Qubes OS - Überblick

E.

20.11.2021

Inhalt

Qubes OS

QUBES OS
A REASONABLY SECURE OPERATING SYSTEM (qubes-os.org)

Qubes OS - ein einigermaßen sicheres Betriebssystem [für kompatible Notebooks]

"If you're serious about security, Qubes OS is the best OS available today. It's what I use, and free."

— Edward Snowden, *whistleblower and privacy advocate*

Betriebssystem: ⏻ → Bios → Bootloader → Betriebssystem

Beispiele:
- Desktop: Ubuntu, Windows, macOS
- Mobile: Android, iOS

Qubes OS im Vergleich zu Ubuntu:

\+ Mehr Schutz und Sicherheit (IT-Security, Privacy, Anonymity)

\- Weniger Bedienkomfort (erfordert Konzentration, Mühe, Geduld)

Mehr Schutz/Sicherheit - lohnt sich das?

Schutz und Sicherheit

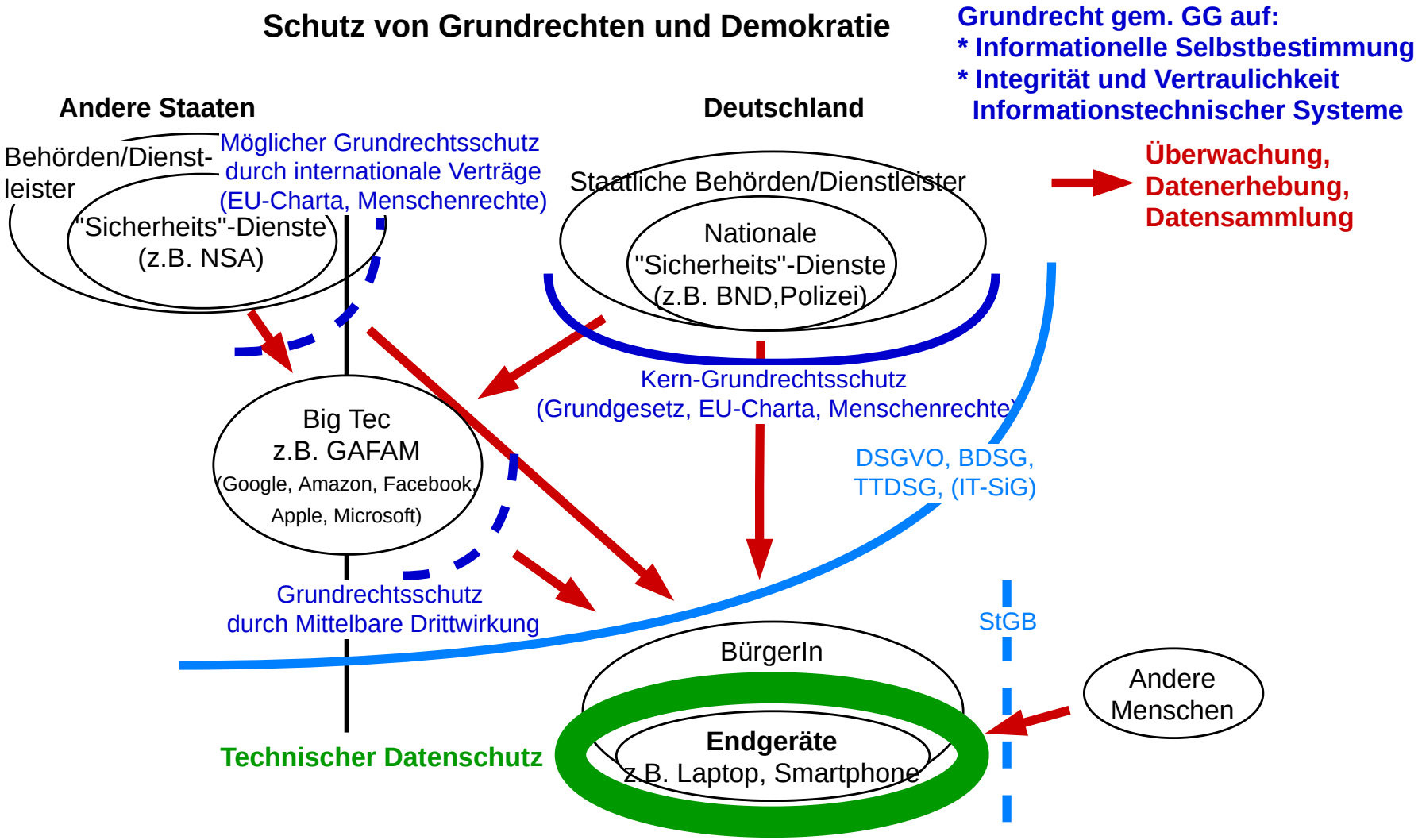
Bei Schutz und Sicherheit geht es darum gewisse Schutzgüter (z.B. Leben, Grundrecht, Haus, IT-System) vor gewissen unerwünschten Ereignissen (z.B. Verletzung, Einbruch) zu schützen.
Bei einer Risikobeurteilung/Bedrohungsanalyse sind folgende Fragen maßgeblich:

- Was sind die Schutzgüter? Wie wichtig sind sie?
- Was sind die unerwünschten Ereignisse? Wie schädlich? Wie wahrscheinlich?
- Welche Schutzmaßnahmen gibt es? Was kosten sie?

Beispiel: Betriebssystem

Schutzgüter: z.B. Vertraulichkeit, Integrität, Verfügbarkeit, Privatheit, Anonymität.
Unerwünschte Ereignisse: z.B. unautorisierter Zugriff auf Daten oder Sensoren (Video/Audio), Zerstörung, Profilbildung/Ausforschung, Identitätsdiebstahl.
Folgerisiken: z.B. Betrug, Erpressung etc..
Schutzmaßnahme: z.B. Nutzung von Qubes OS.

Schutz von Grundrechten und Demokratie: Rechtlicher Schutz, Technischer Schutz



Was bedeuten Endgeräte für den modernen Menschen?

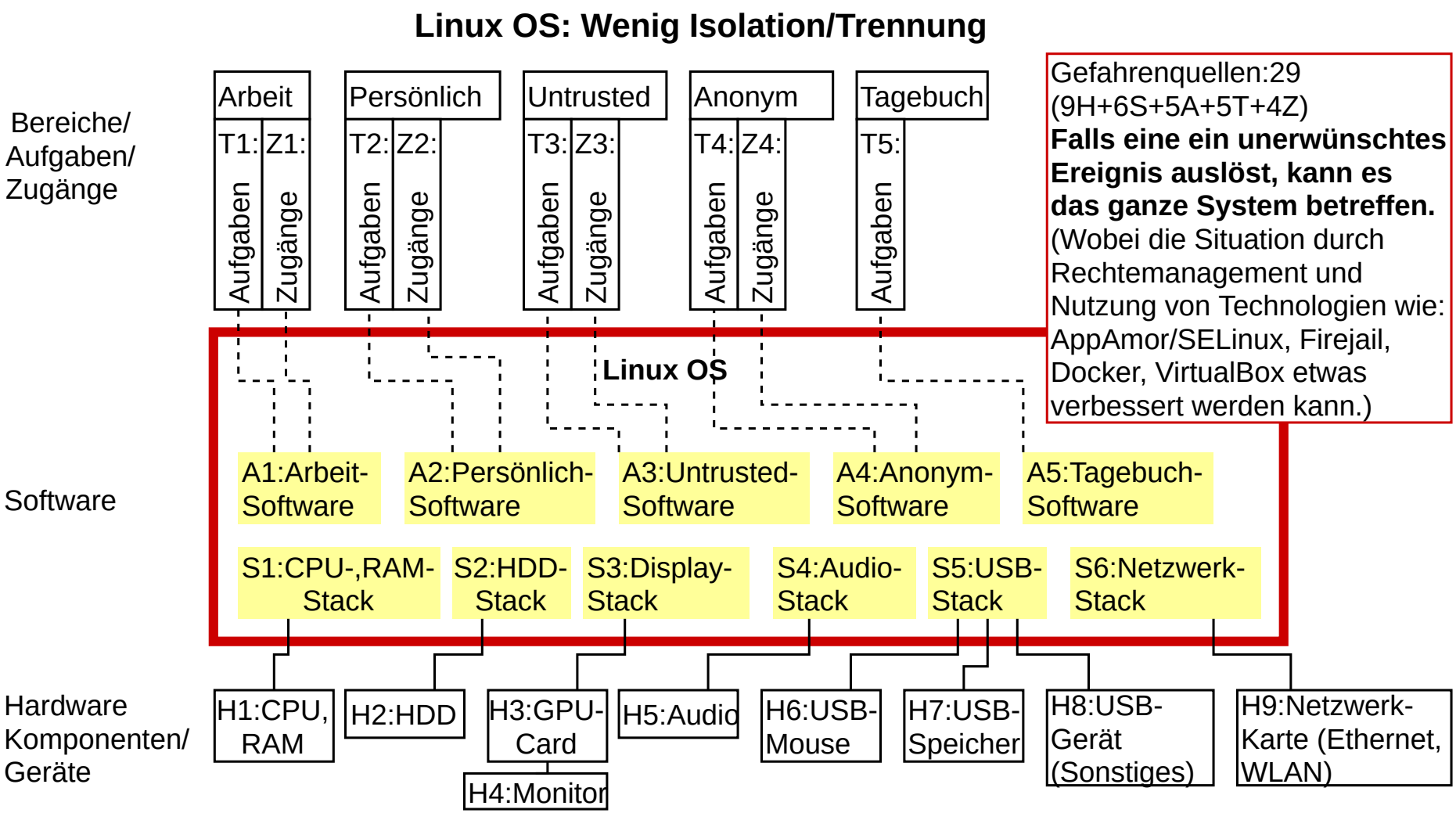
Bedeutung von Endgeräten	Schutzgüter (Beispiele)
Erweiterung des Gehirns	Vertrauliche Fotos, Texte
Persönlicher Assistent	Browser-Historie, Gesundheitsdaten, Finanzdaten, Identitätsdaten, Rechnungsdaten, Wichtige Zugänge
Arbeitsgerät	Personenbezogene Daten, sonstige vertrauliche Daten, vertrauliche/kritische Zugänge
Zugang zu weltweiten Medien/Informationen	Browser-Historie
Kommunikator	Soziale Kontakte, Politische Ausrichtung, Zugang zu Audio/Video-Daten (Echtzeit,Aufnahmen), Kommunikationsinhalte
Navigator	Positions-Daten (G5,GPS, WLAN, Bluetooth, RFID)
Erweiterung der Sensorik	Gesundheitsdaten

Mögliche unerwünschte Ereignisse

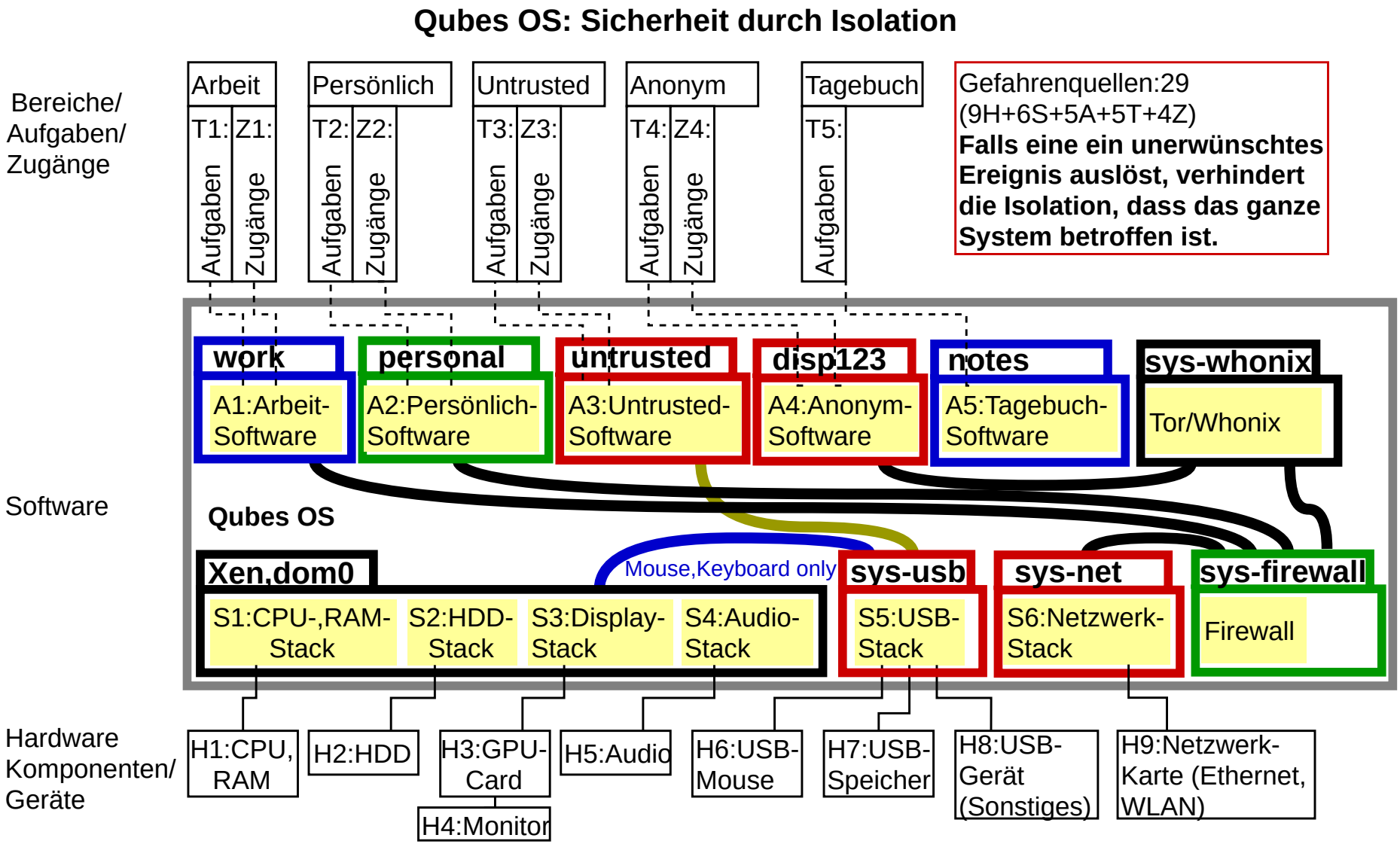
Abstrakte Schutzgüter: 1:Vertraulichkeit, 2:Integrität, 3:Verfügbarkeit, 4:Metadatenschutz

Gefahrenquellen/ Unerwünschte Ereignisse	Mögliche Gründe/Szenarien	Schutz-güter
Defekte Hardware	Gerät fällt herunter, Brand, Verschleiß	3, 2
Verschwundene Hardware	Verloren, vergessen, gestohlen	3, 1
Unauthorisierter Hardware-Zugang	Festplattenkopie, Manipulation der Hardware etc.	1-4
Benutzerfehler	Zeitdruck/Stress, fehlendes Wissen, Fishing/ Social Engineering, Dark Patterns	1-4
Konfigurationsfehler	Siehe Softwarefehler	1-4
Softwarefehler (Design,Implementierung)	Kosten, Interessenkonflikt, Missmanagement, Kompetenzmangel	1-4
Schadsoftware	Spyware,Trojaner,manipulierte Treiber..	1-4
Internet-Zugang	Angriffe aus dem Internet sind günstig.	1-4
Kommunikations-Partner nicht vertrauenswürdig/ zuverlässig/kompetent	Datenschutz-Probleme in der Cloud oder auf anderen Endgeräten.	1-4
Verbundene befallene Geräte/ Kommunikations-Partner	Internet, USB-, Bluetooth-Geräte, WLAN-Hotspot,..	1-4
Befallene interne Hardware-Komponenten	Viren in Komponenten: Festplatte, Modem, Grafikkarte, Netzwerkkarte, USB	1-4
Verbundene Sensoren	Unautorisierter Zugriff auf Sensoren (Audio,Video,GPS,WLAN,Modem)	1,4

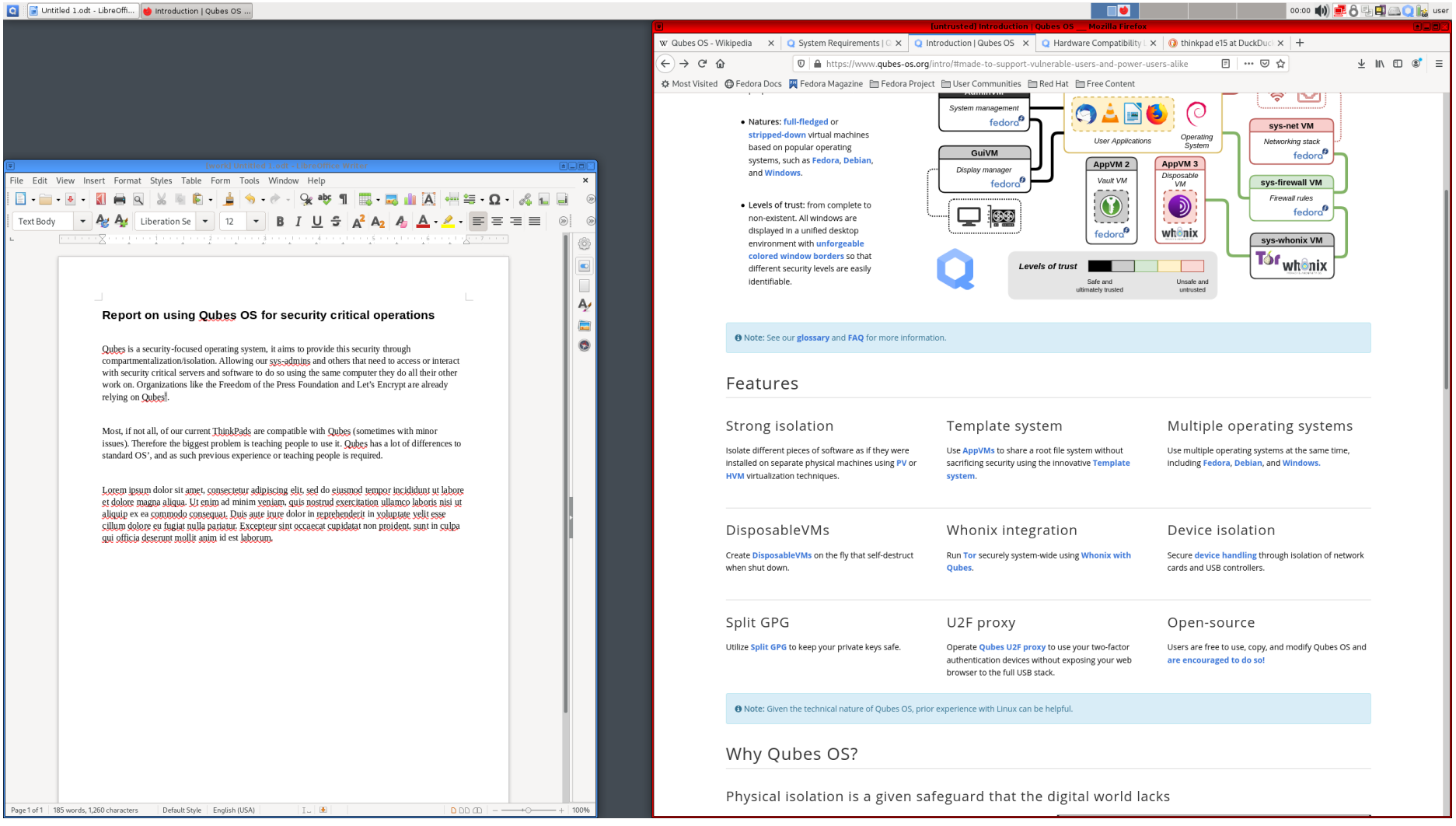
Probleme von Linux etc.



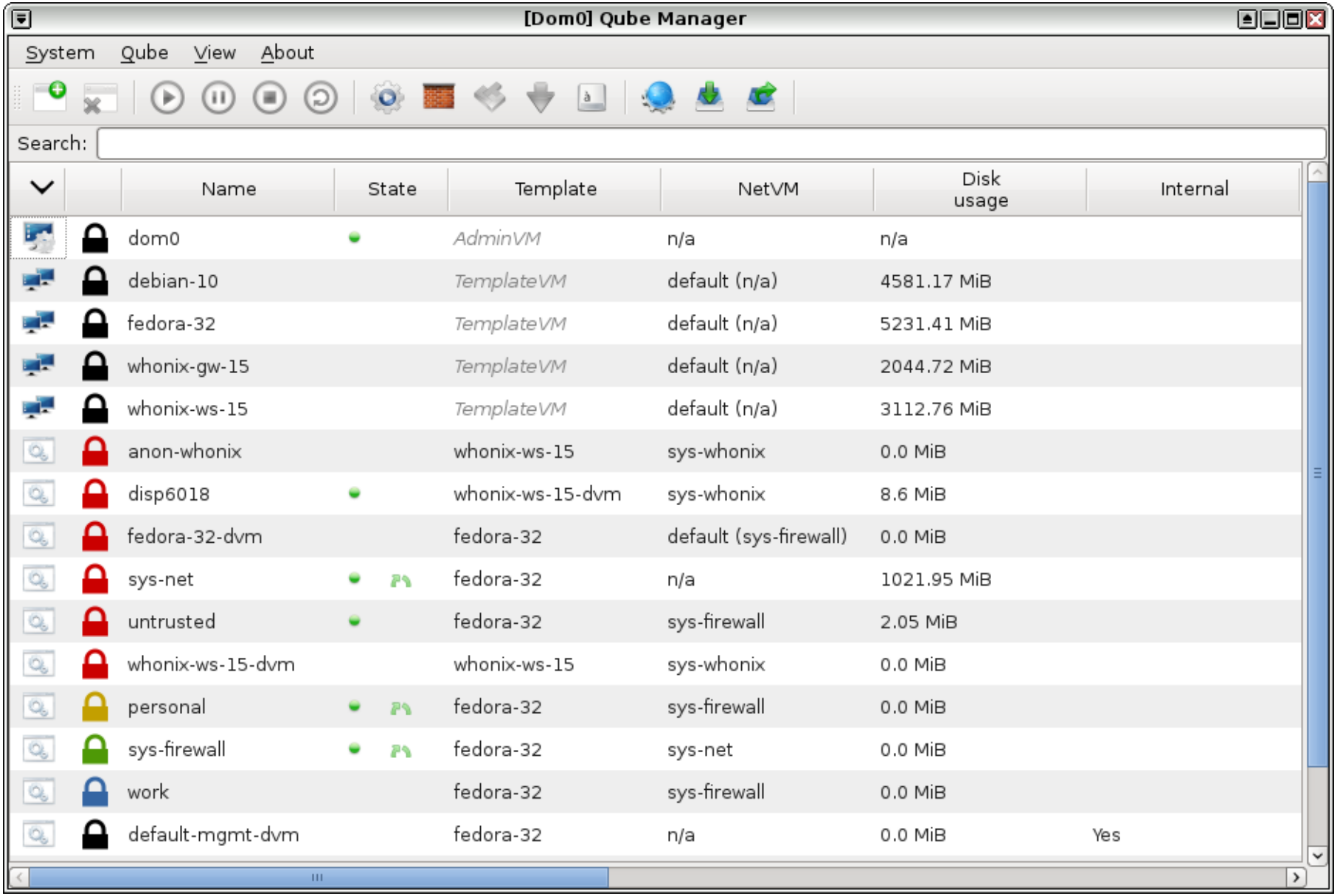
Qubes OS - Schutzkonzepte (Alles Isolieren)



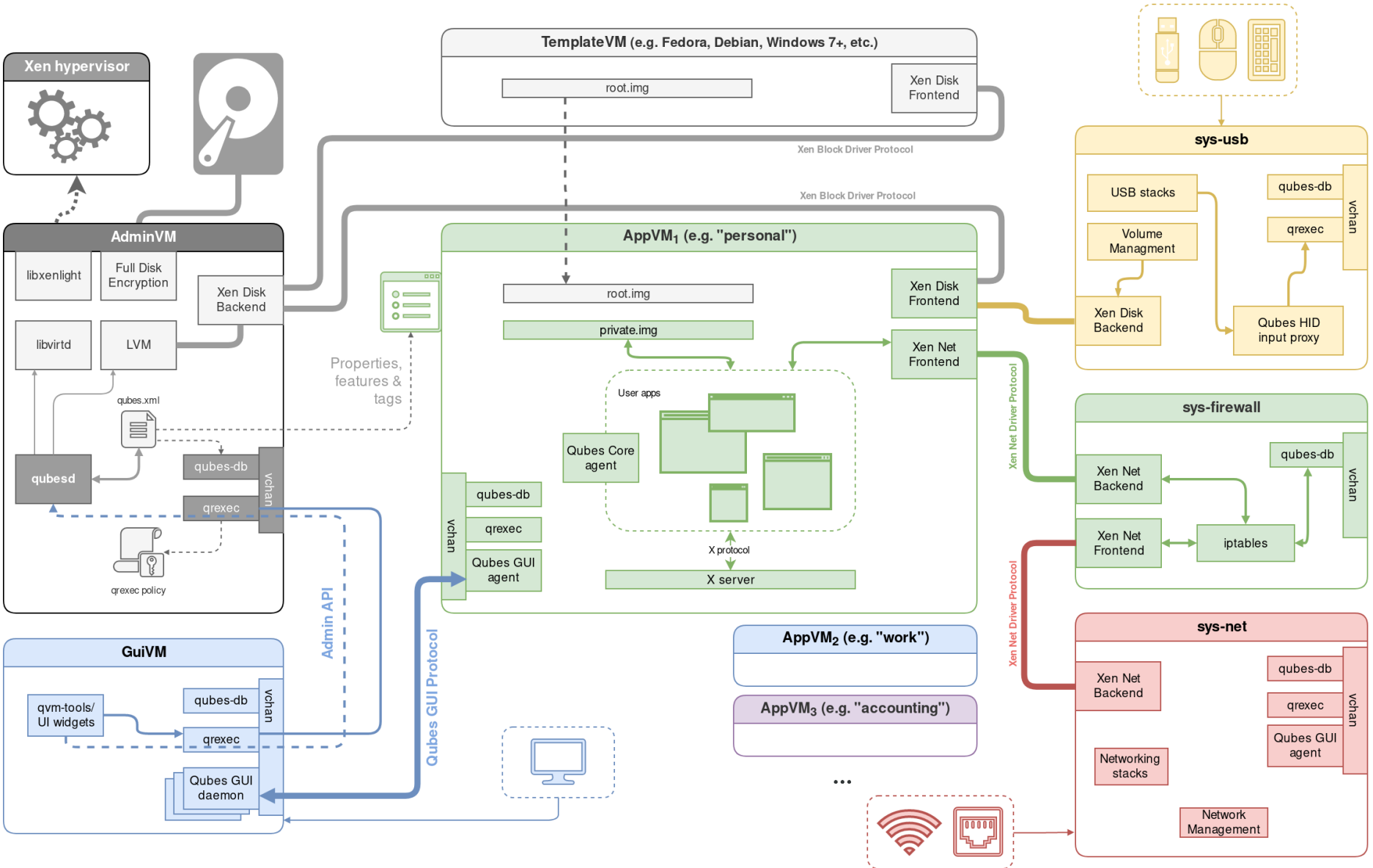
Jedes Fenster enthält VM-Namen und Trust-Farbe



Qubes VM-Manager



Qubes Template vs App-VM (1)



Qubes Schutzkonzepte - Zusammenfassung

1. Isolation von Geräten, Hardware-Komponenten, Treibern und sonstiger zugehöriger Software (erfordert: VT-x,VT-d)
2. Isolation von Bereichen (z.B. work, personal, shopping etc.)
3. Starke Isolation: Nutzung von Xen (Type 1 Hypervisor) zur Erstellung/Verwaltung von Virtuellen Maschinen (VMs).
4. Die VM "dom0" hat privilegierten Zugang. Sie enthält daher möglichst wenig Software und hat keinen Internet-Zugang.
5. Internet-Zugang, Firewall-Regeln, USB-Zugänge können pro VM geregelt werden.
6. Template-System (mehrere App-VMs können ein Template (z.B. debian-11) nutzen)
   a. Die vielen VMs können komfortabel aktualisiert werden (auch offline VMs). Nur Update-Adressen sind (standardmäßig) vom Template aus erreichbar.
   b. Schadsoftware in App-VMs können das Template nicht befallen.
   c. Schadsoftware kann auch in der APP-VM i.d.R. nicht überleben, da alle Änderungen außerhalb des User-Space (/home, /usr/local, /rw) beim nächsten Neustart der VM zurückgesetzt werden.
7. Wegwerf-VMs (disposable), welche nach einmaligem Gebrauch gelöscht werden.
8. Verhältnismäßig komfortabler Copy-Past- und Datei-Transfer-Mechanismus zwischen VMs (dom0 ist davon ausgenommen).
9. Schutz von Metadaten: VMs können auf einfache Weise mit dem Tor-Netzwerk verbunden werden, um die IP-Adresse zu schützen (Whonix).

Qubes OS - Vor- und Nachteile

+ Software kann bequem in Test-VMs getesten werden, ohne das Produktivsystem zu gefährden ⇾ Schutz vor Bugs.
+ Nicht-vertrauenswürdige Software kann in VMs eingesperrt werden - auch ohne Internetzugang ⇾ Schutz vor Viren und Bugs, Metadatenschutz.
+ Nicht-vertrauenswürdige Dateien können in Wegwerf-VMs geöffnet werden.
+ VMs können komplett über Tor geroutet werden.
+ USB-Geräte können eingesperrt werden.
+ Es können viele Betriebssysteme auch Windows und Android parallel genutzt werden.
− Hoher RAM-Bedarf (16GB sind eher knapp).
− Hoher Speicherplatz-Bedarf (1TB ist OK).
− USB-Geräte erfordern erheblichen Mehraufwand.
− Es ist schwierig den Überblick über Daten zu behalten, da nicht mehr nur verschiedene Ordner sondern auch verschiedene VMs berücksichtigt werden müssen.
− Backup-Workflow erfordert mehr Überlegungen.
− VMs können nicht verschachtelt werden (VirtualBox etc. nicht möglich).
− Hinter Qubes steckt nur ein kleines Entwicklerteam, daher stößt man immer mal wieder auf die ein oder anderen Probleme, die aber meist mit etwas technischem Hintergrund und Internet-Suchen gelöst werden können.
− Man braucht einen kompatibles Notebook (VT-x, VT-d oder äquivalent).

Qubes OS - Kleine Live Demo

Qubes OS - Fazit

- Die Lage der IT-Sicherheit ist katastrophal - Endgeräte sind dabei keine Ausnahme.
- Vielen Menschen ist dies nicht bewusst und halten ihre Geräte für vertrauenswürdig.
- Linux ist ein guter erster Schritt, um zumindest dafür zu sorgen, dass kaum noch proprietärer Code auf dem Gerät ausgeführt wird.
- Mit Qubes OS können all die unsicheren Software- und Hardware-Komponenten in VMs eingesperrt werden und ihr Internet-Zugang reguliert werden.
- Solange die Isolation hält, können in den vertrauenswürdigen VMs auch vertrauliche Aufgaben vorgenommen werden.
- Vertrauenswürdige Endgeräte sind die Voraussetzung für vertrauliche Kommunikation.
- Wenn Menschen eine freie Gesellschaft wollen, sollten sie nicht zulassen, dass „Sicherheits“-Dienste und Unternehmen immer tiefer in ihre Privaten Räume eingreifen - sonst landen sie dort wo China jetzt schon ist.
- Derzeit ist der Einsatz von Qubes nur für technisch versierte Nutzer und Unternehmen zu empfehlen. Sobald die sporadischen Fehler behoben sind und es genügend Hilfeseiten gibt, kann es auch in der Breite eingesetzt werden.

Weiterführende Informationen

- Qubes OS: qubes-os.org (englisch)
- Privacy Tools: privacyguides.org (englisch)
- Anonymity Guide: anonymousplanet.org (englisch)

Verwendete Bilder

Beschreibung, Quelle, DSGVO-Relevanz	Öffentlich	Rechteinhaber	Lizenz
Beschreibung: Qubes OS Logo **Quelle:** https://www.qubes-os.org/attachment/icons/qubes-logo-icon-name-slogan-fb.png **DSGVO-Relevanz:** Nein **Sonstiges:** Q wurde aus Layout-Gründen von oben nach links verschoben. Die Marke wurde nur referenzierend genutzt, keine Verwechslungsgefahr.	Ja	Unbekannt	Unbekannt
Beschreibung: Edward Snowden Tweet **Quelle:** https://www.qubes-os.org (2021-11-20) **DSGVO-Relevanz:** Nein, weil Quelle öffentlich und journalistisches Interesse überwiegt.	Ja	Unbekannt	Unbekannt
Beschreibung: Schutz von Grundrechten und Demokratie (S.5) **Quelle:** https://embeach.gitlab.io/2021_qubes_slides/2021QubesOS_Folien.pdf **DSGVO-Relevanz:** Nein	Ja	E.	CC-BY-4.0
Beschreibung: Linux OS: Wenig Isolation/Trennung (S.8) **Quelle:** https://embeach.gitlab.io/2021_qubes_slides/2021QubesOS_Folien.pdf **DSGVO-Relevanz:** Nein	Ja	E.	CC-BY-4.0
Beschreibung: Qubes OS: Sicherheit durch Isolation (S.9) **Quelle:** https://embeach.gitlab.io/2021_qubes_slides/2021QubesOS_Folien.pdf **DSGVO-Relevanz:** Nein	Ja	E.	CC-BY-4.0
Beschreibung: Screenshot Qubes mit blauem und rotem Fenster **Quelle:** https://www.qubes-os.org/attachment/doc/r4.0-snapshot12.png **DSGVO-Relevanz:** Nein	Ja	Unbekannt	Unbekannt
Beschreibung: Screenshot Qubes VM-Manager **Quelle:** https://www.qubes-os.org/attachment/doc/r4.0-qubes-manager.png **DSGVO-Relevanz:** Nein	Ja	Keine Schöpfungshöhe	-
Beschreibung: Qubes Architektur **Quelle:** https://www.qubes-os.org/attachment/doc/qubes-components.png **DSGVO-Relevanz:** Nein	Ja	Unbekannt	Unbekannt

Folien/Kontakt

Die Folien sind erreichbar unter:
`https://embeach.gitlab.io/2021_qubes_slides/2021QubesOS_Folien.pdf`

Fragen/Anregungen: `emb_gitl+qubes@mailbox.org`

Danke für die Aufmerksamkeit! Fragen?