Prüfsummen

Die Prüfsummen der Nedap-Geräte wird durch einfache Addition aller Bytes in den EPROM Speichermodulen gebildet, die die Gerätesoftware enthalten (vgl. Gonggrijp et al, **Anlage B 7**, Abschnitt 5.5.2) Solche einfachen Summen bilden grundsätzlich keinen Schutz gegen Manipulationen, weil sie keine Information über die Reihenfolge der Bytes enthalten. Zudem können veränderte Bereiche dadurch ausgeglichen werden, dass an anderer Stelle eine Veränderung vorgenommen wird, die die Summe wieder ausgleicht. Dies sei anhand des folgenden Beispiels erläutert:

Die Zeichenketten

- "Wahlcomputer in Cottbus."
- "Computerwahl in Cottbus."
- "Computerwahn in Cottbus,"
- "Stimmzettelwahl IN Mainz"

liefern bei der Addition Ihrer Bytes jeweils den Wert 2340 obwohl sie nicht übereinstimmen. Die ersten beiden Zeilen liefern das gleiche Ergebnis, weil die Buchstaben „W“ (87) und „c“ (99) dieselbe Summe ergeben wie die Buchstaben „C“ (67) und „w“ (119). Die zweite und dritte Zeile liefern das gleiche Ergebnis, weil der Austausch des „l“ (108) durch ein „n“ (110) dadurch kompensiert wird, dass auch der Punkt (46) am Ende durch ein Komma ersetzt wird (44).

Es gibt verschiedene Algorithmen, die eine Veränderung eines Datensatzes nahezu unmöglich machen, weil Sie eine Prüfsumme durch eine Funktion berechnen, die sich nicht invertieren lässt. Dadurch ist es praktisch unmöglich, passende Datensätze zu einer gegebenen Prüfsumme zu finden. Deshalb macht die Angabe einer solchen Prüfsumme es unmöglich, einen solchen Datensatz zu manipulieren. Beispiele für solche kryptographischen Algorithmen sind z.B. MD5 und SHA-256.

Die genannten kryptographischen Algorithmen sind seit geraumer Zeit allgemeiner Stand der Technik.

Der MD5-Algorithmus z.B. liefert für die obigen Zeichenketten völlig verschiedene Ergebnisse:

- "Wahlcomputer in Cottbus."
  MD5: 858a4647184139b55c9a067a566ef0ee
- "Computerwahl in Cottbus."
  MD5: 1519fac4a53a9b0c49b0ca95082dac47
- "Computerwahn in Cottbus,"
  MD5: 53212581a9b166c0d4decd9e8a01f342

Die Wahlcomputer verwenden für die Prüfsummenbildung nicht nur einen banalen Algorithmus, sondern bilden die Prüfsumme selbst durch die eingesetzte Gerätesoftware. Eine Selbstprüfung kann jedoch niemals Gewissheit über die Identität der Software liefern, da ein potentieller Angreifer, der die Gerätesoftware manipuliert, den Prüfalgorithmus unproblematisch mitmanipulieren kann, so dass dieser das erwartete Ergebnis ausgibt. Dieses Problem stellt sich unabhängig vom verwendeten Algorithmus und lässt sich nur durch eine externe, von der Geräte-Software unabhängigen Prüfung vermeiden.

Das Bundesministerium des Innern teilt diese Auffassung in seiner Stellungnahme (vgl. **Anlage B 19**, Abschnitt 3.2.1), wenn festgestellt wird, dass zu einer Überprüfung der Software-Authentizität die Entnahme der EPROMS aus dem Gerät erforderlich ist.