Wie entsteht der große Gewinn an Sicherheit?

Höhere Sicherheit entsteht durch vier Maßnahmen:

1. Zu bearbeitende Daten und Programme werden über getrennte Schnittstellen in das System eingegeben. Ein System, das es erlaubt, dieselbe Schnittstelle für den Austausch von Daten und Programmen zu nutzen, kann grundsätzlich nicht sicher sein bezüglich Angriffen, die mit Schad-Software geführt werden.

2. Daten und Programme werden in Kategorien eingeteilt. In herkömmlichen Hardware-Architekturen sind Daten aller Kategorien ungeordnet nebeneinander abgespeichert. Diese Unordnung wird von Hackern genutzt, um Instruktionen als Daten einzuschleusen und dann ausführen zu lassen. (Instruktionen in diesem Sinne sind Anweisungen an Prozessoren, bestimmte Manipulationen an Daten oder Programmen vorzunehmen.)

3. Die einzelnen Datenkategorien werden in eigenen, voneinander unabhängigen Speichereinheiten abgelegt. Hierdurch wird erreicht, dass als Daten eingegebene Speicherinhalte nicht als Instruktionen für die Prozessoren missbraucht werden können.

4. Für die Bearbeitung von Daten und das Verwalten der Programme werden separate Prozessoren genutzt, die unterschiedliche Zugriffsrechte auf die Speichereinheiten haben. Dadurch wird verhindert, dass Daten als Programme behandelt werden oder Programme als Daten.