Wovor schützen S^{3}DVS konkret?

S^{3}DVS sind eine wirksame Maßnahme gegen jegliche Software, die in ein System über folgend genannte Vektoren eingebracht wird:

- Wechselspeicher,
- Internet-Seiten,
- E-Mail-Anhänge,
- infizierte Dateien,
- Netzwerke,
- Daten-Schnittstellen

Dadurch schützen S^{3}DVS zum Beispiel vor den folgend aufgeführten Arten von Schad-Software, einschließlich der von ihnen möglicherweise installierten Programme. Dieser Schutz ist unabhängig von Alter und „Einschleppzeitpunkt“ der Schad-Software, und wirkt somit auch gegen alle zukünftige Versionen von:

- Viren,
- Trojaner
- Würmer,
- Ransomware,
- Rootkits,
- Bootkits

Dabei spielt es keine Rolle, ob die angreifende Schad-Software als Dateiinhalt, datei-los („file-less“) oder kodiert ist. Selbst steganografisch kodierte Schad-Software wird sicher geblockt.

Die aktuelle Entwicklung hat gezeigt, dass S^{3}DVS auch Fehler verhindern, die durch Ausnutzung von Schwachstellen der Prozessorfunktion „speculative execution“ ausgelöst werden können, und Anfang 2018 unter den Namen

- Spectre und
- Meltdown

bekannt wurden und vielfach große finanzielle Schäden verursacht haben. Weil die Entwicklung neuer Prozessoren, die die heutige Schwachstelle dann nicht mehr haben, kostspielig und zeitaufwändig ist, könnten S^{3}DVS als Alternative dazu dienen, weil die betroffenen, bisher gebauten Prozessoren in der Architektur von S^{3}DVS weiterhin fehlerfrei und risikolos funktionieren.