

## Wo liegt der große Vorteil eines Hardware-basierten Ansatzes?

1. Die Ursache für die Angreifbarkeit von Datenverarbeitungssystemen durch Schad-Software liegt bei praktisch allen heute verwendeten programmierbaren Geräten in der Hardware-Architektur begründet. Deren Prinzip hat sich seit den vierziger Jahren des vorigen Jahrhunderts nicht wesentlich geändert. Vor allem wurde versäumt den höheren Anforderungen von Entwicklungen gerecht zu werden, die entstanden sind durch
  - den Gebrauch externer Datenspeicher,
  - das Aufkommen von PC, und
  - Verbindungen über Netzwerke.

Von den Marktteilnehmern wird diese Tatsache aus verschiedenen Gründen gern verschwiegen:

- Von den Hardware-Herstellern, weil sie durch eine disruptive Änderung
  - den Markterfolg ihrer bisherigen Produktion,
  - den externen Software-Support und
  - etablierte Bindungen zu ihren Zulieferern gefährden.
- Von den Software-Herstellern, weil sie einen einträglichen Zweig – Antiviren-Software und dergleichen – in Frage stellen müssten.
- Von beiden, weil die gewinnbringende gegenseitige Abhängigkeit gefährdet werden könnte.

Zu diesen Gründen kommt die Erkenntnis, dass Neuerungen die bestehende Produkte, Verfahren oder Strukturen in nennenswertem Umfang ändern, nur selten mit geringem Aufwand oder schnell umzusetzen sind.

2. Durch die zu erwartende Verwendung von Künstlicher Intelligenz und Quanten-Computern auf Seiten der Hacker werden auf Binärinformationen aufbauende Methoden zum Erlangen von IT-Sicherheit zunehmend angreifbar. Hierzu gehören Nutzernamen, Passwörter, so genannte Zertifikate, biometrische Daten und Krypto-Schlüssel. Weil S<sup>3</sup>DVS prinzipiell ohne solche binären Absicherungen arbeiten, wird die Sicherheit von IT-Systemen durch den Einsatz von Quanten-Computern seitens der Hacker nicht wesentlich beeinträchtigt. Das gefährlichste Szenario dürfte die Übernahme eines Nutzerplatzes durch einen Hacker sein. An dieser Stelle ist seitens der Systemeigner dafür Sorge zu tragen, dass Aufgaben und Berechtigungen derart im System verteilt sind, dass Datenabfluss und Datenmanipulation durch Unbefugte verhindert werden. S<sup>3</sup>DVS liefern die technischen Grundlagen dafür.