Welche Alternativen gibt es zu S³DVS?

Zurzeit ist keine Lösung zu Sicherheitsfragen in der IT bekannt, die - wie S³DVS - auf Änderungen der Hardware-Architektur aufsetzt.

Folglich besteht die Konkurrenz zu S³DVS aus

- „Trusted Platform Modules“:
  Diese relativ junge Technologie benötigt einen zusätzlichen Chip mit kryptografischen Informationen, und beruht auf einer Authentifizierung, die beim Initialisieren des Systems angewandt wird, um die Vertrauenswürdigkeit der Software zu verifizieren. Gegenüber S³DVS hat sie folgende Nachteile:
  - Es kann nur eine Software, bzw. ein Softwarehersteller authentifiziert werden.
  - Es besteht eine dauernde Abhängigkeit von diesem Softwarehersteller.
  - Die Authentifizierung erfolgt an Hand einer – wenn auch langen – Folge von Bits und kann prinzipiell mit den Methoden überwunden werden, die auch zum Hacken von Passworten benutzt werden.
  - Sie bietet keinen Schutz vor Malware, die Schwachstellen ausnutzen wie
    - Stack-Overflows,
    - Spectre oder
    - Meltdown.
  - Dem Nutzer werden Steuer- und Kontrollmöglichkeiten genommen, weil jegliche Software-Konfiguration nur im Rahmen der extern bereitgestellten Programmteile möglich ist.
  - Verschiedenen Organisationen – z.B. das Bundesamt für Sicherheit in der Informationstechnik – stehen dem Verfahren skeptisch gegenüber.
- Antiviren-Software und ähnlichen Produkten, deren Nachteile hinlänglich bekannt sind:
  - Sie wirken nur gegen ihnen bekannte Angreifer,
  - erkennen kodierte Schad-Software nicht,
  - sind wirkungslos gegenüber zukünftigen Angreifern und
  - erfordern häufige Aktualisierungen.
- Anweisungen an Nutzer, mit folgenden Schwachpunkten:
  - Wiederholte Schulungen, Unterweisungen und Ermahnungen sind erforderlich, insbesondere nach Erkennen neuer Angriffsformen,
  - Nachlässigkeit, insbesondere bei Routinearbeiten und
  - Anfälligkeit gegenüber
    - Neugier,
    - Täuschungen,
    - „Social Engineering“ und
    - „Phishing“.