

Qubes OS – Sicherheit durch Isolation

Was ist Qubes OS?

Qubes OS ist ein sicherheitsorientiertes Betriebssystem**, das auf dem Prinzip der Isolation basiert. Anstatt alle Programme im selben System laufen zu lassen, trennt Qubes OS Anwendungen und Aufgaben in virtuelle Maschinen (VMs), sogenannte **Qubes**.

Technische Grundlagen

- **Kernel:** Linux
- **Hypervisor:** Xen
- **GUI-Basis:** Fedora (in „dom0“)
- **Templates:** Fedora, Debian, Whonix u. a.

Jede Anwendung läuft in ihrer eigenen VM. Dadurch bleibt ein kompromittierter Bereich vom Rest des Systems getrennt.

Sicherheitsprinzip: *Security by Isolation*

- Jede Aktivität (z. B. Surfen, Arbeiten, Banking) läuft in einer getrennten Qube.
 - Schadsoftware bleibt in der betroffenen VM isoliert.
 - Das dom0-System (grafische Oberfläche) hat keinen Internetzugang, um Angriffe zu verhindern.
-

Aufbau des Systems

Ebene	Beschreibung
dom0	Verwaltungssystem ohne Internetzugriff
AppVMs	Virtuelle Maschinen für Anwendungen
TemplateVMs	Vorlagen, von denen AppVMs erstellt werden
ServiceVMs	Systemdienste (z. B. Netzwerk, Firewall)

Vorteile

- Hohe Sicherheit durch vollständige Trennung
 - Unterstützung mehrerer Betriebssysteme (Fedora, Debian, Whonix)
 - Klare Trennung von Arbeit, Privatleben und Internetaktivitäten
-

Nachteile

- Erhöhter Ressourcenverbrauch (RAM, CPU)
- komplexe Bedienung für Einsteiger
- Eingeschränkte Hardwarekompatibilität

Weitere Informationen

Website: <https://www.qubes-os.org>

Dokumentation: <https://www.qubes-os.org/doc/> **Video** <https://www.youtube.com/watch?v=uRBgQAwRagQ>

„A reasonably secure operating system“ – Qubes OS

Benjamin Zwettler Niclas Baumgartlinger