Welche Alternativen gibt es zu S³DVS?

Zurzeit ist keine Lösung zu Sicherheitsfragen in der IT bekannt, die - wie S³DVS - auf Änderungen der Hardware-Architektur basiert.
Folglich besteht die Konkurrenz zu S³DVS aus

- **Trusted Platform Modules:**
  Diese 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. (Quelle: Trusted Platform Module – Wikipedia , Stichwort „Kritik“)
- **Secure Boot:**
  Diese Technologie soll sicher stellen, dass ein Computer nur mit vertrauenswürdiger Firmware und Betriebssystemsoftware gebootet wird. Dazu überprüft die Firmware des Computers die digitalen Signaturen von Bootloadern und Softwarekomponenten. Wenn eine Signatur kompromittiert oder ungültig ist, verhindert Secure Boot, dass die betroffene Software geladen wird.Gegenüber S³DVS hat Secure Boot sie folgende Nachteile:
  - Es bietet keinen Schutz (mehr), wenn die Zertifizierungsstelle kompromittiert wird.
  - Die Signatur kann mit kryptografischen Mitteln überwunden werden.
  - Secure Boot wird am Rechner manuell durch Einstellungen in der Firmware aktiviert oder deaktiviert.
  - Beim Einschalten des Gerätes ist nicht erkennbar, ob Secure Boot aktiv ist oder nicht.
  - Eine zentrale Aktivierung/Deaktivierung für mehrere Rechner einer Einrichtung ist nicht möglich.
  - Das BSI schreibt zu Secure Boot: (Es) "besteht weiterhin die Möglichkeit durch Ausnutzung von Schwachstellen Schadcode in den Kernel einzubringen. Eine solche Art der Kompromittierung wird durch Secure Boot weder verhindert, noch signifikant erschwert." (Quelle: Sicherheitsanalyse der UEFI-Integration und Secure Boot-Implementierung von Windows 8 (bund.de))
- **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“.