeignete Authentifizierungsmechanismen zu wählen. Administratoraktivitäten seien zu protokollieren. Unregelmäßigkeiten und Manipulationsversuche müssten erkennbar werden. Hierbei helfen Protokollisierungsfunktionen, Verschlüsselung und eine digitale Signatur (GK, M 4.41).

Bei der Durchführung von Wartungs- und Reparaturarbeiten sollte dokumentiert werden, wann ein System gewartet wurde und welche Fehler behoben wurden. Für solche Arbeiten durch Externe seien Regelungen für die Beaufsichtigung derart zu treffen, dass beurteilt werden könne, ob während der Arbeit unautorisierte Handlungen vollzogen werden (GK, M 2.4). Fremdpersonen, auch Wartungs- und Reinigungspersonal, sei ständig zu begleiten oder zu beaufsichtigen (GK, M 2.16)

Die Bundeswahlgeräteverordnung regelt den Zugang zu den Wahlgeräten nicht. Lediglich für die gefüllten Stimmenspeicher gibt es Vorgaben für den Zeit bis zur Freigabe der Wahlunterlagen. Die BWahlGV bleibt damit hinter den Anforderungen der GK des BSI zurück.

3. Durchsetzung von Sicherheitsmaßnahmen

Die Einhaltung von IT-Sicherheitsmaßnahmen ist laut Grundschutzkatalogen regelmäßig zu kontrollieren (GK, M 2.182) Mitarbeiter seien für die IT-Sicherheit und Gefährdungen zu sensibilisieren, damit die Sinnhaftigkeit der Einhaltung von Regelungen verstanden werde (GK, M 2.198).

Bei der Aufbewahrung und dem Einsatz von Wahlgeräten kommt diesem Punkt eine besondere Bedeutung zu, weil die Geräte nicht regel-

mäßig eingesetzt werden und deshalb der routinemäßige Umgang mit den Geräten fehlt. Entsprechend werden die Geräte üblicherweise von Personen behandelt werden, die mit dem Umgang der Geräte nicht vertraut sind. Die erforderlichen Kontrollen und Maßnahmen zur Sensibilisierung der betroffenen Personen ist beim Umgang mit Wahlgeräten nicht erkennbar.