Qubes OS

A reasonably secure operating system

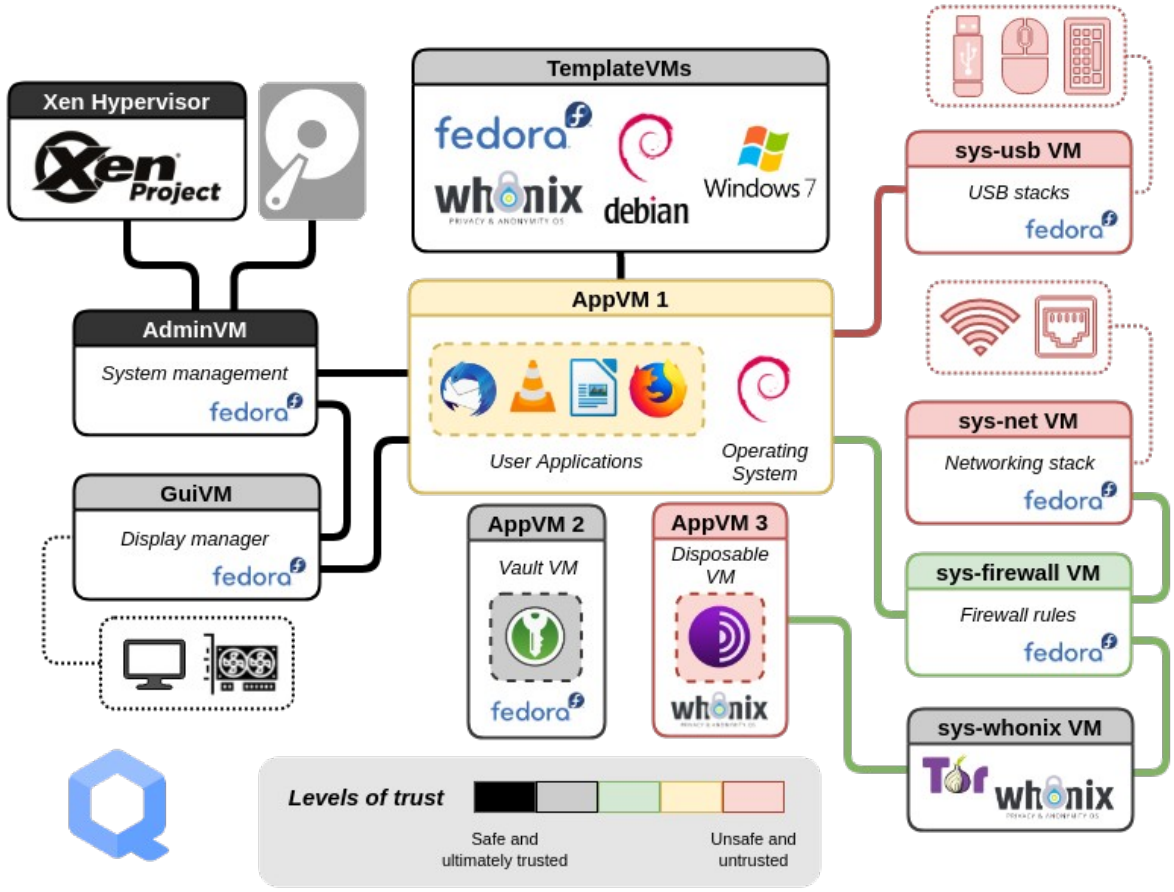
Übersetzung aus der Original-Dokumentation

Inhalt

EINFÜHRUNG

Was ist Qubes OS?

Qubes OS ist ein freies und quelloffenes, sicherheitsorientiertes Betriebssystem für Einzelbenutzer-Desktop-Computing. Qubes OS nutzt die Xen-basierte Virtualisierung, um die Erstellung und Verwaltung von isolierten Abteilungen zu ermöglichen, die Qubes.



Diese Qubes, die als virtuelle Maschinen (VMs) implementiert sind, haben spezifische:

- **Zwecke:** mit einem vordefinierten Satz von einer oder mehreren isolierten Anwendungen, für persönliche oder berufliche Projekte, zur Verwaltung des Netzwerkstapels, der Firewall oder zur Erfüllung anderer benutzerdefinierter Zwecke.
- **Umfang:** vollwertige oder abgespeckte virtuelle Maschinen, die auf gängigen Betriebssystemen wie Fedora, Debian und Windows basieren.
- **Vertrauensebenen:** von vollständig bis nicht existent. Alle Fenster werden in einer einheitlichen Desktop-Umgebung mit fälschungssicheren farbigen Fensterrändern angezeigt, so dass die verschiedenen Sicherheitsstufen leicht erkennbar sind.

Hinweis: Weitere Informationen finden Sie in unserem Glossar und in den häufig gestellten Fragen (FAQ).

Eigenschaften

Starke Isolierung

Isolieren Sie verschiedene Softwarekomponenten so, als ob sie auf separaten physischen Computern installiert wären, indem Sie fortschrittliche Virtualisierungstechniken verwenden.

Vorlagensystem

Verwenden Sie **App Qubes** um ein Root-Dateisystem gemeinsam zu nutzen, ohne die Sicherheit zu beeinträchtigen, indem Sie das innovative **Template-System** verwenden.

Mehrere Betriebssysteme

Verwenden Sie mehrere Betriebssysteme gleichzeitig, darunter **Fedora**, **Debian** und **Windows**.

Wegwerf-Qubes

Erstellen Sie spontan Wegwerf-Qubes **(disposables)**, die sich beim Abschalten selbst zerstören.

Whonix-Integration

Führen Sie **Tor** sicher im ganzen System aus, indem Sie **Whonix mit Qubes** benutzen.

Isolierung der Geräte

Sichere **Gerätehandhabung** durch Isolierung von Netzwerkkarten und USB-Controllern.

GPG aufteilen

Verwenden Sie **Split GPG**, um Ihre privaten Schlüssel sicher aufzubewahren.

U2F-Proxy

Betreiben Sie einen **Qubes U2F-Proxy**, um Ihre Geräte zur Zwei-Faktor-Authentifizierung zu nutzen, ohne dass Ihr Webbrowser den gesamten USB-Stack offenlegt.

Open-Source

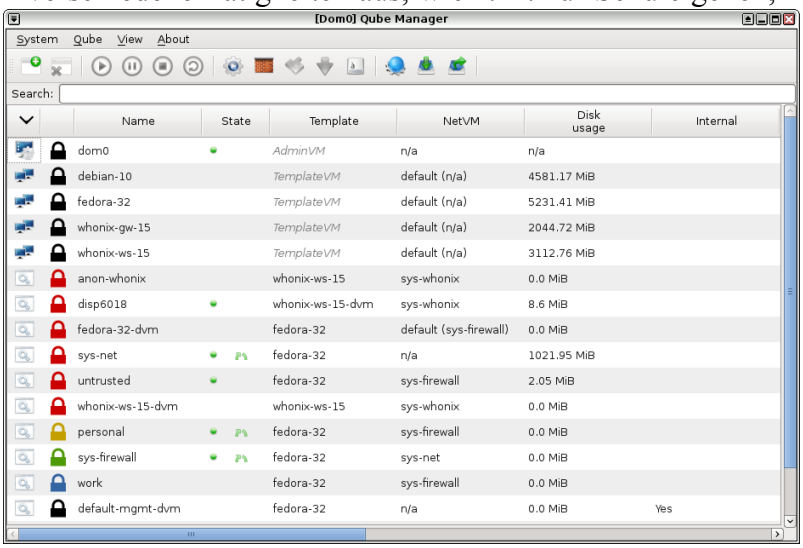
Es steht den Benutzern frei, Qubes OS zu verwenden, zu kopieren und zu modifizieren, und **sie werden dazu ermutigt, dies zu tun**!

Hinweis: Angesichts des technischen Charakters von Qubes OS kann eine vorherige Erfahrung mit Linux hilfreich sein.

Warum Qubes OS?

Die physische Isolierung ist ein gegebener Schutz, der in der digitalen Welt fehlt.

Im Laufe unseres Lebens üben wir verschiedene Tätigkeiten aus, wie z. B. zur Schule gehen, arbeiten, wählen gehen, uns um unsere Familien kümmern und Freunde besuchen. Diese Aktivitäten sind räumlich und zeitlich gebunden: Sie finden isoliert voneinander statt, in ihren eigenen Räumen, die oft eine wesentliche Absicherung darstellen, wie z. B. beim Wählen.

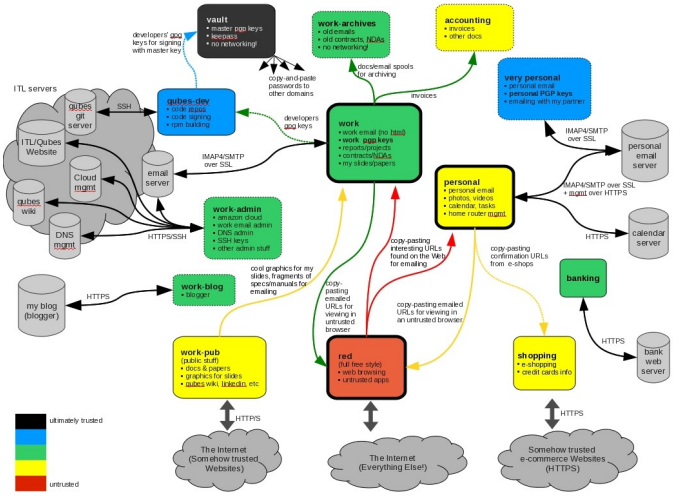


In unserem digitalen Leben ist die Situation ganz anders: Alle unsere Aktivitäten finden in der Regel auf einem einzigen Gerät statt. Dies führt dazu, dass wir uns Sorgen machen, ob es si-

cher ist, auf einen Link zu klicken oder eine App zu installieren, denn wenn wir gehackt werden, ist unsere gesamte digitale Existenz gefährdet.

Qubes beseitigt diese Bedenken, indem es uns ermöglicht, ein Gerät in viele Abteilungen zu unterteilen, ähnlich wie wir ein physisches Gebäude in viele Räume unterteilen. Noch besser ist, dass wir neue Bereiche erstellen können, wann immer wir sie brauchen, und dass es uns ausgefeilte Werkzeuge für die sichere Verwaltung unserer Aktivitäten und Daten in diesen Bereichen bietet.

Qubes ermöglicht es Ihnen, Ihr digitales Leben zu unterteilen

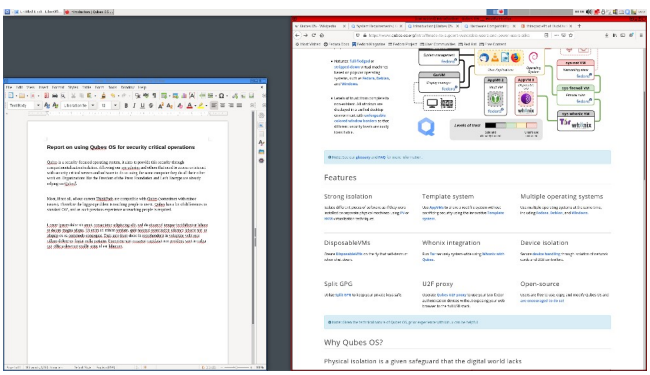


Viele von uns sind zunächst überrascht zu erfahren, dass unsere Geräte nicht die Art von sicherer Abschottung unterstützen, die unser Leben erfordert, und wir sind enttäuscht, dass Softwareanbieter auf generische Schutzmechanismen setzen, die immer wieder neuen Angriffen zum Opfer fallen.

Bei der Entwicklung von Qubes gehen wir davon aus, dass jede Software Fehler enthält. Nicht nur das, sondern die gestressten Softwareentwickler der Welt pumpen in ihrer Eile, Termine einzuhalten, neuen Code in einem atemberaubenden Tempo heraus – viel schneller als die vergleichsweise kleine Population von Sicherheitsexperten jemals hoffen könnte, ihn auf Schwachstellen zu analysieren, geschweige denn alles zu beheben. Anstatt so zu tun, als könnten wir verhindern, dass diese unvermeidlichen Schwachstellen ausgenutzt werden, haben wir Qubes unter der Annahme entwickelt, dass sie ausgenutzt werden. Es ist nur eine Frage der Zeit, bis der nächste Zero-Day-Angriff erfolgt.

In Anbetracht dieser ernüchternden Realität verfolgt Qubes einen äußerst praktischen Ansatz: Eingrenzung, Kontrolle und Eindämmung des Schadens. Es ermöglicht Ihnen, wertvolle Daten von risikoreichen Aktivitäten zu trennen und eine Kreuzkontamination zu verhindern. Das bedeutet, dass Sie alles auf demselben physischen Computer erledigen können, ohne sich Sorgen machen zu müssen, dass ein einziger erfolgreicher Cyberangriff Ihr gesamtes digitales Leben auf einen Schlag zum Erliegen bringt. Tatsächlich hat Qubes deutliche Vorteile gegenüber physischer Trennung (Air Gap).

Entwickelt, um gefährdete Nutzer und Power-User gleichermaßen zu unterstützen



Qubes bietet praktische, brauchbare Sicherheit für gefährdete und aktiv angegriffene Personen wie Journalisten, Aktivisten, Whistleblowers und Forscher. Qubes wurde in dem Bewusstsein entwickelt, dass Menschen Fehler machen, und es ermöglicht Ihnen, sich vor Ihren eigenen Fehlern zu schützen. Es ist ein Ort, an dem Sie unbesorgt auf Links klicken, An-

hänge öffnen, Geräte anschließen und Software installieren können. Es ist ein Ort, an dem *Sie* die Kontrolle über Ihre Software haben, nicht umgekehrt. (Sehen Sie sich einige Beispiele dafür an, wie verschiedene Benutzertypen ihren Arbeitsplatz organisieren).

Qubes ist auch mächtig. Organisationen wie die Freedom of the Press Foundation, Mullvad und Let's Encrypt verlassen sich auf Qubes, wenn sie kritische Datenschutz- und Sicherheitstechnologien für das Internet entwickeln und pflegen, auf die sich wiederum unzählige Nutzer auf der ganzen Welt jeden Tag verlassen. Renommierte Sicherheitsexperten wie Edward Snowden, Daniel J. Bernstein, Micah Lee, Christopher Soghoian, Isis Agora Lovecruft, Peter Todd, Bill Budington und Kenn White nutzen und empfehlen Qubes.

Qubes ist eines der wenigen Betriebssysteme, das die Sicherheit seiner Nutzer über alles andere stellt. Es ist und bleibt freie und quelloffene Software, denn das grundlegende Betriebssystem, das die Kerninfrastruktur unseres digitalen Lebens bildet, *muss* frei und quelloffen sein, um vertrauenswürdig zu sein.

ERSTE SCHRITTE

Nachdem Sie Qubes OS heruntergeladen und installiert haben, ist es an der Zeit, sich an die Arbeit zu machen! (Wenn Sie sich bereits auskennen, können Sie gleich mit der Organisation Ihrer Qubes beginnen).

Die Grundlagen

Qubes OS ist ein Betriebssystem, das aus isolierten Sicherheitsdomänen („Kompartimenten“) besteht, den Qubes. Sie könnten zum Beispiel einen Arbeits-Qube, einen persönlichen Qube, einen Banking-Qube, einen Web-Browsing-Qube und so weiter haben. Sie können so viele Qubes haben, wie Sie wollen! Die meiste Zeit werden Sie einen App-Qube verwenden, einen Qube, der für die Ausführung von Softwareprogrammen wie Webbrowsern, E-Mail-Clients und Textverarbeitungsprogrammen gedacht ist. Jeder App-Qube basiert auf einer anderen Art von Qube, einer Vorlage („Template“). Mehr als ein Qube kann auf demselben Template basieren. Wichtig ist, dass ein Qube sein Template in keiner Weise verändern kann. Das bedeutet, dass, wenn ein Qube jemals kompromittiert wird, sein Template und alle anderen Qubes, die auf diesem Template basieren, sicher bleiben. Das macht Qubes OS so sicher. Selbst wenn ein Angriff erfolgreich ist, ist der Schaden auf einen einzelnen Qube begrenzt.

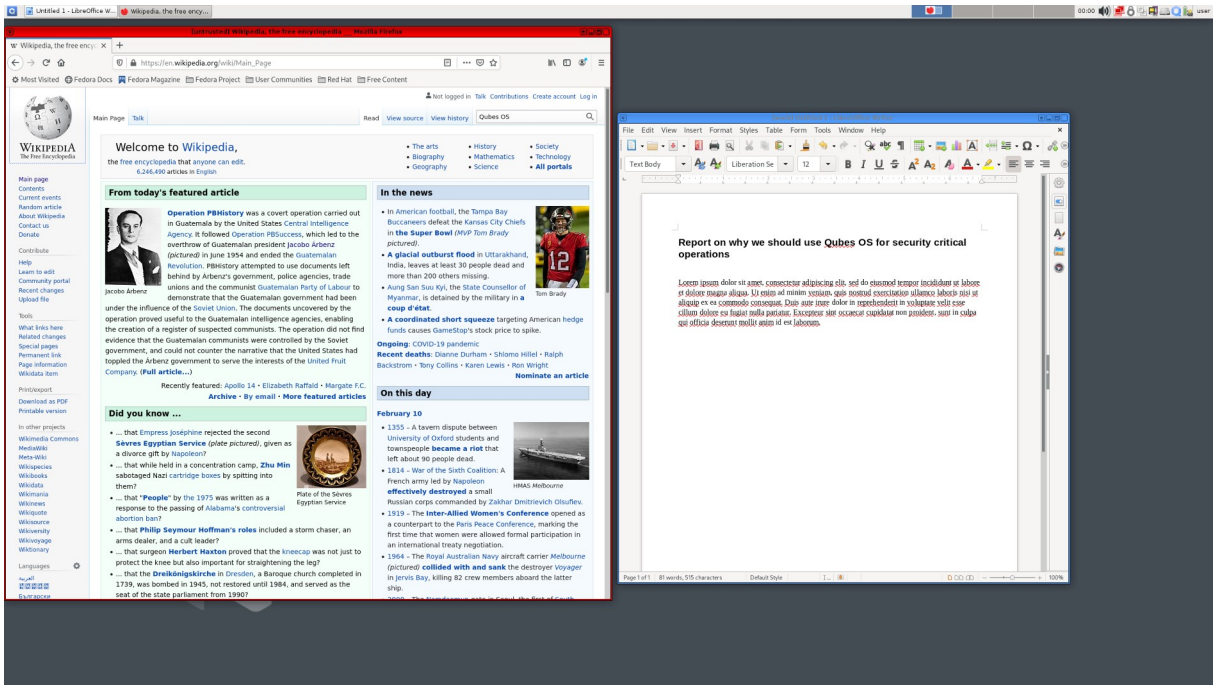
Angenommen, Sie möchten Ihren Lieblings-Webbrowser in mehreren verschiedenen Qubes verwenden. Sie würden den Webbrowser in einer Vorlage installieren, dann könnte jeder Qube, der auf diesem Template basiert, die Webbrowser-Software ausführen (während es immer noch verboten ist, das Template und alle anderen Qubes zu verändern). Auf diese Weise müssen Sie den Webbrowser nur ein einziges Mal installieren, und die Aktualisierung des Templates dient zur Aktualisierung aller darauf basierenden Qubes. Dieses elegante Design spart Zeit und Platz und erhöht gleichzeitig die Sicherheit.

In Ihrem System gibt es auch einige „Service“-Qubes. Jeder Qube, der eine Verbindung zum Internet herstellt, tut dies über einen netzbetreuenden Service-Qube. Wenn Sie auf USB-Geräte zugreifen müssen, übernimmt das ein anderer Service-Qube. Außerdem gibt es einen Verwaltungs-Qube der automatisch viele Aufgaben im Hintergrund erledigt. In den meisten Fällen werden Sie sich nicht darum kümmern müssen, aber es ist gut zu wissen, dass es ihn gibt. Wie die App-Qubes basieren auch die Service-Qubes und die Management-Qubes auf Templates. Templates werden in der Regel nach ihrem Betriebssystem (oft eine Linux-Distribution) und der entsprechenden Versionsnummer benannt. Es gibt viele gebrauchsfertige Templates, aus denen Sie auswählen können, und Sie können so viele herunterladen, wie Sie möchten.

Zu guter Letzt gibt es noch einen ganz besonderen Admin Qube der, wie der Name schon sagt, zur Verwaltung Ihres gesamten Systems dient. Es gibt nur einen Admin-Qube, und der heißt `dom0`. Man kann ihn sich als den Master-Qube vorstellen, der die ultimative Macht über alles hat, was in Qubes OS passiert. `dom0` ist vertrauenswürdiger als jeder andere Qube. Sollte `dom0` jemals kompromittiert werden, wäre es „Game Over“. Das gesamte System wäre effektiv kompromittiert. Deshalb ist alles in Qubes OS speziell darauf ausgerichtet, `dom0` zu schützen und sicherzustellen, dass dies nicht passiert. Aufgrund seiner übergreifenden Bedeutung hat `dom0` keine Netzwerkverbindung und wird nur für die Ausführung der Desktop-Umgebung und des Fenstermanagers verwendet. `dom0` sollte niemals für etwas anderes verwendet werden. Insbesondere sollten Sie niemals Benutzeranwendungen in `dom0` ausführen. (Dafür sind Ihre App-Qubes da!)

Farbe und Sicherheit

Sie wählen eine **Farbe** für jeden Qube aus einer vordefinierten Reihe von Farben aus. Der Rahmen jedes Fensters auf Ihrem Desktop wird entsprechend der Farbe des jeweiligen Qube eingefärbt. Diese farbigen Rahmen helfen Ihnen, den Überblick zu behalten, zu welchem Qube jedes Fenster gehört und wie vertrauenswürdig es ist. Dies ist besonders hilfreich, wenn Sie dieselbe Anwendung in mehreren Qubes gleichzeitig laufen lassen. Wenn Sie zum Beispiel in einem Qube bei Ihrem Bankkonto angemeldet sind, während Sie in einem anderen Qube im Internet surfen, möchten Sie nicht versehentlich Ihr Bankpasswort in der letzteren eingeben! Die farbigen Rahmen helfen, solche Fehler zu vermeiden.



Die meisten Qubes-Benutzer assoziieren Rot mit dem, was nicht vertrauenswürdig und gefährlich ist (wie eine rote Ampel: Stopp! Gefahr!), Grün mit dem, was sicher und vertrauenswürdig ist, und Gelb und Orange mit Dingen in der Mitte. Dieses Farbschema umfasst auch Blau und Schwarz, die in der Regel so interpretiert werden, dass sie zunehmend vertrauenswürdigere Bereiche als Grün anzeigen, wobei Schwarz ultimativ vertrauenswürdig ist. Die Farbe und die damit verbundenen Bedeutungen sind jedoch letztlich Ihnen überlassen. Das System selbst behandelt die Farben nicht unterschiedlich. Wenn Sie zwei identische Qubes erstellen – z. B. schwarz und rot – sind sie gleich, bis Sie anfangen, sie unterschiedlich zu verwenden. Es steht Ihnen frei, die Farben so zu verwenden, wie es für Sie am sinnvollsten ist. Sie könnten zum Beispiel drei oder vier Qubes für Arbeitstätigkeiten verwenden und ihnen allen die gleiche Farbe geben – oder aber unterschiedliche Farben. Das ist ganz Ihnen überlassen.

Benutzeroberfläche

Bei Betriebssystemen wie Windows und macOS ist die Desktop-Umgebung unveränderbar und Teil des Betriebssystems. Bei Linux ist jede beliebige Desktop-Umgebung eine Option. Qubes OS wird mit XFCE als Standard-Desktop-Umgebung installiert, aber es unterstützt auch KDE sowie die Fenstermanager i3 und AwesomeWM.

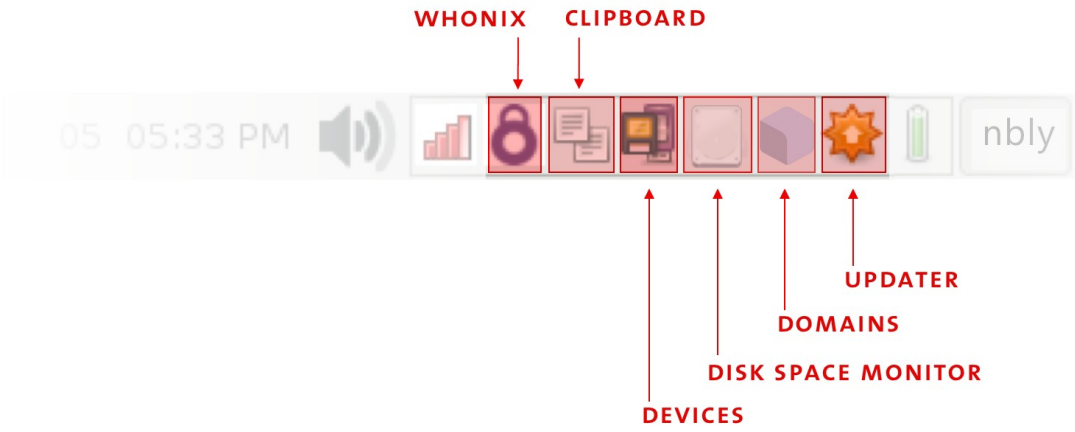
Die Leiste am oberen Rand Ihres Bildschirms in Qubes 4.1 enthält die folgenden XFCE-Komponentenbereiche:

- Die **Ablage (Tray)**, in der sich viele funktionale Widgets befinden.
- **Spaces**, eine Schnittstelle für virtuelle Desktops. Virtuelle Desktops haben keine inhärenten Sicherheitsisolationseigenschaften, aber einige Benutzer finden sie nützlich, um Dinge zu organisieren.
- Die **Taskleiste (Task Bar)**, in der sich die Schaltflächen für offene und ausgeblendete Fenster befinden.
- Das **App-Menü**, in dem Sie eine Anwendung innerhalb eines Qube öffnen, ein `dom0`-Terminal öffnen, auf administrative UI-Tools wie den Qube Manager zugreifen oder Einstellungsfelder für Ihre Desktop-Umgebung aufrufen können.

Um mehr darüber zu erfahren, wie Sie Ihre Desktop-Umgebung anpassen können, empfehlen wir Ihnen, einige Zeit mit der XFCE-Dokumentation zu verbringen.

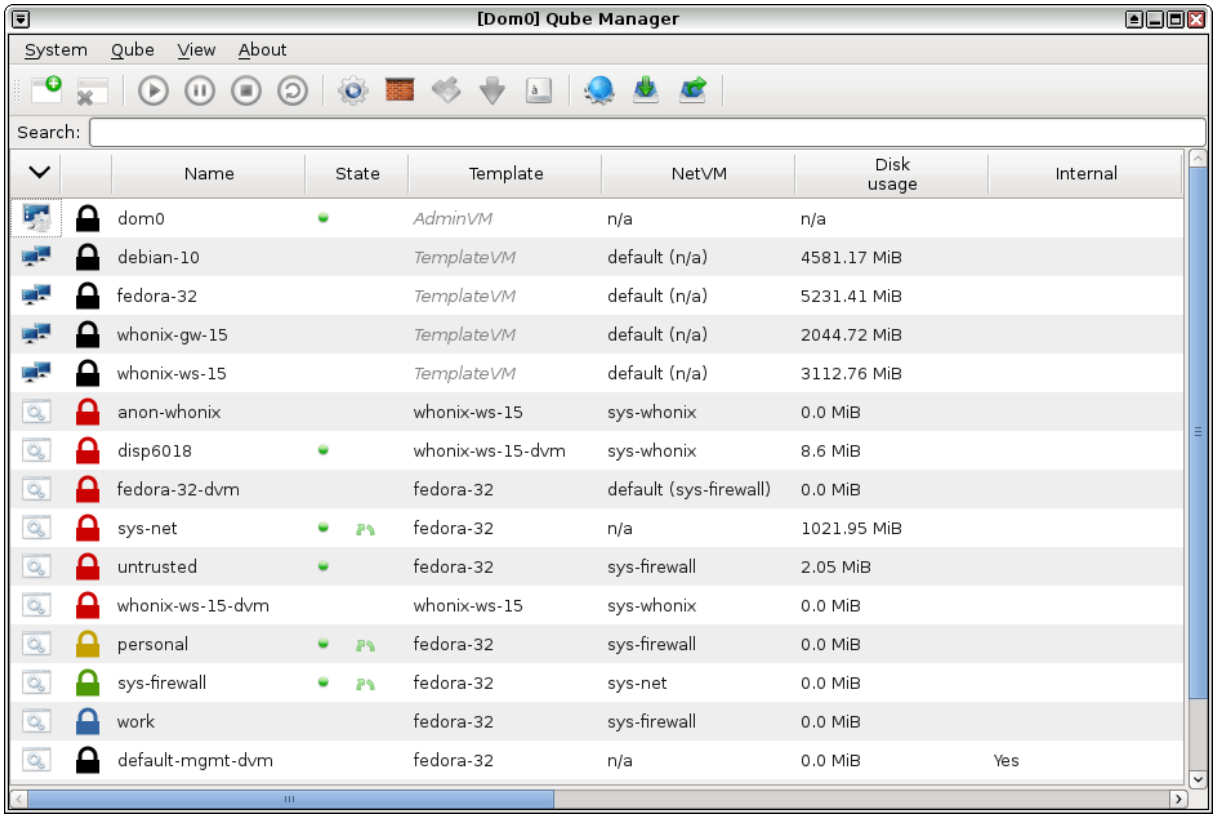
Es gibt mehrere Tray Widgets, die nur in Qubes OS vorhanden sind:

- Das **Whonix SDWDate Widget** ermöglicht es Ihnen, die Tor-Verbindung in Ihrem `sys-whonix` Qube zu kontrollieren.
- Mit der **Qubes-Zwischenablage** können Sie ganz einfach Text aus `dom0` kopieren.
- Das **Qubes-Geräte-Widget** ermöglicht es Ihnen, Geräte – wie USB-Laufwerke und Kameras – an Qubes anzuschließen und zu entfernen.
- Das **Qubes Festplattenplatz-Widget** zeigt Ihnen, wie viel Speicherplatz Sie verbrauchen. Es benachrichtigt Sie, wenn Ihnen der Speicherplatz ausgeht.
- Das **Qubes Domains** Widget ermöglicht es Ihnen, laufende Qubes zu verwalten, sie ein- und auszuschalten und die RAM- und CPU-Auslastung zu überwachen.
- Das **Qubes** Updater-Widget informiert Sie, wenn Updates verfügbar sind und hilft Ihnen, diese zu installieren.



Qube-Manager

Um alle Ihre Qubes gleichzeitig zu sehen, können Sie den **Qube Manager** verwenden (gehen Sie zum App-Menü → Qubes Tools → Qube Manager), der den Status aller Qubes in Ihrem System anzeigt, auch derer, die nicht laufen.



Befehlszeilenschnittstelle

Alle Aspekte von Qubes OS können über Kommandozeilen-Tools gesteuert werden. Das Öffnen eines Terminalemulators in `dom0` kann auf verschiedene Weise erfolgen:

- Rufen Sie das App-Menü auf und wählen Sie oben **Terminal-Emulator**.

- Drücken Sie `Alt+F3` und suchen Sie nach `xfce terminal`.
- Klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie **Terminal hier öffnen**.

Terminal-Emulatoren können auch in anderen Programmen als normale Programme ausgeführt werden. Verschiedene Kommandozeilen-Tools werden in diesem Leitfaden beschrieben, und die gesamte Referenz finden Sie hier.

Erster Systemstart

Wenn Sie Qubes OS installieren, sind einige Qubes für Sie vorkonfiguriert:

- **Templates:** `fedora-XX` und `debian-XX` (`XX` steht für die Versionsnummer)
- **Verwaltungs-Qube:** `dom0`
- **Service-Qubes:** `sys-usb`, `sys-net`, `sys-firewall` und `sys-whonix`
- **App-Qubes**, die so konfiguriert sind, dass sie der Sicherheit Priorität einräumen, indem sie Aufgaben und Datentypen unterteilen: `work`, `personal`, `untrusted` und `vault`. (Es gibt nichts Besonderes an diesen Qubes. Wenn Sie einen schwarzen Qube erstellen und ihn `vault` nennen würden, wäre er der gleiche wie der vorkonfigurierte `vault` Qube. Das sind nur Vorschläge, um Ihnen den Einstieg zu erleichtern.)

Eine Vielzahl von Open-Source-Anwendungen wie Dateimanager, Befehlszeilen-Terminals, Druckermanager, Texteditoren und „Applets“ zur Konfiguration verschiedener Dinge wie Audio oder Teile der Benutzeroberfläche werden ebenfalls standardmäßig installiert – meist innerhalb der Templates. Die meisten werden mit jedem Template gebündelt.

Hinzufügen, Entfernen und Auflisten von Qubes

Mit der Option **Qubes VM erstellen** im App-Menü können Sie ganz einfach einen neuen Qube erstellen. Wenn Sie Qubes hinzufügen oder entfernen möchten, verwenden Sie einfach die Schaltflächen **Hinzufügen** und **Entfernen** des Qube Managers. Sie können Qubes auch über die Kommandozeile hinzufügen, entfernen und auflisten, indem Sie die folgenden Tools verwenden:

- `qvm-create`
- `qvm-remove`
- `qvm-ls`

Wie viele Qubes brauche ich?

Das ist eine gute Frage, aber es gibt keine allgemeingültige Antwort. Es kommt auf die Struktur Ihres digitalen Lebens an, und die ist bei jedem zumindest ein wenig anders. Wenn Sie Ihr System beruflich nutzen wollen, kommt es auch darauf an, was für einen Job Sie haben.

Es ist eine gute Idee, mit den vom Installationsprogramm automatisch erstellten Qubes zu beginnen: `work`, `personal`, `untrusted` und `vault`. Wenn Sie das Gefühl haben, dass eine bestimmte Aktivität nicht in einen der vorhandenen Qubes passt oder Sie einen Teil Ihres

Lebens aufteilen möchten, können Sie einfach einen neuen Qube dafür erstellen. Sie können auch alle Dateien, die Sie benötigen, einfach in den neu erstellten Qube kopieren.

Möchten Sie einige Beispiele sehen? Schauen Sie sich unseren ausführlichen Leitfaden zur Organisation Ihrer Qubes an, der auf der Grundlage unserer Nutzerforschung und der jahrelangen Erfahrung erfahrener Qubes-Benutzer mehrere häufige Anwendungsfälle beschreibt.

Sichere Praktiken

Es ist *sehr wichtig*, Qubes auf dem neuesten Stand zu halten, um sicherzustellen, dass Sie über die neuesten Sicherheitsupdates verfügen. Häufige Aktualisierungen sind eine der besten Möglichkeiten, um vor neuen Bedrohungen geschützt zu sein.

Es ist auch *sehr wichtig*, regelmäßig Backups zu erstellen, damit Sie Ihre Daten nicht unerwartet verlieren. Mit dem Qubes-Backup-System können Sie dies auf sichere und einfache Weise tun.

Anleitungen

Hier finden Sie einige grundlegende Aufgaben, die Sie wahrscheinlich häufig ausführen werden und die für Qubes als Multi-Environment-System einzigartig sind. Eine vollständige Liste finden Sie in der How-To Anleitungen Abschnitt in den Dokumenten.

- Wie Sie Ihre Qubes Organisieren
- Wie Sie Ihr System aktualisieren
- Wie Sie sichern, wiederherstellen und migrieren
- Wie Sie Text kopieren und einfügen
- Wie Sie Dateien kopieren und verschieben
- Wie Sie von `dom0` kopieren
- Wie Sie Software installieren
- Wie Sie Geräte (Blockspeicher, USB- und PCI-Geräte verwenden

Wenn Sie Probleme haben, besuchen Sie bitte die Seite Hilfe, Unterstützung, Mailinglisten und Forum.

Kompatible Hardware

Stellen Sie sicher, dass Ihre Hardware die Systemanforderungen erfüllt, da Qubes OS nicht auf jedem Computertyp laufen kann. Sie können sich auch über Qubes-zertifizierte Hardware informieren und einen Blick auf die Hardware-Kompatibilitätsliste (HCL) werfen.

Herunterladen

Laden Sie eine ISO-Datei herunter, erfahren Sie, wie Sie ihre Authentizität überprüfen können, und folgen Sie unserer Anleitung zur Installation von Qubes OS. Suchen Sie nach dem Quellcode? Sie finden ihn auf GitHub.

Dokumentation

Schauen Sie sich unsere umfangreiche Bibliothek mit Dokumentationen für Benutzer und Entwickler von Qubes OS an. Sie können uns sogar helfen, sie zu verbessern!

WIE SIE IHRE QUBES ORGANISIEREN

Wenn Leute zum ersten Mal von Qubes OS erfahren, ist ihre erste Reaktion oft: „Wow, das sieht wirklich cool aus! Aber... was kann ich damit eigentlich machen?“ Es ist nicht immer offensichtlich, welche Qubes Sie erstellen sollten, was Sie in jeder Qube tun sollten und ob Ihre organisatorischen Ideen aus Sicherheits- oder Nutzungssicht sinnvoll sind.

Jeder Qube ist im Grunde ein sicheres Fach, und Sie können so viele davon erstellen, wie Sie möchten, und sie auf verschiedene Weise miteinander verbinden. Sie sind eine Art Legosteine, mit denen Sie bauen können, was Sie wollen. Aber wenn man nicht weiß, was man bauen soll, kann diese unbegrenzte Freiheit entmutigend sein. Es ist ein bisschen so, als ob man auf ein leeres Dokument starrt, wenn man sich zum ersten Mal hinsetzt, um etwas zu schreiben. Die Möglichkeiten sind endlos, und Sie wissen vielleicht gar nicht, wo Sie anfangen sollen!

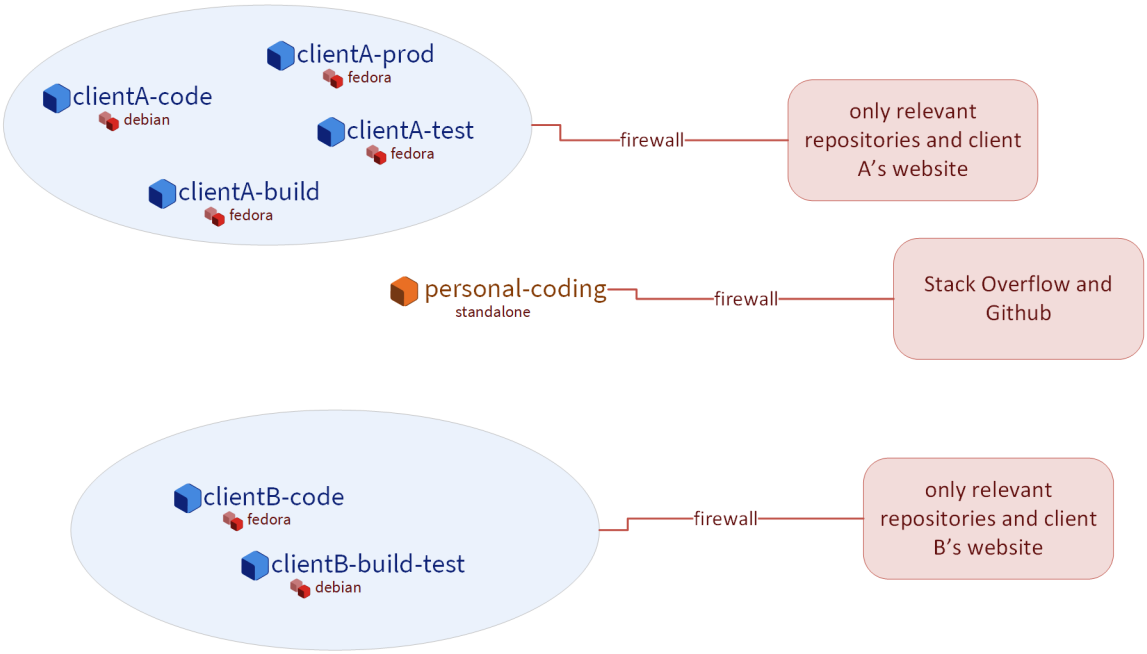
Die Wahrheit ist, dass Ihnen niemand genau sagen kann, wie Sie Ihren Lebenslauf gestalten sollten, denn es gibt keine einzig richtige Antwort auf diese Frage. Es hängt von Ihren Bedürfnissen, Wünschen und Vorlieben ab. Jeder Benutzer hat eine andere optimale Konfiguration. Was wir jedoch tun können, ist, Ihnen einige anschauliche Beispiele zu geben, die auf Fragebögen und Interviews mit Qubes-Benutzern und -Entwicklern sowie auf unseren persönlichen Erfahrungen und Erkenntnissen aus der jahrelangen Nutzung von Qubes basieren. Vielleicht können Sie einige dieser Beispiele an Ihre eigene Situation anpassen. Noch wichtiger ist jedoch, dass Sie durch die Erläuterung der Gründe für verschiedene Entscheidungen lernen, wie Sie denselben Denkprozess auf Ihre eigenen organisatorischen Entscheidungen anwenden können. Lassen Sie uns beginnen!

Alice, die Software-Entwicklerin

Alice ist eine freiberufliche Entwicklerin, die an mehreren Projekten für verschiedene Kunden gleichzeitig arbeitet. Die Projekte haben unterschiedliche Anforderungen und oft auch unterschiedliche Build-Umgebungen. Sie hat für jedes Projekt einen eigenen Satz von Anforderungen. Sie hält sie organisiert, indem sie sich ein Namensschema ausdenkt, wie z.B.:

```
clientA-code
clientA-build
clientA-test
clientA-prod
projectB-code
projectB-build-test
projectB-prod
...
```

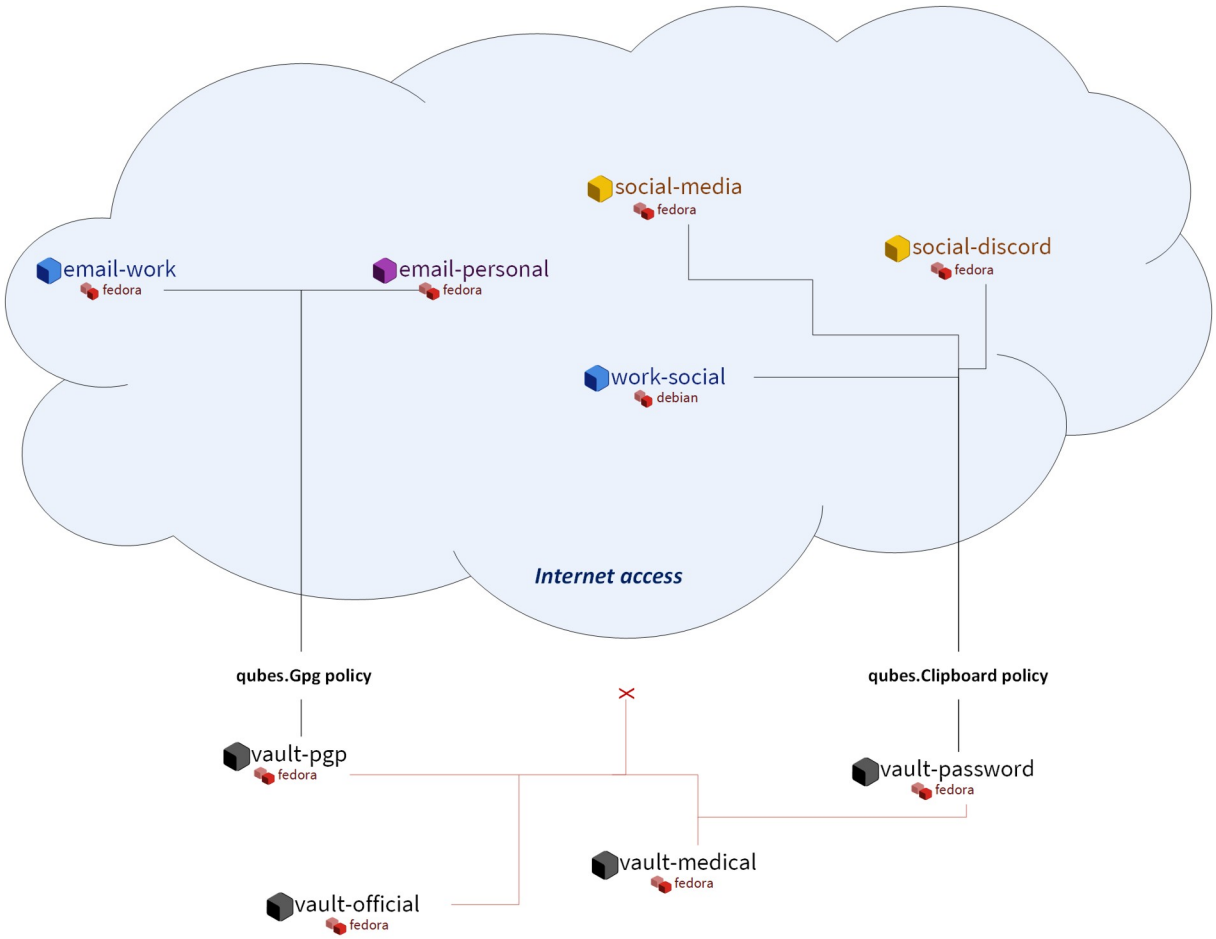
Dies hilft ihr, Gruppen von Qubes in einem Satz zu organisieren. Einige ihrer Qubes basieren auf Debian Templates, während andere auf Fedora Templates beruhen. Der Grund dafür ist, dass einige Softwarepakete in der einen Distribution besser verfügbar sind als in der anderen. Alices Einrichtung sieht wie folgt aus:



- **Mehrere Qubes zum Schreiben von Code.**
  Hier führt sie ihre IDE aus, überträgt den Code und signiert ihre Übertragungen. Diese Qubes basieren auf verschiedenen Templates, je nachdem, welche Tools und welche Entwicklungsumgebung sie benötigt. Im Allgemeinen hat Alice gerne für jeden Kunden oder jedes Projekt einen eigenen Qube dieser Art. So behält sie den Überblick und vermeidet, dass sie versehentlich Zugangsdaten oder Kundencode verwechselt, was katastrophale Folgen haben könnte. Außerdem kann sie so ihren Kunden wahrheitsgemäß sagen, dass ihr Code immer sicher von dem aller anderen Kunden isoliert ist. Sie benutzt gerne die Qubes Firewall, um den Netzwerkzugang dieser Qubes nur auf die Code-Repositories zu beschränken, die sie in diesem Qube benötigt, um zu vermeiden, dass sie versehentlich mit irgendetwas anderem in ihrem lokalen Netzwerk oder im Internet interagiert. Alice hat auch einige Qubes dieser Art für persönliche Programmierprojekte, an denen sie nur zum Spaß arbeitet, wenn sie „Freizeit" hat (was auch immer das sein mag).

- **Mehrere Qubes zum Bauen und Testen.**
  Auch hier hat Alice normalerweise für jeden Kunden oder jedes Projekt einen davon, um die Dinge zu organisieren. Dies kann jedoch ziemlich umständlich und speicherintensiv werden, wenn viele solcher Qubes gleichzeitig laufen, so dass Alice manchmal denselben Qube für das Bauen und Testen oder für mehrere Projekte, die dieselbe Umgebung benötigen, verwendet, wenn sie entscheidet, dass die marginalen Vorteile einer zusätzlichen Aufteilung die Mühe nicht wert sind. Hier holt sie sich alle Abhängigkeiten, die sie braucht, kompiliert ihren Code, führt ihre Build-Toolchain aus und testet ihre Arbeitsergebnisse. In einigen Fällen hält sie es für sinnvoll, dafür Standalones zu verwenden, damit es einfacher ist, verschiedene Softwareteile schnell zu installieren, ohne mit dem Neustart des Templates und einem App-Qube jonglieren zu müssen. Außerdem findet sie es manchmal notwendig (oder einfach nur praktisch), Änderungen an den Konfigurationsdateien im Root-Dateisystem vorzunehmen, und sie möchte nicht befürchten müssen, dass diese Änderungen bei einem App-Qube-Neustart verloren gehen. Sie weiß, dass sie bind-dirs verwenden könnte, um diese Änderungen dauerhaft zu machen, aber manchmal möchte sie sich nicht mit all dem aufhalten und denkt, dass es sich nicht lohnt, nur für diesen einen Qube. Insgeheim ist sie froh, dass Qubes OS sie nicht verurteilt und ihr einfach die Freiheit gibt, Dinge zu tun, wie sie will, während sie alles sicher unterteilt. In solchen Momenten tröstet sie sich mit dem

Wissen, dass die Dinge in einem Qube chaotisch und unorganisiert sein können, während ihr digitales Leben insgesamt gut organisiert bleibt.



- **Mehrere E-Mail- Qubes.**
  Da Alice eine Liebhaberin der Kommandozeile ist, verwendet sie gerne einen terminalbasierten E-Mail-Client, so dass sowohl ihre Arbeits- als auch ihre private E-Mail-Qubes auf einer Vorlage mit installiertem Mutt basieren. Die E-Mail-Qubes, mit denen sie PGP-signierte und verschlüsselte E-Mails sendet und empfängt, greifen sicher auf die privaten Schlüssel in ihrem PGP-Backend-Qube zu (mehr dazu unten). Um sich vor bösartigen Anhängen zu schützen, hat sie Mutt so konfiguriert, dass alle angehängten Dateien in Wegwerf-Qubes (Disposable Qubes) geöffnet werden.

- **Mehrere Qubes für Kommunikationstools,**
  wie Signal, Slack, Zoom, Telegram, IRC und Discord. Hier führt sie Telefonkonferenzen durch und chattet mit Kunden. Sie verwendet USB Passthrough, um ihre Webcam je nach Bedarf an jeden Qube anzuschließen, und trennt sie danach wieder ab. Ebenso gibt sie jedem Qube Zugriff auf ihr Mikrofon, solange es benötigt wird, und nimmt den Zugriff danach wieder zurück. Auf diese Weise muss sie sich nicht auf die Stummschalttaste eines bestimmten Video-Chatprogramms verlassen und muss sich keine Sorgen machen, dass sie ausspioniert wird, wenn sie gerade nicht telefoniert. Sie hat auch eine Vorliebe für Social-Media-Plattformen wie Twitter, Reddit und Hacker News, um sich zu vernetzen und über neue Entwicklungen auf dem Laufenden zu bleiben (zumindest behauptet sie das; in Wirklichkeit geht es dort hauptsächlich um Fehden über die Überlegenheit von Programmiersprachen, Kriege zwischen Vim und Emacs und Kreuzzüge zwischen Tabs und Leerzeichen).

- **Ein GPG-Backend-Tresor.**
  Tresore sind komplett offline und vom Netzwerk isoliert. Dieser spezielle Tresor enthält die privaten Schlüssel von Alice (z.B. für Code Signing und E-Mail) und wird von mehreren anderen „Frontend"-Qubes über das Split GPG-System sicher angesprochen. Split GPG erlaubt nur den von Alice explizit autorisierten Frontend-Qubes, PGP-Operationen (z.B. Signieren und Verschlüsseln) im Backend-Tresor anzufordern. Selbst dann hat kein Qube jemals direkten Zugang zu Alices privaten Schlüsseln, außer dem Backend-Tresor selbst.

- **Ein Passwortmanager-Tresor.**
  Dies ist ein weiterer vollständig offline, vom Netzwerk isolierter Qube, in dem Alice ihren Offline-Passwortmanager, KeePassXC, verwendet, um alle ihre Benutzernamen und Passwörter zu speichern. Sie verwendet das sichere Kopier- und Einfügesystem, um Anmeldedaten schnell in andere Qubes zu kopieren, wenn sie sich bei etwas anmelden muss.

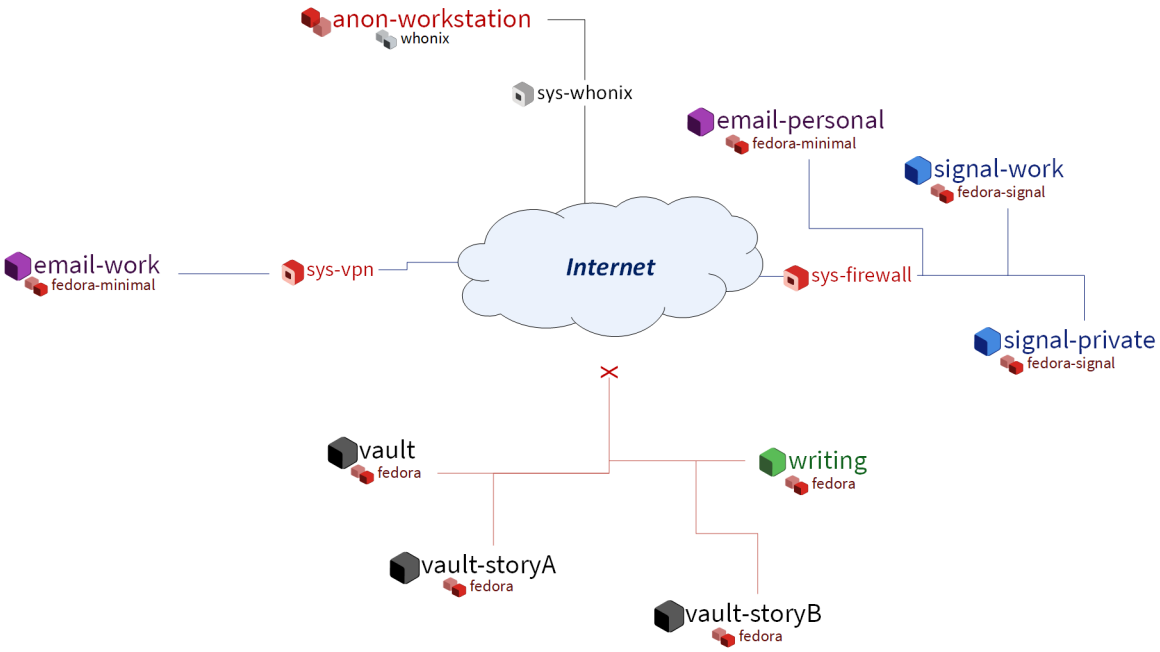
- **Persönliche Qubes.**
  Eines der Dinge, die Alice an Qubes am meisten liebt, ist, dass sie es sowohl für die Arbeit als auch für private Dinge nutzen kann, ohne sich Gedanken über eine gegenseitige Verunreinigung machen zu müssen. Dementsprechend hat sie mehrere Qubes, die sich auf ihr Privatleben beziehen. Zum Beispiel hat sie einen Offline-Tresor, in dem ihre medizinischen Dokumente, Testergebnisse und Impfungen gespeichert sind. Sie hat einen weiteren Offline-Tresor für ihre Regierungsdokumente, ihre Geburtsurkunde, Scans ihres Reisepasses und so weiter. Sie hat auch einige persönliche Konten in sozialen Medien in einem separaten Tresor, um mit Familienmitgliedern und Freunden aus der Schule in Kontakt zu bleiben.

Wenn sie ihre Arbeit für einen bestimmten Kunden beendet hat, schickt Alice ihre Ergebnisse ab, sichert die Qubes, die die Arbeit für diesen Kunden enthalten, und löscht sie aus ihrem System. Wenn sie diese Qubes jemals wieder benötigt oder sie einfach nur referenzieren möchte, kann sie sie einfach aus ihrer Sicherungskopie wiederherstellen, und der interne Status jedes Qube wird genau so sein, wie er war, als sie das Projekt beendet hat.

Bob, der Enthüllungsjournalist

Im Rahmen seiner Recherche und Berichterstattung ist Bob häufig gezwungen, mit verdächtigen Dateien zu arbeiten, die oft von anonymen Quellen stammen. So kann es vorkommen, dass er eine E-Mail mit einem Anhang erhält, in dem behauptet wird, es handele sich um einen Hinweis auf eine Geschichte, an der er gerade arbeitet. Natürlich weiß er, dass es sich dabei genauso gut um Malware handeln könnte, die seinen Computer infizieren soll. Qubes OS ist für Bob unverzichtbar, da es ihm ermöglicht, all diese verdächtigen Daten sicher zu handhaben und sie so zu isolieren, dass sie nicht den Rest seines Computers infizieren können.

Bob ist kein super technischer Typ. Er zieht es vor, seine Werkzeuge einfach zu halten, damit er sich auf das konzentrieren kann, was ihm wichtig ist: die Wahrheit aufzudecken, die Schuldigen zu entlarven, die Unschuldigen zu entlasten und Licht in die dunklen Ecken der Gesellschaft zu bringen. Er beschäftigt sich nicht mit den technischen Details der Funktionsweise seines Computers, aber er ist sich bewusst, dass ständig Leute gehackt werden und dass die Art seiner Arbeit ihn zu einem Ziel machen könnte. Er möchte seine Quellen, seine Kollegen, seine Familie und sich selbst schützen, und er weiß, dass die Computersicherheit dabei eine wichtige Rolle spielt. Er hat einen Qubes-Laptop, den er nur für die Arbeit verwendet und der Folgendes enthält:



- **Ein Offline-Qube zum Schreiben.**
  Darauf läuft nur LibreOffice Writer. Hier schreibt Bob alles, was er schreibt. Dieses Fenster ist normalerweise neben einem anderen Fenster geöffnet, das Recherchen oder Material aus einer Quelle enthält.

- **Mehrere E-Mail-Qubes.**
  Einer ist für den Empfang von E-Mails aus der breiten Öffentlichkeit. Ein anderer ist für E-Mails an seinen Redakteur und seine Kollegen gedacht. Beide basieren auf einem minimalen Template mit installiertem Thunderbird. Er hat beide so konfiguriert, dass alle Anhänge in Wegwerfprogrammen (Disposables) geöffnet werden, die offline sind, für den Fall, dass ein Anhang eine Signalanwendung enthält, die versucht, nach Hause zu telefonieren.

- **Whonix Qubes.**
  Er hat den Standarddienst `sys-whonix` von Qubes, um einen Torifizierten Netzwerkzugang bereitzustellen, und er benutzt den Wegwerf-Qube `anon-Workstation`, um den Tor-Browser zu benutzen, um für die Geschichten, die er schreibt, zu recherchieren. Da es sich oft um heikle Themen handelt, in die einflussreiche Personen verwickelt sein könnten, ist es wichtig, dass er diese Recherchen mit einem gewissen Grad an Anonymität durchführen kann. Er möchte nicht, dass die Personen, gegen die er ermittelt, wissen, dass er über sie recherchiert. Er möchte auch nicht, dass seine Netzwerkanfragen zu seiner Arbeits- oder Privat-IP-Adresse zurückverfolgt werden. Whonix hilft ihm bei diesen beiden Anliegen. Er hat auch ein anderes Whonix-basiertes Template für den anonymen Empfang von Hinweisen über Tor, da einige hochriskante Hinweisgeber, mit denen er zu tun hatte, sagten, dass sie mit keiner anderen Form der Kommunikation ein Risiko eingehen können.

- **Zwei Qubes für Signal.**
  Bob hat zwei Qubes für die Signal-App (beide auf der gleichen Vorlage, auf der auch die Signal-Desktop-App installiert ist). Einer ist mit seiner eigenen Handynummer verknüpft, um mit Kollegen und anderen bekannten, vertrauenswürdigen Kontakten zu kommunizieren. Beim anderen handelt es sich um eine öffentliche Nummer, die als zusätzliche Möglichkeit für Quellen dient, ihn vertraulich zu erreichen. Dies ist beson-

ders nützlich für Personen, die Tor nicht benutzen, aber für die eine unverschlüsselte Kommunikation gefährlich sein könnte.

- **Mehrere Datentresore.**
  Wenn jemand Bob Material schickt, das sich als nützlich erweist, oder wenn er bei seinen eigenen Nachforschungen auf nützliches Material stößt, speichert er eine Kopie in einem komplett offline, vom Netzwerk isolierten Tresor-Qube. Bei den meisten dieser Dateien handelt es sich um PDF-Dateien und Bilder, einige sind jedoch auch Audiodateien, Videos und Textdateien. Da die meisten von ihnen aus unbekannten oder nicht vertrauenswürdigen Quellen stammen, ist sich Bob nicht sicher, ob es sicher wäre, sie alle in denselben Tresor zu legen, also erstellt er für den Fall der Fälle verschiedene Tresore (normalerweise einen für jede Geschichte oder jedes Thema). Dies hat den Nebeneffekt, dass die Dinge besser geordnet werden können.

- **Ein VPN Qube und zugehörige Qubes für den Zugriff auf Arbeitsressourcen.**
  Auf die Server bei der Arbeit kann nur vom Netzwerk des Unternehmens aus zugegriffen werden. Bob hat daher bestimmte Qubes, die mit einem VPN-Qube verbunden sind, damit er seine Arbeit hochladen und auf alles, was er im lokalen Netzwerk braucht, zugreifen kann, wenn er nicht vor Ort ist.

- **Ein Passwortmanager-Tresor.**
  Bob speichert alle seine Anmeldedaten in dem Standard-Passwortmanager, der mit seinem Offline-Tresor-Qube geliefert wurde. Er kopiert sie sicher und fügt sie bei Bedarf in andere Qubes ein.

Ein Kollege half Bob anfangs bei der Einrichtung seines Qubes-Systems und zeigte ihm, wie er es benutzen kann. Da Bobs Arbeitsabläufe ziemlich einheitlich und unkompliziert sind, ändert sich die Art und Weise, wie seine Qubes organisiert sind, nicht wesentlich, und das ist für ihn genau richtig. Sein Kollege sagte ihm, er solle sich an ein paar einfache Regeln halten: *Kopieren oder verschieben Sie keine Texte oder Dateien von weniger vertrauenswürdigen zu vertrauenswürdigeren Qubes; aktualisieren Sie Ihr System, wenn Sie dazu aufgefordert werden; und machen Sie regelmäßig Backups.* Bob hat es nicht nötig, neue Software auszuprobieren oder Einstellungen zu ändern. Er kann also alles tun, was er täglich tun muss, ohne mit der Befehlszeile arbeiten zu müssen.

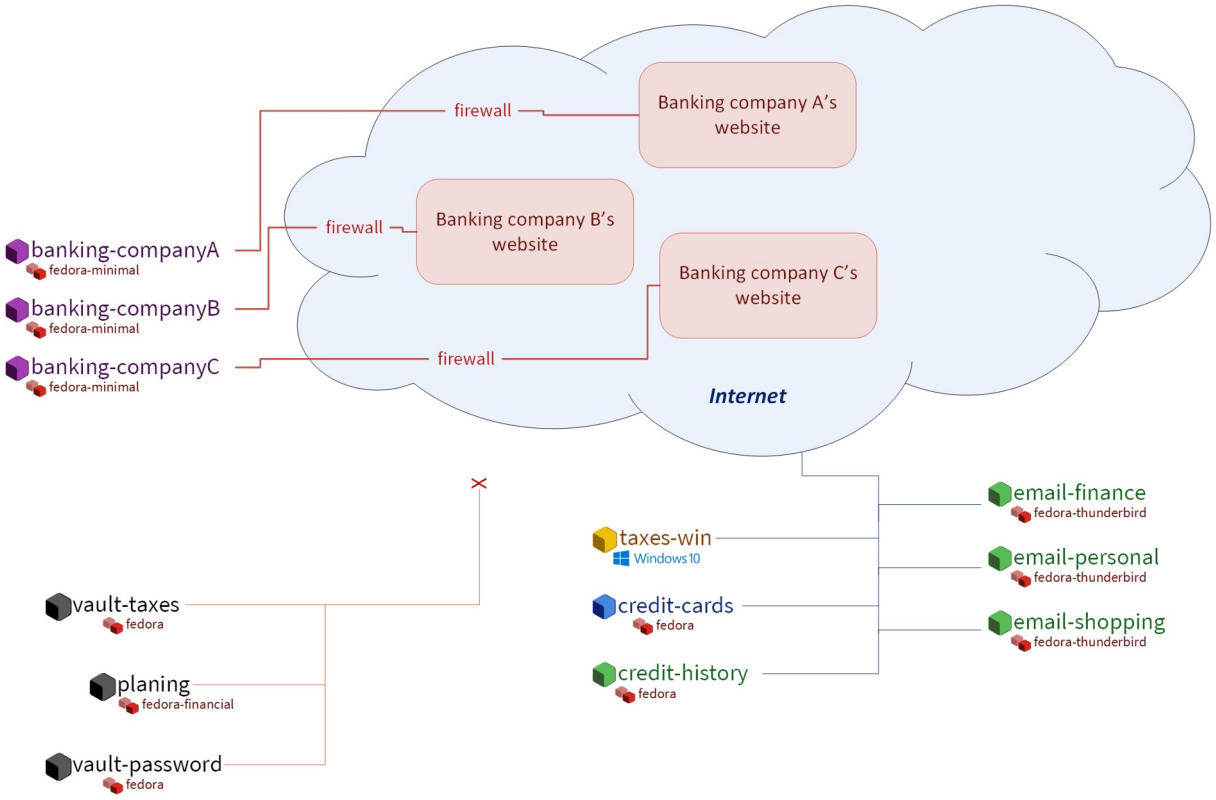
Carol, die Investorin

Carol arbeitet hart und lebt unter ihren Möglichkeiten, um Geld zu sparen und es für ihre Zukunft zu investieren. Sie hofft, eines Tages finanziell unabhängig zu sein und vielleicht sogar vorzeitig in den Ruhestand zu gehen, und sie hat beschlossen, dass sie dies am besten erreichen kann, indem sie langfristig investiert und den Zinseszins wirken lässt. Nachdem sie jedoch einige Nachforschungen über die Gesetze zum Schutz der finanziellen Interessen der Verbraucher in ihrem Land angestellt hatte, erfuhr sie, dass es keine gesetzliche Garantie dafür gibt, dass die Kunden im Falle eines Diebstahls oder Betrugs entschädigt werden. Die verschiedenen Versicherungs- und Schutzorganisationen garantieren eine Entschädigung nur im Falle des Zusammenbruchs eines Finanzinstituts, was etwas ganz anderes ist, als wenn ein einzelner Kunde gehackt wird. Und obwohl viele Finanzinstitute ihre eigenen Richtlinien zur Cyberkriminalität haben, garantieren sie selten, wenn überhaupt, ausdrücklich die Entschädigung für den Fall, dass ein Kunde gehackt wird (und nicht das Institut selbst).

Carol hat nachgeforscht, wie Diebe tatsächlich versuchen könnten, ihr hart verdientes Geld zu stehlen, und war überrascht zu erfahren, dass sie über alle möglichen Tricks verfügen, die sie nie in Betracht gezogen hatte. Sie war zum Beispiel davon ausgegangen, dass ein Diebstahl

zumindest eine Überweisung von ihrem Konto erfordern würde. Das schien eine sichere Annahme zu sein. Doch dann las sie von „Pump-and-Dump“-Angriffen, bei denen Diebe Penny Stocks aufkaufen, sich in die Maklerkonten unschuldiger Menschen einhacken und dann die Gelder der Opfer verwenden, um dieselben Penny Stocks zu kaufen und so den Preis in die Höhe zu treiben, so dass die Diebe ihre Aktien auf dem Markt „absetzen“ können und die Opfer mit wertlosen Aktien zurücklassen. Es wird niemals Geld auf das Konto des Opfers überwiesen oder von ihm abgehoben; es wird lediglich zum Kauf und Verkauf von Wertpapieren verwendet. Alle Sicherheitsvorkehrungen, die verhindern, dass neue Bankkonten hinzugefügt werden, oder die eine zusätzliche Genehmigung für ausgehende Überweisungen erfordern, tragen in solchen Fällen nicht zum Schutz der Gelder der Opfer bei. Und dies ist nur ein Beispiel! Carol erkannte, dass sie nicht davon ausgehen konnte, dass die bestehenden Sicherheitsvorkehrungen gegen bestimmte, bekannte Angriffe ausreichend waren. Sie musste über Sicherheit auf einer grundlegenderen Ebene nachdenken und sie von Grund auf in ihr digitales Leben einbauen.

Nachdem sie all dies gelernt hatte, beschloss Carol, dass es letztlich an ihr lag, sich selbst um ihre Cybersicherheit zu kümmern. Sie konnte sich nicht darauf verlassen, dass jemand anderes das für sie tut. Sicher, die meisten Leute benutzen normale Verbrauchertechnik und kommen damit wahrscheinlich zurecht, aber, so erinnerte sie sich, die meisten Leute haben auch nicht so viel zu verlieren. Dieses Risiko wollte sie für ihre Zukunft nicht eingehen, vor allem, weil sie wusste, dass wahrscheinlich kein staatliches Rettungspaket auf sie wartet und dass die vage beruhigende Marketingsprache der Maklerfirmen über Cybersicherheit rechtlich nicht bindend ist. Also begann Carol, mehr über Computersicherheit zu lesen und stieß schließlich auf Qubes OS, nachdem sie im Internet nach dem „sichersten Betriebssystem“ gesucht hatte. Sie las, wie es aufgebaut ist und warum. Obwohl sie nicht sofort alle technischen Details verstand, leuchtete ihr das Grundprinzip der Sicherheit durch Kompartmentalisierung intuitiv ein, und je mehr sie über die technischen Aspekte erfuhr, desto mehr wurde ihr klar, dass dies genau das war, wonach sie gesucht hatte. Heute sieht ihre Einrichtung wie folgt aus:



- **Einen Qube für jede Wertpapierfirma und Bank.**
  Carol hat einige verschiedene Pensionskonten, Maklerkonten und Bankkonten. Sie behandelt jeden Qube wie ein „sicheres Terminal“, über das sie nur auf die Website des jeweiligen Instituts zugreift. Sie tätigt ihre Transaktionen und speichert alle Auszüge und Bestätigungen, die sie herunterlädt, in diesem Qube. Sie verwendet die Qubes Firewall, um nur den Zugriff auf die Website dieses Instituts in diesem Qube zu ermöglichen, damit sie nicht versehentlich andere Websites besucht. Da sie hauptsächlich mit Websites und PDFs arbeitet, basieren die meisten von Carols Anwendungen auf einem minimalen Template, in dem nur ein Webbrowser (der auch als PDF-Viewer dient) und ein Dateimanager installiert sind.

- **Einen Qube für alle ihre Kreditkartenkonten.**
  Carol wollte zunächst für jedes Kreditkartenkonto einen eigenen Qube erstellen, entschied sich dann aber dagegen. Zum einen ist der Verbraucherschutz bei Kreditkartenbetrug in ihrem Land viel besser als beim Verlust von Vermögenswerten durch Diebstahl oder Betrug bei einem Bank- oder Maklerkonto, so dass das Sicherheitsrisiko nicht so hoch ist. Zweitens kann ein Angreifer mit dem Zugang zu den Online-Konten ihrer Kreditkarten oder ihren alten Kreditkartenabrechnungen nicht viel anrichten, da der Online-Zugang zu diesen Konten in der Regel keine Ausgaben oder Abhebungen zulässt. Selbst das schlimmste Szenario wäre hier also nicht katastrophal, anders als bei ihren Bank- und Maklerkonten. Drittens macht sie sich keine allzu großen Sorgen darüber, dass die Websites ihrer Kreditkartenunternehmen dazu benutzt werden könnten, sich gegenseitig oder ihren Qube zu verknüpfen (solange es sich auf einen einzigen Qube beschränkt, ist sie mit diesem Risiko einverstanden). Und nicht zuletzt: Sie hat viel zu viele Kreditkarten! Carol ist zwar sehr sparsam, aber sie sammelt gerne die Anmeldeboni, die für die Eröffnung neuer Karten angeboten werden, und hat daher schon einige davon angesammelt. (Allerdings achtet sie immer darauf, ihr Guthaben jeden Monat zu tilgen, so dass sie keine Zinsen zahlt. Außerdem ist sie sehr diszipliniert und gibt nur so viel aus, wie sie ohnehin ausgeben würde, und lässt sich nicht dazu verleiten, mehr auszugeben, nur um eine Ausgabeanforderung zu erfüllen oder weil sie es kann). Jedenfalls hat Carol beschlossen, dass der winzige Vorteil, den sie aus einem separaten Qube für jede Kreditkarten-Website ziehen würde, den Aufwand für die Verwaltung so vieler zusätzlicher Qubes nicht wert wäre.

- **Einen Qube für Kreditüberwachung, Kreditberichte und Kreditverlaufsdienste.**
  Carol hat hart gearbeitet, um sich eine gute Kreditwürdigkeit aufzubauen, und sie macht sich Sorgen wegen Identitätsdiebstahls, also hat sie einen Qube für die Verwaltung ihrer kostenlosen Kreditüberwachungsdienste und das Herunterladen ihrer kostenlosen jährlichen Kreditberichte.

- **Zwei Qubes für Steuern.**
  Carol hat einen Windows Qube, auf dem sie ihre reine Windows-Steuersoftware ausführt. Außerdem hat sie einen Offline-Tresor, in dem sie alle steuerrelevanten Formulare und Dokumente nach Jahren geordnet speichert.

- **Einen Qube für die Finanzplanung und -verfolgung.**
  Carol liebt Tabellenkalkulationen, und so verwaltet sie in diesem Offline-Qube eine Haupttabelle, in der sie alle ihre Investitionen und ihre Sparrate verfolgt. Außerdem bewahrt sie hier ihre Budgettabelle, ihre Versicherungstabelle und ihre schriftliche Erklärung zur Investitionspolitik auf. Dieser Qube basiert auf einem Template mit zusätzlicher Produktivitätssoftware wie LibreOffice und Gnumeric (damit Carol ihre eigenen Monte-Carlo-Simulationen durchführen kann).

- **Verschiedene E-Mail-Qubes.**
  Carol hat gerne einen E-Mail-Qube für ihre wichtigsten Finanzkonten, einen weiteren für ihre Kreditkartenkonten, Online-Einkaufskonten und Versicherungsgesellschaften und einen weiteren für persönliche E-Mails. Sie basieren alle auf dem gleichen Template mit installiertem Thunderbird.

- **Einen Passwortmanager-Tresor.**
  Ein vom Netzwerk isolierter Tresor, in dem Carol alle Benutzernamen und Passwörter ihrer Konten in KeePassXC speichert. Sie benutzt die globale Zwischenablage von Qubes, um sie zu kopieren und in ihre anderen Qubes einzufügen, wenn sie sich bei ihren Konten anmelden muss.

Bonus: Carol erforscht neue Finanztechnologien

Die überwiegende Mehrheit von Carols Vermögen liegt in breit angelegten, kostengünstigen, passiv verwalteten Indexfonds. In letzter Zeit interessiert sie sich jedoch für Kryptowährungen. Sie ist immer noch entschlossen, ihre bewährten Investitionen beizubehalten, und sie war schon immer skeptisch gegenüber neuen Anlageklassen, insbesondere gegenüber solchen, die keinen Cashflow generieren oder die oft mit Betrug oder wilder Spekulation in Verbindung gebracht werden. Sie findet jedoch die Möglichkeit, einen Teil ihres Vermögens selbst zu verwahren, aus der Perspektive des langfristigen Risikomanagements interessant, insbesondere als Absicherung gegen bestimmte Arten von politischen Risiken.

Einige von Carols Freunden warnten sie, dass Kryptowährungen extrem volatil sind und dass Hackerangriffe und Diebstahl an der Tagesordnung sind. Carol stimmte ihnen zu und versicherte ihnen, dass sie sich über die Risiken informiert hat und sicherstellen wird, dass sie nie mehr investiert, als sie sich leisten kann, zu verlieren.

Carol hat ihr Qubes-Setup wie folgt ergänzt:

- **Einen eigenständigen Qube zum Ausführen von Bitcoin Core und einen Offline-Wallet-Tresor.**
  Carol findet das Design und die Sicherheitseigenschaften von Bitcoin sehr interessant, daher experimentiert sie mit dem Betrieb eines vollständigen Knotens. Sie hat auch einen netzwerkisolierten Tresor erstellt, um zu versuchen, eine Kopie von Bitcoin Core komplett offline als „Cold Storage“ Wallet zu betreiben. Sie versucht immer noch herauszufinden, wie das im Vergleich zu einer tatsächlichen Hardware-Wallet, einer Papier-Wallet oder einer physisch getrennten befindlichen Maschine ist, aber sie hat herausgefunden, dass sie alle unterschiedliche Sicherheitseigenschaften haben. Sie hat auch kürzlich von der Verwendung von Electrum als „geteilter“ Geldbörse in Qubes gehört und ist daran interessiert, dies weiter zu erforschen.

- **Whonix Qubes.**
  Carol hat irgendwo gelesen, dass Bitcoin-Knoten aus Gründen des Datenschutzes und der Sicherheit über Tor betrieben werden sollten. Sie fand es sehr praktisch, dass Whonix bereits in Qubes integriert ist, also hat sie einfach ihren Bitcoin-Vollknoten-Qube so eingestellt, dass sie `sys-whonix` als ihren Netzwerk Qube benutzt.

- **Verschiedene Qubes für DeFi und Web3.**
  Carol hat auch angefangen, sich mit DeFi (dezentralisierte Finanzen) und Web3 auf Ethereum und anderen Smart Contract Blockchains zu beschäftigen, also empfahl ihr ein Freund, sich eine Ledger Hardware Wallet zu besorgen. Sie lud die Ledger Live Software in einen App-Qube herunter und richtete ihr System so ein, dass es den Ledger erkennt. Sie kann nun ihren USB-Qube starten, ihren Ledger an einen USB-Port

anschließen, das Qubes-Geräte-Widget verwenden, um ihn mit ihrem Ledger Live-Qube zu verbinden, und von dort aus mit der Software interagieren. Sie hat einen separaten Qube mit der Metamask-Erweiterung in einem Webbrowser installiert. Sie kann auch das Qubes-Geräte-Widget verwenden, um ihren Ledger mit dieser Qube zu verbinden, so dass sie Metamask in Verbindung mit ihrem Ledger verwenden kann, um mit intelligenten Verträgen und dezentralen Börsen zu interagieren.

- **Verschiedene Qubes für Untersuchungen und zentralisierte Börsen.**
  Carol verwendet diese, wenn sie Block-Explorer-Websites, Coin-Listing- und Market-Cap-Websites, Aggregations-Tools oder einfach nur den neuesten Buzz auf Crypto Twitter überprüfen möchte.

Carol stellt sicher, dass sie alle ihre Dateien, die wichtige Kontoauszüge, Bestätigungen, Tabellen, Kryptowährungs-Wallets und ihren Passwortmanager-Tresor enthalten, sichert. Wenn sie über zusätzlichen Speicherplatz verfügt, sichert sie auch ihre Templates und sogar ihren Bitcoin-Vollknoten-Qube, aber sie überspringt sie, wenn sie keine Zeit oder keinen Platz hat, da sie weiß, dass sie sie später immer wieder neu erstellen und alles, was sie braucht, aus dem Internet herunterladen kann.

Fazit

Die Personen, die wir heute kennen gelernt haben, mögen fiktiv sein, aber sie repräsentieren die Bedürfnisse von realen Benutzern wie Ihnen. Vielleicht stellen Sie fest, dass sich Ihre eigenen Bedürfnisse mit mehr als einem dieser Charaktere überschneiden. In diesem Fall kann es sinnvoll sein, bestimmte Teilbereiche Ihres gesamten Qubes-Systems anhand verschiedener Beispiele zu modellieren. Wahrscheinlich ist Ihnen auch aufgefallen, dass es Gemeinsamkeiten zwischen den Beispielen gibt. Die meisten Leute müssen zum Beispiel E-Mail verwenden, also brauchen die meisten Leute mindestens ein E-Mail-Qubes und eine geeignete Vorlage, auf der es basiert. Aber nicht jeder wird Split GPG brauchen, und nicht jeder wird denselben E-Mail-Client verwenden wollen. Andererseits braucht fast jeder einen Passwort-Manager, und es ist fast immer sinnvoll, ihn in einem offline, vom Netzwerk isolierten Tresor aufzubewahren.

Mit zunehmender Erfahrung mit Qubes werden Sie vielleicht mit einigen der Entscheidungen, die unsere fiktiven Freunde getroffen haben, nicht einverstanden sein. Das ist in Ordnung! Es gibt viele verschiedene Möglichkeiten, ein Qubes-System zu organisieren, und das wichtigste Kriterium ist, dass es den Bedürfnissen seines Besitzers dient. Da die Bedürfnisse jedes Einzelnen anders sind, ist es völlig normal, dass man die Dinge ein wenig anders angeht. Dennoch gibt es einige allgemeine Prinzipien, die fast alle Benutzer als hilfreich empfinden, besonders wenn sie zum ersten Mal damit anfangen.

Wenn Sie Ihr eigenes Qubes-System entwerfen, sollten Sie einige der folgenden Lektionen aus unseren Fallstudien im Hinterkopf behalten:

- **Wahrscheinlich werden Sie Ihre Meinung im Laufe der Entwicklung ändern.**
  Sie werden feststellen, dass ein Qube eigentlich in zwei aufgeteilt werden sollte, oder Sie werden feststellen, dass es nicht wirklich sinnvoll ist, zwei Qubes getrennt zu halten und sie stattdessen zu einem zu verschmelzen. Das ist in Ordnung. Qubes OS unterstützt Ihre Fähigkeit, sich anzupassen und Änderungen vorzunehmen, während Sie arbeiten. Versuchen Sie, eine flexible Denkweise beizubehalten. Die Dinge werden sich mit der Zeit einpendeln und Sie werden Ihren Rhythmus finden. Änderungen an der Art und Weise, wie Sie Ihre Qubes organisieren, werden mit der Zeit weniger drastisch und seltener werden.

- **Machen Sie regelmäßig Backups.**
  Der Verlust von Daten ist nie lustig, sei es durch versehentliches Löschen, einen Systemabsturz, fehlerhafte Software oder einen Hardwaredefekt. Wenn Sie sich angewöhnen, jetzt regelmäßig Sicherungskopien zu erstellen, ersparen Sie sich in Zukunft eine Menge Ärger. Viele Menschen nehmen Datensicherungen erst dann ernst, wenn sie einen katastrophalen Datenverlust erleiden. Das liegt in der menschlichen Natur. Wenn Sie das schon einmal erlebt haben, dann kennen Sie den Schmerz. Nehmen Sie sich jetzt vor, dies nie wieder geschehen zu lassen. Wenn Sie es noch nie erlebt haben, sollten Sie sich glücklich schätzen und versuchen, aus den Erfahrungen anderer zu lernen. Gute Backups erlauben es Ihnen auch, bei der Umstrukturierung etwas freier zu sein. Sie können Dateien löschen, die Sie nicht mehr benötigen, ohne sich Sorgen machen zu müssen, dass Sie sie eines Tages wieder brauchen könnten, da Sie wissen, dass Sie sie jederzeit von einer Sicherung wiederherstellen können.

- **Überlegen Sie, welche Programme Sie ausführen und wo Sie Daten speichern wollen.**
  In manchen Fällen ist es sinnvoll, Programme auszuführen und Daten in demselben Qube zu speichern, z. B. wenn die Daten von diesem Programm erzeugt werden. In anderen Fällen ist es sinnvoll, Qubes zu haben, die ausschließlich zum Speichern von Daten dienen (z.B. Offline-Datenspeicher) und andere Qubes, die ausschließlich zum Ausführen von Programmen dienen (z.B. Qubes, die nur für den Webbrowser bestimmt sind). Denken Sie daran, dass bei der Erstellung von Backups nur Daten gesichert werden müssen, die nicht ersetzt werden können. So können Sie minimale Backups erstellen, die im Vergleich zur Gesamtgröße Ihrer Installation recht klein sind. Templates, Service-Qubes und Qubes, die ausschließlich zur Ausführung von Programmen dienen und keine Daten enthalten, müssen nicht unbedingt gesichert werden, solange Sie sicher sind, dass Sie sie bei Bedarf wiederherstellen können. Aus diesem Grund ist es sinnvoll, sich Notizen darüber zu machen, welche Pakete Sie in welchen Templates installiert und welche Anpassungen und Konfigurationen Sie vorgenommen haben. Dann können Sie auf Ihre Notizen zurückgreifen, wenn Sie das nächste Mal diese Anpassungen wieder vornehmen müssen. Natürlich ist es auch keine schlechte Idee, von allem eine Sicherungskopie zu erstellen. Das erfordert zwar etwas mehr Zeit und Speicherplatz, aber für manche Leute ist es genauso wichtig wie die Sicherung ihrer unersetzlichen Daten. Wenn Ihr System unternehmenskritisch ist und Sie sich nicht mehr als eine gewisse Ausfallzeit leisten können, sollten Sie auf jeden Fall alles sichern!

- **Überprüfen Sie Ihr eigenes Verhalten.**
  Wenn Sie zum Beispiel einen Weg finden wollen, dass sich zwei Qubes den gleichen Speicherplatz teilen, dann ist das wahrscheinlich ein Zeichen dafür, dass diese beiden Qubes gar nicht erst getrennt werden sollten. Die gemeinsame Nutzung von Speicherplatz bricht die Sicherheitsmauer zwischen den beiden Qubes weitgehend auf, wodurch die Trennung irgendwie sinnlos wird. Aber Sie hatten wahrscheinlich einen guten Grund dafür, dass Sie aus den beiden Qubes zwei getrennte Qubes machen wollten und nicht nur einen. Was genau war dieser Grund? Wenn es mit Sicherheit zu tun hat, warum sind Sie dann damit einverstanden, dass sie frei Daten austauschen, die es dem einen ermöglichen, den anderen zu infizieren? Wenn Sie sicher sind, dass die gemeinsame Nutzung der Daten nicht dazu führen würde, dass der eine den anderen infiziert, was ist dann der Sicherheitsgrund, sie getrennt zu halten? Indem Sie Ihren eigenen Denkprozess auf diese Weise kritisch überprüfen, können Sie Ungereimtheiten und Widersprüche aufdecken, die es Ihnen ermöglichen, Ihr System zu verfeinern, was zu

einer logischeren Organisation führt, die Ihren Anforderungen mit der Zeit immer besser gerecht wird.

- **Gehen Sie nicht davon aus, dass ein Gegner nicht in der Lage wäre, Ihr System anzugreifen, nur weil *Sie* keine Möglichkeit dazu finden.**
  Wenn Sie darüber nachdenken, ob es eine gute Idee ist, verschiedene Aktivitäten oder Daten in einem einzigen Qube zu kombinieren, denken Sie vielleicht: „Ich kann nicht erkennen, wie diese ein Risiko für einander darstellen." Das Problem ist, dass wir oft Angriffsvektoren übersehen, die raffinierte Angreifer erkennen und gegen uns verwenden können. Schließlich halten die meisten Menschen die Verwendung eines herkömmlichen monolithischen Betriebssystems nicht für riskant, während in Wirklichkeit ihr gesamtes digitales Leben auf einen Schlag zum Erliegen kommen kann. Deshalb lautet eine gute Faustregel: Im Zweifelsfall sollte man eine Kompartmentalisierung vornehmen.

- **Aber denken Sie daran, dass die Kompartmentalisierung – wie alles andere auch – bis zum Äußersten getrieben werden kann.**
  Das richtige Maß hängt von Ihrem Temperament, Ihrer Zeit, Ihrer Geduld, Ihrer Erfahrung, Ihrer Risikobereitschaft und Ihrem Fachwissen ab. Kurz gesagt, es kann so etwas wie ein Zuviel an Abschottung geben! Sie müssen auch in der Lage sein, Ihren Computer tatsächlich effizient zu *nutzen*, um die Dinge zu tun, die Sie tun müssen. Wenn Sie z. B. sofort versuchen, alles in Wegwerf-Qubes (Disposables) zu erledigen, und dabei ständig Arbeit verlieren (z. B. weil Sie vergessen, sie zu übertragen, bevor sich der Wegwerf-Qube selbst zerstört), dann ist das ein großes Problem! Ihre zusätzlichen, selbst auferlegten Sicherheitsmaßnahmen beeinträchtigen genau das, was sie eigentlich schützen sollen. In solchen Momenten sollten Sie tief durchatmen und sich daran erinnern, dass Sie den größten Teil der Sicherheitsvorteile bereits erreicht haben, indem Sie Qubes OS von Anfang an eingesetzt und eine grundlegende Abschottung vorgenommen haben (z.B. kein zufälliges Surfen im Internet in Templates). Jeder weitere Schritt der Härtung und Kompartmentalisierung darüber hinaus stellt einen inkrementellen Gewinn mit abnehmendem Grenznutzen dar. Versuchen Sie, das Perfekte nicht zum Feind des Guten werden zu lassen!

HÄUFIG GESTELLTE FRAGEN (FAQ)

Allgemein & Sicherheit

Was ist Qubes OS?

Qubes OS ist ein sicherheitsorientiertes Betriebssystem, mit dem Sie Ihr digitales Leben in Abteilungen, den sogenannten "Qubes", organisieren können. Wenn eine Qube kompromittiert wird, bleiben die anderen sicher, so dass ein einziger Cyberangriff nicht mehr Ihr gesamtes digitales Leben auf einen Schlag lahm legen kann. Sie können sich die Verwendung von Qubes OS so vorstellen, als hätten Sie viele verschiedene Computer auf Ihrem Schreibtisch für unterschiedliche Aktivitäten, aber mit dem Komfort eines einzigen physischen Rechners, einer einzigen einheitlichen Desktop-Umgebung und einer Reihe von Werkzeugen für die sichere Verwendung von Qubes als Teile eines einheitlichen Systems.

Ist Qubes OS freie und quelloffene Software?

Es gibt zwei verschiedene Bedeutungen des Wortes „frei“, wenn es um freie Software geht. Der Unterschied wird gemeinhin durch die Ausdrücke „Freibier“ und „frei verwendbar wie Sprache“ ausgedrückt.

Der erste Sinn ist ganz einfach. Qubes OS ist „frei wie Bier“, d. h., es wird kostenlos zur Verfügung gestellt, obwohl Spenden sehr willkommen sind.

Der zweite Sinn ist etwas komplizierter. Qubes OS ist *größtenteils* „frei verwendbar wie Sprache“, aber nicht vollständig. Die gesamte Software, die vom Qubes OS Projekt *selbst* erstellt wird, ist freie (oder „libre“) und quelloffene Software (FOSS oder FLOSS). Das bedeutet, dass jeder die Software in Übereinstimmung mit der Lizenz verwenden, kopieren, studieren und verändern darf. Es bedeutet auch, dass der Quellcode öffentlich zugänglich ist, so dass jeder ihn prüfen und zu ihm beitragen kann.

Da Qubes OS jedoch ein sicherheitsorientiertes Betriebssystem ist, enthält es einige unfreie Firmware, die nicht vom Qubes OS Projekt erstellt wurde (z.B. CPU-Mikrocode), was notwendig ist, um vor bekannten Sicherheitslücken zu schützen. Darüber hinaus bedeutet die Architektur von Qubes OS als Meta-Betriebssystem, dass es andere Software (einschließlich ganzer Betriebssysteme) von verschiedenen Upstream-Projekten enthält, von denen einige auch eigene unfreie Software enthalten können. Um den Installationsprozess für eine Vielzahl von Nutzern auf vielen verschiedenen Geräten zu erleichtern, enthalten die Standard-Qubes-Templates auch einige unfreie Firmware und Treiber.

Siehe auch: Wird Qubes versuchen, nach den GNU Free System Distribution Guidelines (GNU FSDG) zertifiziert zu werden?

Warum ist die Sicherheit des Betriebssystems wichtig?

Die meisten Menschen verwenden ein Betriebssystem wie Windows oder macOS auf ihren Desktop- und Laptop-Computern. Diese Betriebssysteme sind beliebt, weil sie in der Regel einfach zu bedienen sind und in der Regel auf den gekauften Computern vorinstalliert sind. Sie bringen jedoch Probleme mit sich, wenn es um die Sicherheit geht. So kann es vorkommen, dass Sie einen harmlos aussehenden E-Mail-Anhang oder eine Website öffnen, ohne zu bemerken, dass Sie in Wirklichkeit Malware (bösartige Software) auf Ihrem Computer ausführen lassen. Je nachdem, um welche Art von Malware es sich handelt, kann sie alles Mögli-

che tun, von der Anzeige unerwünschter Werbung über die Protokollierung Ihrer Tastenanschläge bis hin zur Übernahme Ihres gesamten Computers. Dies könnte alle Informationen gefährden, die auf diesem Computer gespeichert sind oder auf die er zugreift, z. B. Gesundheitsdaten, vertrauliche Mitteilungen oder in einem privaten Tagebuch niedergeschriebene Gedanken. Malware kann auch die Aktivitäten stören, die Sie mit Ihrem Computer durchführen. Wenn Sie Ihren Computer z. B. für Finanztransaktionen verwenden, kann die Malware ihrem Ersteller ermöglichen, in Ihrem Namen betrügerische Transaktionen durchzuführen.

Sind Antivirenprogramme und Firewalls nicht genug?

Leider reichen herkömmliche Sicherheitsmaßnahmen wie Antivirenprogramme und (Software- und/oder Hardware-)Firewalls nicht mehr aus, um raffinierte Angreifer abzuwehren. Heutzutage ist es zum Beispiel üblich, dass Malware-Entwickler überprüfen, ob ihre Malware von signaturbasierten Antivirenprogrammen erkannt wird. Wenn dies der Fall ist, verschlüsseln sie ihren Code, bis er von den Antivirenprogrammen nicht mehr erkannt wird, und senden ihn dann aus. Die besten dieser Programme werden anschließend aktualisiert, sobald die Antivirenprogrammierer die neue Bedrohung entdecken, was jedoch in der Regel erst einige Tage nach dem Auftauchen der neuen Angriffe geschieht. Zu diesem Zeitpunkt ist es für diejenigen, die bereits gefährdet sind, zu spät. Fortschrittlichere Antivirensoftware mag in dieser Hinsicht besser abschneiden, ist aber immer noch auf einen erkenntnisbasierten Ansatz beschränkt. Es werden ständig neue Zero-Day-Schwachstellen in der von uns allen genutzten Software, z. B. in unseren Webbrowsern, entdeckt, und kein Antivirenprogramm und keine Firewall kann verhindern, dass alle diese Schwachstellen ausgenutzt werden.

Wie bietet Qubes OS Sicherheit?

Qubes verfolgt einen Ansatz, der als **Sicherheit durch Kompartmentalisierung** bezeichnet wird und der es Ihnen ermöglicht, die verschiedenen Bereiche Ihres digitalen Lebens in sicher isolierte Abteilungen, die so genannten *Qubes,* einzuteilen.

Dieser Ansatz ermöglicht es Ihnen, die verschiedenen Dinge, die Sie auf Ihrem Computer tun, in isolierten Qubes sicher voneinander getrennt zu halten, so dass ein Qube, der kompromittiert wird, die anderen nicht beeinträchtigt. Sie könnten zum Beispiel einen Qube für den Besuch nicht vertrauenswürdiger Websites und einen anderen Qube für Online-Banking haben. Auf diese Weise sind Ihre Online-Banking-Aktivitäten nicht gefährdet, wenn Ihr nicht vertrauenswürdiger Browser-Qube durch eine mit Malware verseuchte Website kompromittiert wird. Wenn Sie sich Sorgen über bösartige E-Mail-Anhänge machen, kann Qubes dafür sorgen, dass jeder Anhang in einem eigenen Einweg-Qube geöffnet wird. Auf diese Weise können Sie mit Qubes alles auf demselben physischen Computer erledigen, ohne sich Sorgen machen zu müssen, dass ein einziger erfolgreicher Cyberangriff Ihr gesamtes digitales Leben auf einen Schlag zum Erliegen bringt.

Außerdem sind alle diese isolierten Fenster in ein einziges, benutzbares System integriert. Programme werden in ihren eigenen, separaten Bereichen isoliert, aber alle Fenster werden in einer einzigen, einheitlichen Desktop-Umgebung mit nicht fälschbaren farbigen Fensterrändern angezeigt, so dass Sie Fenster verschiedener Sicherheitsstufen leicht erkennen können. Übliche Angriffsvektoren wie Netzwerkkarten und USB-Controller werden in eigenen Hardware-Qubes isoliert, während ihre Funktionalität durch sichere Netzwerke, Firewalls und USB-Geräteverwaltung erhalten bleibt. Integrierte Kopier- und Einfügevorgänge für Dateien und die Zwischenablage erleichtern die Arbeit über verschiedene Qubes hinweg, ohne die Sicherheit zu beeinträchtigen. Das innovative Template-System trennt die Software-Installation

von der Software-Nutzung und ermöglicht es den Qubes, ein gemeinsames Root-Dateisystem zu nutzen, ohne die Sicherheit zu beeinträchtigen (und spart zudem Speicherplatz). Qubes ermöglicht es Ihnen sogar, PDFs und Bilder mit wenigen Klicks zu bereinigen. Wer sich Sorgen um physische Hardware-Angriffe macht, wird von Anti Evil Maid profitieren.

Wie gewährleistet Qubes OS den Datenschutz?

Es kann keinen Datenschutz ohne Sicherheit geben, da Sicherheitslücken die Umgehung von Datenschutzmaßnahmen ermöglichen. Daher eignet sich Qubes besonders gut für die Implementierung wirksamer Datenschutzinstrumente.

Benutzer, die sich um ihre Privatsphäre sorgen, werden die Integration von Whonix in Qubes zu schätzen wissen, die es einfach macht, Tor sicher zu benutzen. Für weitere Informationen über die korrekte und sichere Nutzung dieses mächtigen Werkzeugs, siehe Qubes-Whonix-Anleitungen.

Die Datenschutzrichtlinien für unsere Website, Repositories, Qubes OS selbst und mehr finden Sie unter Datenschutzbestimmungen.

Was ist mit der Privatsphäre in Nicht-Whonix-Qubes?

Der wichtigste Weg, auf dem Qubes OS Privatsphäre bietet, ist durch seine Integration mit Whonix gegeben. Qubes OS erhebt nicht den Anspruch, besondere Datenschutz- (im Gegensatz zu Sicherheits-) Eigenschaften in Nicht-Whonix-Qubes zu bieten. Dies gilt auch für Disposables.

Der Schutz der Privatsphäre ist weitaus schwieriger, als gemeinhin angenommen wird. Neben dem Webbrowser gibt es auch VM-Fingerabdrücke und fortgeschrittene Angriffe zur Deanonymisierung, die die meisten Benutzer noch nie in Betracht gezogen haben (und dies sind nur einige Beispiele). Das Whonix-Projekt ist auf den Schutz vor diesen Risiken spezialisiert.

Um die gleichen Ergebnisse in Nicht-Whonix-Qubes (einschließlich Disposables) zu erzielen, müsste man Whonix neu erfinden. Eine solche Verdoppelung des Aufwands macht keinen Sinn, wenn Whonix bereits existiert und bereits in Qubes OS integriert ist.

Wenn Sie also Privatsphäre brauchen, sollten Sie Whonix-Qubes verwenden. Denken Sie jedoch daran, dass es schwierig ist, Privatsphäre zu erreichen und zu wahren. Whonix ist ein leistungsfähiges Werkzeug, aber kein Werkzeug ist perfekt. Lesen Sie die Dokumentation gründlich und gehen Sie bei der Verwendung sorgfältig vor.

Wie verhält sich Qubes OS im Vergleich zur Verwendung eines „Live-CD“-Betriebssystems?

Wenn Sie Ihren Computer von einer Live-CD (oder -DVD) booten, um sensible Aktivitäten auszuführen, kann dies sicherlich sicherer sein als die Verwendung Ihres Hauptbetriebssystems, aber diese Methode birgt immer noch viele der Risiken herkömmlicher Betriebssysteme. Beispielsweise sind beliebte Live-Betriebssysteme (wie Tails und andere Linux-Distributionen) nach wie vor **monolithisch** in dem Sinne, dass die gesamte Software immer noch auf demselben Betriebssystem läuft. Das bedeutet wiederum, dass, wenn Ihre Sitzung kompromittiert wird, auch alle Daten und Aktivitäten, die innerhalb dieser Sitzung ausgeführt werden, potenziell gefährdet sind.

Wie lässt sich Qubes OS mit der Ausführung von VMs in einem herkömmlichen Betriebssystem vergleichen?

Nicht jede Software für virtuelle Maschinen ist gleich, wenn es um die Sicherheit geht. Vielleicht haben Sie schon einmal von VMs in Verbindung mit Software wie VirtualBox oder VMware Workstation gehört. Diese sind als „Typ 2“ oder „gehostete“ Hypervisoren bekannt. (Der **Hypervisor** ist die Software, Firmware oder Hardware, die virtuelle Maschinen erstellt und ausführt.) Diese Programme sind beliebt, weil sie in erster Linie benutzerfreundlich sind und unter gängigen Betriebssystemen wie Windows laufen (das als Host-Betriebssystem bezeichnet wird, da es die VMs „hostet“). Die Tatsache, dass Hypervisoren vom Typ 2 unter dem Host-Betriebssystem ausgeführt werden, bedeutet jedoch, dass sie wirklich nur so sicher sind wie das Host-Betriebssystem selbst. Wenn das Host-Betriebssystem jemals kompromittiert wird, sind alle VMs, die es hostet, ebenfalls gefährdet.

Im Gegensatz dazu verwendet Qubes einen „Typ 1“- oder „Bare-Metal“-Hypervisor namens Xen. Hypervisoren vom Typ 1 laufen nicht innerhalb eines Betriebssystems, sondern direkt auf dem „Bare Metal“ der Hardware. Dies bedeutet, dass ein Angreifer in der Lage sein muss, den Hypervisor selbst zu unterwandern, um das gesamte System zu kompromittieren, was wesentlich schwieriger ist.

Qubes sorgt dafür, dass mehrere VMs, die unter einem Typ-1-Hypervisor laufen, sicher als integriertes Betriebssystem genutzt werden können. So werden beispielsweise alle Ihre Anwendungsfenster auf demselben Desktop mit speziellen farbigen Rändern angezeigt, die die Vertrauensstufen der jeweiligen VMs angeben. Es ermöglicht auch Dinge wie sichere Kopier-/Einfügevorgänge zwischen VMs, sicheres Kopieren und Übertragen von Dateien zwischen VMs und sichere Netzwerke zwischen VMs und dem Internet.

Wie schneidet Qubes OS im Vergleich zur Verwendung eines separaten physischen Computers ab?

Die Verwendung eines separaten physischen Computers für sensible Aktivitäten kann sicherlich sicherer sein als die Verwendung eines Computers mit einem herkömmlichen Betriebssystem für alles, aber es gibt immer noch Risiken zu berücksichtigen. Im Folgenden werden kurz einige der wichtigsten Vor- und Nachteile dieses Ansatzes im Vergleich zu Qubes erläutert:

Vorteile

- Die physische Trennung beruht nicht auf einem Hypervisor. (Es ist sehr unwahrscheinlich, dass ein Angreifer aus dem Hypervisor von Qubes ausbricht, aber wenn es ihm gelänge, könnte er möglicherweise die Kontrolle über das gesamte System erlangen.)
- Die physische Trennung kann eine natürliche Ergänzung zur physischen Sicherheit sein. (Zum Beispiel könnten Sie es als natürlich empfinden, Ihren sicheren Laptop in einen Safe zu sperren, wenn Sie Ihren unsicheren Laptop mitnehmen).

Nachteile

- Die physische Trennung kann mühsam und teuer sein, da Sie für jede benötigte Sicherheitsstufe einen eigenen physischen Rechner beschaffen und einrichten müssen.
- Es gibt im Allgemeinen keine sichere Möglichkeit, Daten zwischen physisch getrennten Computern mit konventionellen Betriebssystemen zu übertragen. (Qubes verfügt über ein sicheres Inter-VM-Dateiübertragungssystem, um dies zu bewerkstelligen).

- Physikalisch getrennte Computer, auf denen herkömmliche Betriebssysteme laufen, sind aufgrund ihres monolithischen Charakters immer noch unabhängig voneinander für die meisten herkömmlichen Angriffe anfällig.
- Schadsoftware, die Luftlücken überbrücken kann, gibt es schon seit einigen Jahren und wird immer häufiger eingesetzt.

(Weitere Informationen zu diesem Thema finden Sie in dem Artikel Softwarekompartmentalisierung vs. physische Trennung).

Was ist das Hauptkonzept hinter Qubes?

Aufbau von Sicherheit nach dem Prinzip „Sicherheit durch Abschottung (oder Isolierung)".

Wie sieht es mit anderen Ansätzen für die Sicherheit aus?

Die beiden anderen populären Ansätze sind „Sicherheit durch Korrektheit" und „Sicherheit durch Obskurität". Wir glauben nicht, dass einer dieser beiden Ansätze heute in der Lage ist, angemessene Sicherheit zu bieten, und wir glauben auch nicht, dass sie dies in absehbarer Zukunft tun werden.

Wie unterscheidet sich Qubes von anderen Sicherheitslösungen?

In diesem Artikel finden Sie eine ausführliche Diskussion.

Ist Qubes nur eine weitere Linux-Distribution?

Wenn Sie es wirklich eine Distribution nennen wollen, dann ist es eher eine „Xen-Distribution" als eine Linux-Distribution. Aber Qubes ist viel mehr als nur ein Xen-Paket. Es hat seine eigene VM-Verwaltungsinfrastruktur mit Unterstützung für VM-Templates, zentralisierte VM-Aktualisierung usw. Es hat auch eine sehr einzigartige GUI-Virtualisierungsinfrastruktur.

Was ist mit sicheren Sprachen und formal verifizierten Mikrokerneln?

Kurz gesagt: Diese Lösungen sind heute nicht realistisch. Wir erörtern dies ausführlicher in unserem Dokument zur Spezifikation der Architektur.

Warum verwendet Qubes Virtualisierung?

Wir sind der Meinung, dass dies derzeit der einzig praktikable Ansatz ist, um eine starke Isolierung zu implementieren und gleichzeitig die Kompatibilität mit bestehenden Anwendungen und Treibern zu gewährleisten.

Verwendet Qubes eine vollständige Festplattenverschlüsselung (FDE)?

Ja, natürlich! Die vollständige Festplattenverschlüsselung ist standardmäßig aktiviert. Konkret verwenden wir LUKS/dm-crypt. Sie können Ihre Verschlüsselungsparameter sogar manuell konfigurieren, wenn Sie möchten!

Was bedeuten all diese Begriffe?

Alle Qubes-spezifischen Begriffe sind im Glossar definiert

Läuft bei Qubes jede Anwendung in einer eigenen VM?

Nein! Das würde nicht viel Sinn machen. Qubes verwendet leichtgewichtige VMs, um Sicherheits-Qubes zu erstellen (z.B. „Arbeit“, „Privat“ und „Banking“). Ein typischer Benutzer benötigt wahrscheinlich etwa fünf Qubes. Sehr paranoide Benutzer oder solche, die ein hochrangiges Ziel sind, könnten ein Dutzend oder mehr Qubes verwenden.

Warum verwendet Qubes Xen anstelle von KVM oder einem anderen Hypervisor?

Kurz gesagt: Wir sind der Meinung, dass die Xen-Architektur die Entwicklung sicherer Systeme ermöglicht (d. h. mit einer viel kleineren TCB (Trusted Computing Base), was wiederum eine geringere Angriffsfläche bedeutet). Wir erörtern dies in unserem Dokument zur Spezifikation der Architektur sehr viel ausführlicher.

Wie wird Qubes von Xen Security Advisories (XSAs) beeinflusst?

Siehe den XSA-Tracker.

Was ist mit diesem anderen/neuen (Mikro-)Kernel/Hypervisor?

Wenn Sie eine Diskussion über einen anderen (Mikro-)Kernel oder Hypervisor im Zusammenhang mit Qubes beginnen, empfehlen wir dringend, zuerst die folgenden Fragen zu beantworten:

1. Welche Arten von Containern werden zur Isolierung verwendet? Prozesse? PV-VMs? Vollständig virtualisierte VMs (HVMs)? Und welche zugrunde liegende H/W-Technologie wird verwendet (Ring0/3, VT-x)?
2. Erfordert es speziell geschriebene/erstellte Anwendungen (z. B. gepatchter Firefox)?
3. Benötigt es benutzerdefinierte Treiber, oder kann es Linux/Windows-Treiber verwenden?
4. Unterstützt es VT-d und erlaubt es die Erstellung von nicht vertrauenswürdigen Treiberdomänen?
5. Unterstützt es S3-Schlaf?
6. Funktioniert es auf mehreren CPUs/Chipsätzen?

7. Wie hoch sind die Leistungskosten, mehr oder weniger? (z. B. „XYZ verhindert die gleichzeitige Ausführung von zwei Domänen/Prozessen auf gemeinsam genutzten Kernen eines einzelnen Prozessors“ usw.)
8. Andere besondere Merkmale? Z.B. Beseitigung kooperativer verdeckter Kanäle zwischen VMs?

Hier sind die Antworten für Xen 4.1 (das wir ab dem 2014-04-28 verwenden):

1. Virtuelle Maschinen für PV und HVM (Ring0/3 für PV-Domänen, VT-x/AMD-v für HVMs).
2. Führt unmodifizierte Usermode-Anwendungen (Binärdateien) aus.
3. Führt unveränderte Linux-Treiber aus (`dom0` und Treiberdomänen). PV-VMs erfordern speziell geschriebene PV-Treiber.
4. Vollständige VT-d-Unterstützung einschließlich nicht vertrauenswürdiger Treiberdomänen.
5. S3-Schlaf gut unterstützt.
6. Funktioniert mit den meisten modernen CPUs/Chipsätzen.
7. Größte Leistungseinbußen bei Festplattenoperationen (insbesondere in Qubes, wenn komplexes 2-Layer-Mapping für Linux-Qubes verwendet wird). Keine GPU-Virtualisierung.
8. Funktioniert™ meistens :)

Welche Virtualisierungsmodi werden von VMs verwendet?

Hier finden Sie einen Überblick über die VM-Virtualisierungsmodi:

VM-Typ	Modus
Standard-VMs ohne PCI-Geräte (die meisten VMs)	PVH
Standard-VMs mit PCI-Geräten	HVM
Stub-Domänen – Standard-VMs ohne PCI-Geräte	n/a
Stub-Domänen – Standard-VMs mit PCI-Geräten	PV
Stub-Domänen – HVMs	PV

Was ist das Besondere an Qubes' GUI-Virtualisierung?

Wir haben das Subsystem für die GUI-Virtualisierung mit zwei Hauptzielen entwickelt: Sicherheit und Leistung. Unsere GUI-Infrastruktur führt nur etwa 2.500 Zeilen C-Code (LOC) in die privilegierte Domäne (`dom0`) ein, was sehr wenig ist und somit wenig Raum für Bugs und potenzielle Angriffe lässt. Gleichzeitig ist unsere GUI-Implementierung dank der intelligenten Nutzung des gemeinsamen Speichers von Xen sehr effizient, so dass sich die meisten virtualisierten Anwendungen wirklich so anfühlen, als ob sie nativ ausgeführt würden.

Warum passwortloses sudo?

Bitte beachten Sie diese Seite.

Warum ist dom0 so alt?

Bitte beachten Sie:

- Installieren und Aktualisieren von Software in dom0
- Anmerkung zu `dom0` und EOL

Empfehlen Sie coreboot als Alternative zum Hersteller-BIOS?

Ja, wo es möglich ist, sollte eine Open-Source-Boot-Firmware vertrauenswürdiger sein als eine Closed-Source-Implementierung. coreboot ist daher eine Voraussetzung für Qubes Certified Hardware. Die Anzahl der Rechner, die coreboot derzeit unterstützt, ist begrenzt und die Verwendung von Blobs, die vom Hersteller bereitgestellt werden, ist im Allgemeinen immer noch erforderlich. Wenn coreboot Ihren Rechner unterstützt und nicht bereits installiert ist, benötigen Sie in der Regel zusätzliche Hardware, um es zu flashen. Weitere Informationen finden Sie auf der coreboot-Website/im IRC-Kanal.

Wie sollte ich Probleme mit der Dokumentation melden?

Wenn Sie das Problem selbst beheben können, lesen Sie bitte, wie Sie die Dokumentation bearbeiten können. Wenn nicht, sehen Sie bitte unter Problemverfolgung nach.

Wird Qubes versuchen, nach den GNU Free System Distribution Guidelines (GNU FSDG) zertifiziert zu werden?

Wir wünschten, wir könnten es, aber die traurige Realität ist, dass ein Betriebssystem *nicht sicher sein kann*, wenn es nicht ein gewisses Minimum an proprietären, quelloffenen „Blobs“ (z. B. CPU-Mikrocode-Updates) enthält. Ein zu 100 % freies Betriebssystem, das alle diese Blobs ausschließt, ist anfällig für bekannte Angriffe und daher für jeden Anwendungsfall, bei dem Sicherheit eine Rolle spielt, ungeeignet.

Stattdessen zielt Qubes darauf ab, so frei wie möglich zu sein*, ohne die Sicherheit zu opfern*. Der gesamte Code, der vom Qubes OS Projekt selbst erstellt wird, ist zu 100% frei. Damit Benutzer diesen Code jedoch tatsächlich sicher auf ihrer Hardware ausführen können, müssen wir ihn mit einer kleinen Anzahl von unfreien Blobs koppeln, was Qubes, wie auch die große Mehrheit der Open-Source-Linux-Distributionen, von der GNU FSDG-Zertifizierung disqualifiziert.

Die vier Grundfreiheiten gehören zum Kern unserer Philosophie, aber auch die Sicherheit. Zusammen bestimmen sie unsere Entscheidungen und motivieren unser Handeln. Qubes zielt darauf ab, sowohl die Sicherheit als auch die Softwarefreiheit in dem Maße zu maximieren, wie sie in der heutigen Welt miteinander vereinbar sind.

Siehe auch Ist Qubes OS freie und quelloffene Software? und die Qubes OS-Softwarelizenz.

Sollte ich der Qubes-Website vertrauen?

Diese Website wird auf GitHub Pages gehostet (Warum?). Daher liegt sie weitgehend außerhalb unserer Kontrolle. Wir betrachten dies jedoch nicht als Problem, da wir ausdrücklich mit Misstrauen in die Infrastruktur arbeiten. Aus diesem Grund sind wir der Meinung, dass niemand übermäßiges Vertrauen in die Live-Version dieser Website im Web setzen sollte. Wenn

Sie stattdessen Ihre eigene vertrauenswürdige Kopie dieser Website auf sichere Weise erhalten wollen, sollten Sie unsere Website-Repos klonen, Überprüfen Sie die PGP-Signaturen auf den Commits und/oder Tags signiert mit den doc-signing keys (was bedeutet, dass der Inhalt Überprüfen Sie), und dann entweder Rendern Sie die Website auf Ihrem lokalen Rechner oder lesen Sie einfach den Quelltext, der zum größten Teil absichtlich in Markdown geschrieben ist, damit die Webseite als reiner Text lesbar ist, genau aus diesem Grund. Wir haben uns besondere Mühe gegeben, dies alles so einzurichten, dass niemand der Infrastruktur vertrauen muss und dass die Inhalte dieser Website maximal verfügbar und zugänglich sind.

Was bedeutet es, „der Infrastruktur zu misstrauen“?

Ein zentraler Grundsatz der Qubes-Philosophie lautet „Misstraue der Infrastruktur“, wobei sich „die Infrastruktur“ auf Dinge wie Hosting-Anbieter, CDNs, DNS-Dienste, Paket-Repositories, E-Mail-Server, PGP-Keyserver usw. bezieht. Als Projekt konzentrieren wir uns auf die Sicherung der Endpunkte, anstatt zu versuchen, „die Mitte“ (d.h. die Infrastruktur) zu sichern, da eines unserer Hauptziele darin besteht, die Benutzer davon zu befreien, dass sie ihre Sicherheit unbekannten Dritten anvertrauen müssen. Stattdessen wollen wir, dass die Nutzer so wenig wie möglich vertrauen müssen (idealerweise nur sich selbst und bekannten Personen, denen sie freiwillig vertrauen).

Die Nutzer können niemals die gesamte Infrastruktur, auf die sie angewiesen sind, vollständig kontrollieren, und sie können niemals allen Stellen, die sie kontrollieren, vollständig vertrauen. Daher glauben wir, dass die beste Lösung darin besteht, nicht zu versuchen, die Infrastruktur vertrauenswürdig zu machen, sondern sich stattdessen auf Lösungen zu konzentrieren, die dies überflüssig machen. Wir sind der Meinung, dass viele Versuche, die Infrastruktur vertrauenswürdig erscheinen zu lassen, in Wirklichkeit nur die Illusion von Sicherheit vermitteln und letztlich den tatsächlichen Nutzern einen schlechten Dienst erweisen. Da wir dies weder fördern noch gutheißen wollen, bringen wir unser Misstrauen gegenüber der Infrastruktur ausdrücklich zum Ausdruck.

Siehe auch: Sollte ich der Qubes-Website vertrauen?

Warum verwenden Sie GitHub?

Drei Hauptgründe:

- Wir misstrauen der Infrastruktur einschließlich GitHub (obwohl es Aspekte gibt, an denen wir noch arbeiten).
- Es ist frei (wie Freibier). Wir müssten entweder Zeit oder Geld aufwenden, um eine Lösung selbst zu implementieren oder jemanden dafür zu bezahlen, und beides können wir im Moment nicht entbehren.
- Der Verwaltungs- und Gemeinkostenaufwand ist gering, was angesichts der knappen Zeit, die wir haben, sehr wichtig ist.

Siehe auch: Sollte ich der Qubes-Website vertrauen?

Warum hat die Qubes-Website nicht die Sicherheitsfunktion X?

Obwohl wir die Benutzer davor warnen unangemessenes Vertrauen in diese Website zu setzen, weil wir Misstrauen in die Infrastruktur haben, haben wir keine Einwände gegen die Aktivierung von Sicherheitsfunktionen auf der Website, wenn dies relativ kostengünstig ist und

den Besuchern der Website einen gewissen Nutzen bringt. Wenn also Funktion X nicht aktiviert ist, hat das höchstwahrscheinlich einen der drei folgenden Gründe:

- Unsere GitHub Pages-Plattform unterstützt dies nicht.
- Unsere Plattform unterstützt dies, aber wir haben beschlossen, es nicht zu aktivieren.
- Unsere Plattform unterstützt diese Funktion, aber wir wissen nicht, ob wir sie aktivieren können oder ob wir es vergessen haben, dies zu tun.

Wenn Sie der Meinung sind, dass wir diese Funktion aktivieren können und sollten, lassen Sie es uns bitte wissen!

Benutzer

Kann ich YouTube-Videos in Qubes ansehen?

Auf jeden Fall.

Kann ich Anwendungen wie Spiele ausführen, die Hardware-Beschleunigung erfordern?

Diese werden nicht funktionieren. Wir bieten keine GPU-Virtualisierung für Qubes an. Dies ist hauptsächlich eine Sicherheitsentscheidung, da die Implementierung eines solchen Features höchstwahrscheinlich eine große Menge an Komplexität in die GUI-Virtualisierungsinfrastruktur einbringen würde. Qubes erlaubt jedoch die Verwendung von beschleunigter Grafik (z.B. OpenGL) im Window Manager von `dom0`, so dass alle ausgefallenen Desktop-Effekte trotzdem funktionieren sollten. App-Qubes verwenden eine reine Software-Implementierung von OpenGL (auf CPU-Basis), die für einfache Spiele und Anwendungen gut genug sein kann.

Weitere Diskussionen über das Potenzial für GPU-Passthrough auf Xen/Qubes finden Sie in den folgenden Threads:

- GPU-Übergabe an HVM
- Klarstellungen zur GPU-Sicherheit

Ist Qubes ein Mehrbenutzersystem?

Nein. Qubes gibt nicht vor, ein Mehrbenutzersystem zu sein. Qubes geht davon aus, dass der Benutzer, der `dom0` kontrolliert, das gesamte System kontrolliert. Es ist sehr schwierig, Multi-User-Unterstützung **sicher zu** implementieren. Siehe hier für Details.

In Qubes 4.x werden wir jedoch Verwaltungsfunktionen implementieren. Siehe Admin API und Core Stack für weitere Details.

Was sind die Systemanforderungen für Qubes OS?

Siehe die Systemanforderungen.

Gibt es eine Liste von Hardware, die mit Qubes OS kompatibel ist?

Siehe die Hardware-Kompatibilitätsliste.

Gibt es eine zertifizierte Hardware für Qubes OS?

Siehe Zertifizierte Hardware.

Wie viel Speicherplatz benötigt jeder Qube?

Jeder Qube wird aus einem Template erstellt und teilt sich das Root-Dateisystem mit diesem Template (schreibgeschützt). Dies bedeutet, dass jeder Qube nur so viel Speicherplatz benötigt, wie für die Speicherung seiner eigenen privaten Daten erforderlich ist. Dies bedeutet auch, dass es möglich ist, die Software für mehrere Qubes gleichzeitig zu aktualisieren, indem ein einziger Aktualisierungsprozess in dem Template ausgeführt wird, auf dem diese Qubes basieren. (Diese Qubes müssen dann neu gestartet werden, damit die Aktualisierung in ihnen wirksam wird).

Wie viel Speicherplatz wird für Qubes empfohlen?

Bitte beachten Sie die Systemanforderungen.

Kann ich Qubes auf einem System ohne VT-x/AMD-V oder VT-d/AMD-Vi/AMD IOMMU installieren?

Die neuesten Informationen finden Sie in den Systemanforderungen. Wenn Sie bei der Installation eine Fehlermeldung erhalten, die besagt, dass Ihre „Hardware nicht über die erforderlichen Funktionen verfügt, um fortzufahren“, stellen Sie sicher, dass die Virtualisierungsoptionen in Ihrer BIOS/UEFI-Konfiguration aktiviert sind. Möglicherweise können Sie zu Testzwecken auch ohne die erforderlichen CPU-Funktionen installieren, aber VMs (insbesondere `sys-net`) funktionieren dann möglicherweise nicht korrekt und es gibt keine Sicherheitsisolierung. Für weitere Informationen siehe Qubes-zertifizierte Hardware.

Warum ist VT-x/AMD-V wichtig?

Standardmäßig verwendet Qubes die Virtualisierungsmodi PVH und HVM von Xen, die VT-x/AMD-V erfordern. Das bedeutet, dass ohne VT-x/AMD-V keine VMs in einer Standard-Qubes-Installation gestartet werden können. Wenn Ihrem System VT-x/AMD-V fehlt, dann fehlt ihm auch VT-d/AMD-Vi/AMD IOMMU. (Siehe nächste Frage.)

Warum ist VT-d/AMD-Vi/AMD IOMMU wichtig?

Auf einem System ohne VT-d/AMD-Vi/AMD IOMMU gibt es keinen wirklichen Sicherheitsvorteil durch eine separate NetVM, da ein Angreifer immer einen einfachen DMA-Angriff ausführen kann, um von der NetVM zu `dom0` zu gelangen. Nichtsdestotrotz funktionieren alle anderen Sicherheitsmechanismen von Qubes, wie z.B. die Qube Trennung, ohne VT-d/AMD-Vi/AMD IOMMU. Daher wäre ein System, auf dem Qubes ohne VT-d/AMD-Vi/AMD IOMMU läuft, immer noch wesentlich sicherer als eines, auf dem Windows, Mac oder Linux läuft.

Was ist ein DMA-Angriff?

Direct Memory Access (DMA) ist ein Mechanismus, mit dem PCI-Geräte auf den Systemspeicher zugreifen können (Lesen/Schreiben). Ohne VT-d/AMD-Vi/AMD IOMMU kann jedes PCI-Gerät auf den gesamten Speicher zugreifen, unabhängig von der VM, der es zugewiesen ist (oder wenn es in `dom0` belassen wird). Die meisten PCI-Geräte erlauben es dem Treiber, eine beliebige DMA-Operation anzufordern (z.B. „lege empfangene Netzwerkpakete an dieser Adresse im Speicher ab“ oder „hole diesen Speicherbereich und sende ihn an das Netzwerk“). Ohne VT-d/AMD-Vi/AMD IOMMU hat man also unbegrenzten Zugriff auf das gesamte System. Jetzt muss man nur noch wissen, wo man lesen/schreiben muss, um das System zu übernehmen, anstatt einfach abzustürzen. Aber da man den gesamten Speicher lesen kann, ist das gar nicht so schwer.

Wie lässt sich dies nun auf Qubes OS anwenden? Der obige Angriff erfordert den Zugriff auf ein PCI-Gerät, was bedeutet, dass er nur von der NetVM- oder USB-VM aus durchgeführt werden kann, so dass jemand zuerst in eine dieser VMs einbrechen muss. Das ist aber gar nicht so schwer, denn es gibt eine Menge komplexen Code, der den Netzwerkverkehr verarbeitet. Es gibt eine Reihe von Fehlern in DHCP-Clients, DNS-Clients usw. Die meisten Angriffe auf die NetVM und die USB-VM (aber nicht alle!) erfordern, dass man sich in der Nähe des Zielsystems befindet, z. B. mit demselben Wi-Fi-Netzwerk verbunden ist oder im Falle einer USB-VM physischen Zugang zu einem USB-Anschluss hat.

Kann ich AMD-v anstelle von VT-x verwenden?

Ja, und siehe diese Nachricht.

Kann ich Qubes in einer virtuellen Maschine (z.B. auf VMware) installieren?

Einige Benutzer konnten dies tun, aber es wird weder empfohlen noch unterstützt. Qubes sollte Bare-Metal installiert werden. (Schließlich verwendet es seinen eigenen Bare-Metal-Hypervisor!)

Wie viele Qubes sollte ich haben? Wie kann ich sie am besten organisieren?

Wie Sie Ihre Qubes organisieren zeigt anhand von Beispielen, wie verschiedene Arten von Nutzern ihr Qubes OS System einrichten können, um ihre speziellen Anwendungsfälle zu unterstützen.

Was ist ein Terminal?

Ein Terminal-Emulator, heute oft nur noch als *Terminal* bezeichnet, ist ein Programm, das ein Textfenster bereitstellt. Innerhalb dieses Fensters wird normalerweise eine Shell ausgeführt. Eine Shell bietet eine Befehlszeilenschnittstelle, über die der Benutzer Befehle eingeben und ausführen kann.

Siehe Einführungen auf Wikibooks: hier, hier und hier.

Warum funktioniert mein Netzwerkadapter nicht?

Möglicherweise haben Sie einen Adapter (kabelgebunden, drahtlos), der nicht mit den von Qubes gelieferten Open-Source-Treibern kompatibel ist. Möglicherweise müssen Sie einen binären Blob installieren, der Treiber aus dem linux-firmware-Paket bereitstellt.

Öffnen Sie ein Terminal und führen Sie `sudo dnf install linux-firmware` in dem Template aus, auf dem Ihre NetVM basiert. Sie müssen die NetVM neu starten, nachdem die Vorlage heruntergefahren wurde.

Kann ich Qubes OS zusammen mit einem anderen Betriebssystem installieren (dual-boot/multi-boot)?

Sie sollten das nicht tun, denn es stellt ein Sicherheitsrisiko für Ihre Qubes OS Installation dar. Aber wenn Sie das Risiko verstehen und akzeptieren, lesen Sie die Dokumentation über Multibooting. Sie beginnt mit einer Erklärung der Risiken einer solchen Installation.

Welche Version von Qubes verwende ich?

Siehe hier.

Mein Qubes hat nach einem Template-Update keinen Internetzugang mehr. Was sollte ich tun?

Siehe Update-Fehlerbehebung.

Meine Tastaturlayout-Einstellungen verhalten sich nicht korrekt. Was sollte ich tun?

Siehe Hardware-Fehlerbehebung.

Meine `dom0`- und/oder Templateaktualisierung stockt, wenn ich versuche, sie über die grafische Benutzeroberfläche zu aktualisieren. Was sollte ich tun?

Dies kann in der Regel durch eine Aktualisierung über die Befehlszeile behoben werden.

Öffnen Sie in `dom0` ein Terminal und führen Sie `sudo qubes-dom0-update` aus.

Öffnen Sie in Ihren Templates ein Terminal und führen Sie `sudo dnf upgrade` aus.

Wie führe ich eine Windows-HVM im nicht nahtlosen Modus (d. h. als einzelnes Fenster) aus?

Aktivieren Sie den „Debug-Modus“ in den Einstellungen des Qube, indem Sie entweder das Kästchen „Run in debug mode“ im Einstellungsmenü des Qubes VM Managers aktivieren oder den Befehl `qvm-prefs` ausführen.

Ich habe eine USB-VM erstellt und ihr USB-Controller zugewiesen. Jetzt lässt sich die USB-VM nicht mehr starten.

Dies liegt wahrscheinlich daran, dass eine der Steuerungen keinen Reset unterstützt. Siehe die USB-Fehlerbehebungsanleitung.

Ich habe ein PCI-Gerät einem Qube zugewiesen, dann die Zuweisung aufgehoben und den Qube heruntergefahren. Warum ist das Gerät in `dom0` nicht verfügbar?

Dies ist eine beabsichtigte Funktion. Ein Gerät, das zuvor einer weniger vertrauenswürdigen Qube zugewiesen war, könnte `dom0` angreifen, wenn es dort automatisch neu zugewiesen würde. Um das Gerät in `dom0` wieder zu aktivieren, müssen Sie entweder:

- Den physischen Computer neu starten.

oder folgende Schritte ausführen:

- Gehen Sie zu sysfs (`/sys/bus/pci`), suchen Sie das richtige Gerät, lösen Sie es vom pciback-Treiber und verbinden Sie es wieder mit dem Originaltreiber. Ersetzen Sie `<BDF>` durch die ID Ihres Geräts, zum Beispiel `00:1c.2:`
- `echo 0000:<BDF> > /sys/bus/pci/drivers/pciback/unbind`
- `MODALIAS=`cat /sys/bus/pci/devices/0000:<BDF>/modalias``
- `MOD=`modprobe -R $MODALIAS | head -n 1``
- `echo 0000:<BDF> > /sys/bus/pci/drivers/$MOD/bind`

Siehe auch hier.

Wie kann ich Videodateien abspielen?

Wenn Sie Probleme mit der Wiedergabe einer Videodatei in einem Qube haben, fehlen Ihnen wahrscheinlich die erforderlichen Codecs. Der einfachste Weg, dies zu beheben, ist, den VLC Media Player zu installieren und diesen zum Abspielen Ihrer Videodateien zu verwenden. Sie können dies in mehreren verschiedenen Template-Distributionen tun (Fedora, Debian, etc.).

Für Debian:

- (Empfohlen) Klonen Sie eine bestehende Debian-Vorlage
- Installieren Sie VLC in dieser Vorlage:
- `$ sudo apt install vlc`
- Verwenden Sie VLC zur Wiedergabe Ihrer Videodateien.

Für Fedora:

- (Empfohlen) Klonen einer bestehenden Fedora-Vorlage
- Aktivieren Sie die entsprechenden RPMFusion-Repos in der gewünschten Fedora-Vorlage.
- Installieren Sie VLC in dieser Vorlage:
- `$ sudo dnf install vlc`

- Verwenden Sie VLC zur Wiedergabe Ihrer Videodateien.

Wie kann ich auf mein externes Laufwerk zugreifen?

Der empfohlene Ansatz ist, nur die spezifische Partition, die Sie verwenden wollen, von `sys-usb` zu einem anderen Qube via `qvm-block zu übertragen`. Sie werden im Ziel-Qube als `/dev/xvd*` angezeigt und müssen manuell gemountet werden. Eine andere Möglichkeit ist, das gesamte USB-Laufwerk an die Ziel-Qube anzuschließen. Dies könnte jedoch theoretisch zu einem Angriff führen, da es den Ziel-Qube zwingt, die Partitionstabelle des Geräts zu analysieren. Wenn Sie glauben, dass Ihr Gerät sicher ist, können Sie es anschließen.

In Qubes 4.0 wird dies mit dem Geräte-Widget in der Werkzeugleiste erreicht (standardmäßig in der oberen rechten Ecke, suchen Sie nach einem Symbol mit einem gelben Quadrat). Klicken Sie im oberen Teil der Liste auf das Laufwerk, das Sie anschließen möchten, und wählen Sie dann den Qube aus, an den es angeschlossen werden soll. Obwohl Sie auch das gesamte USB-Gerät an einen Qube anhängen können, indem Sie es im unteren Teil der Liste auswählen, sollte dieser Ansatz im Allgemeinen nicht verwendet werden, da Sie den Ziel-Qube einer unnötigen zusätzlichen Angriffsfläche aussetzen.

Obwohl externe Medien wie externe Festplatten oder Flash-Laufwerke, die über USB angeschlossen sind, im USB-Qube verfügbar sind, wird nicht empfohlen, direkt vom USB-Qube aus auf sie zuzugreifen. Weitere Informationen finden Sie unter Block (Storage) Devices.

Mein verschlüsseltes Laufwerk erscheint nicht in Debian Qube.

Dies ist ein Problem, das Qubes auf Basis von Debian Jessie betrifft. Das Problem ist in Stretch behoben und betrifft keine Fedora-basierten Qubes.

Ein gemischtes Laufwerk mit einigen verschlüsselten Partitionen wird in Nautilus korrekt angezeigt. Die verschlüsselten Partitionen werden identifiziert und der Benutzer wird beim Versuch, die Partition zu mounten, zur Eingabe eines Passworts aufgefordert.

Ein vollständig verschlüsseltes Laufwerk erscheint nicht in Nautilus.

Die Abhilfe besteht darin, das Laufwerk manuell zu entschlüsseln und zu mounten:

- Schließen Sie das USB-Gerät an den Qube an – es sollte als `/dev/xvdi` oder ähnlich angeschlossen sein.
- `sudo cryptsetup open /dev/xvdi bk --type luks`
- `sudo cryptsetup status /dev/mapper/bk` (Zeigt nützliche Statusinformationen an.)
- `sudo mount /dev/mapper/bk /mnt`

Das entschlüsselte Gerät ist nun unter `/mnt` verfügbar – wenn Sie es nicht mehr benötigen, hängen Sie es aus und schließen Sie das Laufwerk.

- `sudo umount /mnt`
- `sudo cryptsetup close bk --type luks`
- Entfernen Sie den USB vom Qube.

Windows Update steckt fest.

Das hat nichts mit Qubes zu tun. Es ist ein langjähriger Windows-Fehler.

Firefox ist im Vollbildmodus eingefroren.

Drücken Sie zweimal `F11`.

Ich habe seltsame Grafikfehler, z. B. wird der Bildschirm teilweise schwarz.

Wenn das Problem dem in diesem Thread beschriebenen ähnelt, versuchen Sie, den Fenster-Compositor zu deaktivieren:

- Q → System Tools → Window Manager Tweaks → Compositor → „Display Compositing aktivieren“ deaktivieren

Bitte melden Sie sich (über die Mailinglisten), wenn dieses Problem bei Ihnen auftritt und ob die Deaktivierung des Compositors das Problem behebt oder nicht.

Mein HVM in Qubes R4.0 lässt mich kein OS starten/installieren

Ich sehe ein Popup-Fenster mit SeaBios und 4 Zeilen, die letzte ist `Probing EDD (edd=off to disable!... ok.`

Geben Sie an einer `dom0`-Eingabeaufforderung ein:

```
qvm-prefs <HVMname> kernel ""
```

Wenn ich versuche, ein Template zu installieren, heißt es, dass keine Übereinstimmung gefunden wurde.

Siehe VM-Fehlerbehebung.

Ich erhalte ständig die Fehlermeldung „Failed to synchronize cache for repo“, wenn ich versuche, meine Fedora-Vorlagen zu aktualisieren

Siehe Update-Fehlerbehebung.

Beim Booten wird die Meldung „Failed to start Load Kernel Modules“ angezeigt

Die vollständige Nachricht sieht wie folgt aus:

```
[FAILED] Der Start von Load Kernel Modules ist fehlgeschlagen.
Siehe 'systemctl status systemd-modules-load.service' für Details.
```

Dies ist nur kosmetischer Natur und kann getrost ignoriert werden.

Warum ist Qubes so langsam und wie kann ich es schneller machen?

Beim Booten startet Qubes mehrere virtuelle Maschinen. Wenn so viele Qubes gleichzeitig laufen, belastet das unweigerlich die Ressourcen Ihres Computers und verursacht Langsamkeit. Der effektivste Weg, um Qubes zu beschleunigen, ist eine leistungsfähigere Hardware - eine schnelle CPU, viel Speicher und schnelle SSDs. Qubes ist beim Lesen von der Festplatte wegen des VM-Overheads langsamer, weshalb wir empfehlen, es auf einer schnellen SSD zu installieren.

Könnten Sie bitte meine Präferenz als Standard festlegen?

Es wäre toll, wenn Qubes standardmäßig so konfiguriert wäre, wie wir es mögen, mit all unseren bevorzugten Programmen und Einstellungen. Dann könnten wir Qubes einfach installieren, ohne irgendwelche Programme installieren oder Einstellungen vornehmen zu müssen. Wir könnten sogar denken, dass, wenn ein bestimmtes Programm oder eine bestimmte Einstellung für *uns* so gut funktioniert, es auch für *alle anderen* gut funktionieren würde, so dass wir eigentlich allen einen Gefallen tun würden! Das Problem ist, dass Qubes Zehntausende von verschiedenen Benutzern mit völlig unterschiedlichen Bedürfnissen und Zwecken hat. Es gibt keine bestimmte Konfiguration, die für alle ideal ist (auch wenn wir glauben, dass unsere Präferenz für alle besser wäre). Das Beste, was wir tun können, ist, die Macht in die Hände der Nutzer zu legen, ihre Qubes-Installationen so zu konfigurieren, wie sie es möchten (natürlich unter Berücksichtigung von Sicherheitseinschränkungen). Aus diesem Grund gewähren wir im Allgemeinen keine Anfragen, die darauf abzielen, dass die Lieblingsprogramme der Benutzer standardmäßig installiert werden oder dass eine Einstellung, die offensichtlich von den Benutzerpräferenzen abhängt, so geändert wird, dass sie den Wünschen des Antragstellers entspricht.

Siehe auch: Wie steht Qubes zum Wechsel von Gastdistributionen?

Die auf einem Qube installierte Software ist nach einem Neustart nicht mehr vorhanden. Warum?

Die Software muss im Template installiert sein, auf dem Ihr Qube basiert.

Entwickler

Gibt es Einschränkungen für die Software, die die Qubes-Entwickler verwenden wollen?

Ja. Im Allgemeinen werden die Qubes-Entwickler keine Software verwenden, wenn es nicht eine *einfache* Möglichkeit gibt, sowohl ihre **Integrität** als auch ihre **Authentizität** zu überprüfen, vorzugsweise über PGP-Signaturen (siehe Überprüfen von Signaturen). Genauer gesagt:

- Wenn PGP-Signaturen verwendet werden, sollte(n) der/die signierende(n) Schlüssel einen gut veröffentlichten Fingerabdruck haben, der über mehrere unabhängige Kanäle überprüfbar ist, oder den Entwicklern über ein Netz des Vertrauens zugänglich sein.
- Wenn die Software sicherheitssensibel ist und eine Kommunikation mit der Außenwelt erfordert, ist eine „geteilte“ Implementierung zu bevorzugen (Beispiele siehe Split GPG und Split Bitcoin).

- Wenn die Software Abhängigkeiten hat, sollten diese gepackt und in Repos für eine der folgenden Versionen verfügbar sein: aktuelle, von Qubes unterstützte Version von Fedora (bevorzugt) oder Debian (es sei denn, alle unsicheren Abhängigkeiten können in einer nicht vertrauenswürdigen VM in einer „geteilten“ Implementierung laufen).
- Wenn die Software aus dem Quellcode erstellt werden muss, müssen der Quellcode und alle Ersteller signiert werden. (Je umständlicher und zeitaufwändiger die Erstellung aus dem Quellcode ist, desto unwahrscheinlicher ist es, dass die Entwickler ihn verwenden).

Warum muss `dom0` 64-Bit sein?

Seit 2013 unterstützt Xen keine 32-Bit-x86-Architektur, und Intel VT-d, das Qubes zur Isolierung von Geräten und Treibern verwendet, ist nur auf Intel 64-Bit-Prozessoren verfügbar.

Darüber hinaus ist es mit Funktionen wie verbessertem ASLR oft schwieriger, einen Fehler unter x64 Linux auszunutzen als unter x86 Linux. Obwohl wir Qubes von Anfang an so konzipiert haben, dass potenzielle Angriffsvektoren begrenzt werden, ist uns dennoch bewusst, dass einige der Codes, die in `dom0` laufen, z.B. unser GUI-Daemon oder der xen-store-Daemon, auch wenn sie noch so einfach sind, einige Bugs enthalten könnten. Und da wir keine separate Speicherdomäne implementiert haben, befinden sich die Festplatten-Backends in `dom0` und sind von den VMs aus „erreichbar“, was die potenzielle Angriffsfläche noch vergrößert. Als wir also vor der Wahl zwischen einem 32-Bit- und einem 64-Bit-Betriebssystem für `dom0` standen, war die Entscheidung fast klar. Die 64-Bit-Option bietet etwas (vielleicht wenig, aber etwas) mehr Schutz gegen einige Klassen von Angriffen und hat gleichzeitig keine Nachteile, außer der zusätzlichen Anforderung eines 64-Bit-Prozessors. Und auch wenn Qubes jetzt einen 64-Bit-Prozessor „braucht“, machte es keinen Sinn, Qubes auf einem System ohne 3-4 GB Speicher laufen zu lassen, und diese haben ohnehin 64-Bit-CPUs.

Was ist die empfohlene Build-Umgebung für Qubes OS?

Jede rpm-basierte 64-Bit-Umgebung, wobei Fedora das bevorzugte Betriebssystem ist.

Wie kann ich Qubes aus Quellen erstellen?

Siehe diese Anweisungen.

Wie kann ich einen Patch einreichen?

Siehe den Artikel Qubes Source Code Repositories.

Wie steht Qubes zum Wechsel von Gastdistributionen?

Im Allgemeinen versuchen wir, die Kultur der einzelnen Distributionen zu respektieren, behalten uns aber das Recht vor, Änderungen vorzunehmen, die wir für angemessen halten. Siehe die Diskussion zu Ausgabe #1014 für ein Beispiel.

Diese Leitlinie dient vor allem dazu, die Wartung zu erleichtern, und zwar auf mehreren Ebenen:

- Weniger Änderungen bedeuten eine einfachere Migration zu neuen Upstream-Distributionsversionen.
- Die Upstream-Dokumentation stimmt mit der in der Qubes-VM laufenden Distribution überein.
- Es ist weniger wahrscheinlich, dass wir Qubes-spezifische Probleme einführen.
- Jede offiziell unterstützte Distribution sollte (idealerweise) den gleichen Satz an Qubes-spezifischen Funktionen bieten – eine Änderung in einer unterstützten Distribution sollte auch in anderen, einschließlich neuen zukünftigen Distributionen, nachvollzogen werden.

Warum beheben Sie keine Upstream-Fehler, die Qubes OS betreffen?

Zunächst ein paar Hintergrundinformationen für den Fall, dass Sie neu in der Welt der Open-Source-Software sind: Es gibt eine große Anzahl verschiedener Open-Source-Projekte, die sich jeweils auf die Software konzentrieren, die sie erstellen und pflegen. Einige konzentrieren sich auf bestimmte Frameworks, Bibliotheken und Hintergrundsubsysteme, die die meisten Benutzer nie zu Gesicht bekommen. Andere konzentrieren sich auf bestimmte Tools und Anwendungen, die diese Frameworks, Bibliotheken und Hintergrundsubsysteme nutzen. Wieder andere konzentrieren sich auf die Kombination vieler verschiedener Werkzeuge und Anwendungen. Und einige, wie Qubes OS, sind ganze Betriebssysteme, die alle Arten anderer Software enthalten. Wenn eine Software eine andere Software verwendet, wird die verwendete Software als „vorgelagert“ bezeichnet, während die Software, die sie verwendet, als „nachgelagert“ bezeichnet wird. So verwendet Qubes OS beispielsweise den Xen-Hypervisor, so dass Xen in Bezug auf Qubes ein „Upstream“-Projekt ist und Qubes in Bezug auf Xen ein „Downstream“-Projekt (dies gilt auch für das jeweilige Projekt, das die Software erstellt und pflegt).

Viele Open-Source-Betriebssysteme, einschließlich Qubes OS, sind transparent in Bezug auf die Tatsache, dass sie „Kompilationen“ von Upstream-Software sind. Im Gegensatz dazu neigen proprietäre, kommerzielle Betriebssysteme wie Windows und macOS dazu, diese Tatsache entweder zu verschleiern oder die Verwendung von Upstream-Software zu vermeiden und stattdessen alles selbst zu machen, weil sie über eine riesige Belegschaft und kommerzielle Einnahmen verfügen, die ihnen dies ermöglichen. Wenn Sie daran gewöhnt sind, ein proprietäres, kommerzielles Betriebssystem zu verwenden, dann werden Sie vielleicht etwas Zeit brauchen, um sich an die Tatsache zu gewöhnen, dass Qubes OS eine Zusammenstellung vieler verschiedener Teile von Open-Source-Software ist.

Lassen Sie uns nun zur ursprünglichen Frage kommen: Warum beheben wir keine Upstream-Fehler, die Qubes OS betreffen? Diese Frage kann auf unterschiedliche Weise auftauchen. Zum Beispiel fragen sich viele Leute, besonders diejenigen, die nicht damit vertraut sind, wie die Entwicklung von Open-Source-Software funktioniert, warum wir manchmal Probleme als „nicht unser Fehler“ schließen. Kümmern wir uns nicht um die Qubes-Nutzer, die von diesen Fehlern betroffen sind? Sind wir wirklich so kalt und herzlos?

Im Gegenteil, gerade weil uns die Qubes-Benutzer so sehr am Herzen liegen, tun wir dies. Es ist wichtig zu verstehen, dass Qubes OS verschiedene Softwareteile aus einer sehr großen Anzahl von Upstream-Projekten kombiniert (vor allem, da es ganze separate Betriebssysteme in sich selbst enthält) und dass viele dieser Projekte viel größere Arbeitskräfte und viel mehr finanzielle Mittel haben als wir. Sie sind besser in der Lage, Fehler in ihrer eigenen Software zu beheben. Sie sind nicht nur diejenigen, die den Code geschrieben haben, sondern sie wissen auch besser, wie man Fehlerbehebungen am besten in die gesamte Codebasis integriert, um

die Wartbarkeit zu gewährleisten. Außerdem gehört ihnen der Code. Wir können kein anderes Projekt dazu zwingen, einen Patch zu akzeptieren, selbst wenn wir aufrichtig glauben, dass es eine gute Fehlerbehebung ist. In einigen Fällen müssen wir unsere eigene Abspaltung eines Upstream-Projekts pflegen, was unsere laufende Wartungslast nur noch erhöht.

Im Gegensatz zu einigen der großen Upstream-Projekte, deren Software wir verwenden, ist das Qubes OS Projekt klein, schlank und konzentriert sich auf ein Ziel: die Erstellung und Pflege eines einigermaßen sicheren Betriebssystems für normale Desktop-Benutzer. Die Qubes-Kernentwickler sind Spezialisten. Sie gehören zu den Besten der Welt, wenn es um Virtualisierungssicherheit, Low-Level-Systemsicherheit und die Implementierung von Sicherheit durch Partitionierung auf Betriebssystemebene geht. Es gibt viele Aspekte der Qubes-OS-Entwicklungsarbeit, für die sie in einzigartiger Weise qualifiziert sind. Daher ist es nur sinnvoll, ihre Zeit dort zu konzentrieren, wo sie den größten Nutzen bringt, nämlich auf sicherheitsrelevante Arbeiten, die nur sie erledigen können. Im Gegensatz dazu wäre es eine verschwenderische Fehlallokation von Fähigkeiten und Talenten (zum langfristigen Nachteil der Qubes-Benutzer), wenn sie Fehler beheben würden, die in Code stecken, den sie nicht geschrieben haben, der nicht zu ihnen gehört, der (in einigen Fällen) zu einem großen Upstream-Projekt mit reichlich Zeit und Ressourcen gehört und den das Upstream-Projekt genauso gut beheben kann (und in vielen Fällen *besser* geeignet ist, da dies *ihr* Spezialgebiet ist).

Außerdem basiert die Frage von vornherein auf einer falschen Annahme, denn wir beheben bereits einige Upstream-Fehler, die Qubes OS betreffen. Zum Beispiel haben die Qubes-Kernentwickler signifikante Beiträge zu Xen geleistet, insbesondere im Bereich der Sicherheit, da unsere Entwickler auf diesen Bereich spezialisiert sind. Die ursprüngliche Frage sollte also anders formuliert werden: „Warum beheben Sie nicht *alle* Upstream-Fehler, die Qubes OS betreffen?“ Wir hoffen, dass Sie uns zustimmen, dass dies eine unangemessene Erwartung wäre.

„Nun gut“, denken Sie vielleicht, „aber es gibt immer noch einen Fehler, der mich betrifft! Was kann ich dagegen tun?“ Erinnern Sie sich an das, was wir oben darüber besprochen haben, wie die Open-Source-Welt funktioniert. Wenn es einen Fehler in einem Stück Upstream-Software gibt, dann gibt es ein Open-Source-Projekt, das für die Erstellung und Wartung dieser Software verantwortlich ist. Sie sind diejenigen, die den Code geschrieben haben und die am besten in der Lage sind, den Fehler zu beheben. Sie sollten stattdessen einen Fehlerbericht im Fehlerverfolgungssystem *dieses* Projekts einreichen. Damit helfen Sie nicht nur allen anderen betroffenen Qubes-Benutzern, sondern auch *allen* nachfolgenden Benutzern dieser Software!

(Anmerkung: Wenn Sie sich über Fälle wundern, in denen ein Fehler bereits von Upstream behoben wurde, aber noch nicht in Ihrer Qubes OS Version angekommen ist, lesen Sie bitte Backports. Dies sind *keine* Fälle, in denen ein Problem als „nicht unser Fehler“ geschlossen wird).

Ist die E/A-Emulationskomponente (QEMU) Teil der Trusted Computing Base (TCB)?

Nein. Im Gegensatz zu vielen anderen Virtualisierungssystemen unternimmt Qubes besondere Anstrengungen, um QEMU *außerhalb* der TCB zu halten. Dies wurde dank der sorgfältigen Verwendung von Xen’s stub domain Funktion erreicht. Weitere Einzelheiten darüber, wie wir die Verwendung von Xen’s nativer Stub-Domain verbessert haben, finden Sie hier.

Wird Secure Boot unterstützt?

UEFI Secure Boot wird nicht von Haus aus unterstützt, da die UEFI-Unterstützung in Xen sehr einfach ist. Die Abhängigkeit von der UEFI-Integrität für Secure Boot ist wohl nicht das beste Design. Die relevanten Binärdateien (`shim.efi`, `xen.efi`, Kernel / `initramfs`) sind nicht vom Qubes-Team signiert und Secure Boot wurde nicht getestet. Intel TXT (verwendet in Anti Evil Maid) versucht zumindest, das Vertrauen in das BIOS zu vermeiden oder einzuschränken. Siehe das Heads-Projekt [1] [2] für ein besser gestaltetes, nicht-UEFI-basiertes sicheres Boot-Schema mit sehr guter Unterstützung für Qubes.

Was ist der klassische Weg, um Qubes OS zu erkennen?

Überprüfen Sie die Existenz der Datei `/usr/share/qubes/marker-vm`. Zusätzlich enthält die letzte Zeile die Qubes-Version (z.B. `4.0`). Die Datei wurde nach der ersten Qubes 4.0 Version eingeführt. Wenn Sie nicht vollständig aktualisierte Systeme unterstützen müssen, überprüfen Sie die Existenz von `/usr/bin/qrexec-client-vm`.

Gibt es eine Möglichkeit, Aufgaben für die kontinuierliche Integration oder DevOps zu automatisieren?

Ja, Qubes unterstützt von Haus aus die Automatisierung über Salt (SaltStack). Es gibt auch das inoffizielle Toolkit ansible-qubes. (**Warnung:** Da es sich hierbei um ein externes Projekt handelt, das nicht vom Qubes-Team geprüft oder gebilligt wurde, kann die Verwaltung von `dom0` ein Sicherheitsrisiko darstellen.)

HILFE, UNTERSTÜTZUNG, MAILINGLISTEN UND FORUM

Die Qubes-Gemeinschaft ist hier, um zu helfen! Da Qubes ein sicherheitsorientiertes Betriebssystem ist, möchten wir sicherstellen, dass Sie sicher bleiben Wir wollen sicherstellen, dass Sie die Unterstützung bekommen, die Sie brauchen, und wir wollen sicherstellen, dass unsere Gemeinschaft ein freundlicher und produktiver Ort bleibt, indem wir sicherstellen, dass wir alle den Verhaltenskodex befolgen und Diskussionsrichtlinien.

Wie man Hilfe und Unterstützung erhält

Lassen Sie uns zunächst feststellen, welche Art von Hilfe Sie benötigen.

Ich habe ein Problem oder eine Frage.

Kein Grund zur Sorge! Wir empfehlen folgendes Vorgehen:

1. Sehen Sie in der Dokumentation nach. Möglicherweise gibt es bereits eine Seite zu diesem Thema. Überprüfen Sie insbesondere die Seiten Anleitungen und Fehlersuche.
2. Durchsuchen Sie die häufig gestellten Fragen (FAQ). Ihre Frage könnte bereits beantwortet sein.
3. Versuchen Sie Suche im Issue Tracker. Möglicherweise gibt es bereits eine offene **oder geschlossene** Frage zu Ihrem Problem. Der Issue Tracker wird ständig mit bekannten Fehlern aktualisiert und kann Workarounds für Probleme enthalten, die Sie haben. Wenn es oben angeheftete Probleme gibt, sollten Sie diese zuerst überprüfen!
4. Versuchen Sie, das Qubes Forum zu durchsuchen. Vielleicht gibt es bereits ein passendes Thema.
5. Versuchen Sie, die Archive der Qubes-Benutzer zu durchsuchen. Vielleicht gibt es bereits einen entsprechenden Thread.

Ich habe weder eine Lösung noch eine Antwort gefunden!

Es tut uns leid, das zu hören! In diesem Fall empfehlen wir, im Qubes Forum oder auf der Qubes-Benutzer Mailingliste. Wählen Sie den Ort, den Sie bevorzugen, aber fragen Sie bitte nicht in beiden gleichzeitig! Bevor Sie fragen, lesen Sie bitte unsere Diskussionsleitlinien und StackOverflow's Ratschläge, wie man gute Fragen stellt. Vergessen Sie nicht: Sicher bleiben!

Ich brauche keine Unterstützung, aber ich glaube, ich habe einen Fehler gefunden.

Wir wären Ihnen dankbar, wenn Sie es melden würden (aber stellen Sie bitte sicher, dass es nicht schon jemand anderes gemeldet hat)! Details finden Sie unter Problemverfolgung.

Ich brauche keine Unterstützung, aber ich möchte eine Funktion beantragen.

Wir können nichts versprechen, aber wir würden es gerne in Betracht ziehen! Details finden Sie unter Problemverfolgung.

Wo ist der beste Ort, um über Qubes zu diskutieren?

Das wäre das Qubes Forum und die Qubes-Benutzer Mailingliste. Bitte werfen Sie einen Blick auf unsere Diskussionsrichtlinien bevor Sie eintauchen. Viel Spaß!

Wie kann ich mich beteiligen und einen Beitrag leisten?

Vielen Dank für Ihre Anfrage! Unter „Wie kann ich beitragen?“ finden Sie alle Möglichkeiten, die Sie haben.

Ich möchte eine Sicherheitslücke melden.

Das klingt eher so, als würden Sie uns helfen! Vielen Dank! Bitte sehen Sie Sicherheitsprobleme in Qubes OS melden.

Sicher bleiben

Die Mailinglisten und das Forum von Qubes sind öffentlich zugänglich. Die Inhalte werden von Suchmaschinen gecrawlt und von Drittanbietern archiviert, auf die wir keinen Einfluss haben. Bitte senden oder posten Sie nichts, was Sie nicht gerne öffentlich diskutiert sehen möchten. Wenn Sie Wert auf Vertraulichkeit legen, verwenden Sie bitte PGP-Verschlüsselung in einer E-Mail außerhalb der Liste.

Die Qubes-Gemeinschaft umfasst Menschen aus allen Bereichen des Lebens und aus der ganzen Welt. Die einzelnen Personen unterscheiden sich in Bezug auf ihre Erfahrungen und ihr technisches Fachwissen. Sie werden mit anderen in Kontakt kommen, deren Ansichten und Ziele sich von Ihren eigenen unterscheiden. Jeder kann schreiben, was er will, solange es nicht gegen unseren Verhaltenskodex verstößt. Seien Sie freundlich und offen, aber glauben Sie nicht alles, was Sie lesen. Benutzen Sie ein gutes Urteilsvermögen und seien Sie besonders vorsichtig, wenn Sie Anweisungen (z. B. das Kopieren von Befehlen) befolgen, die von anderen auf den Listen gegeben werden.

Es ist immer möglich, dass ein böser Akteur versucht, sich als ein Mitglied des Qubes-Teams irgendwo im Internet auszugeben. Bitte gehen Sie nicht davon aus, dass jemand, der behauptet, ein offizielles Mitglied des Qubes-Teams zu sein, dies auch wirklich ist, ohne eine angemessene Form der Authentifizierung, wie z.B. eine verifizierte PGP-signierte Nachricht. (Aber bedenken Sie, dass jeder einen Schlüssel mit einem beliebigen Namen generieren und ihn verwenden kann, um eine Nachricht mit PGP zu signieren, so dass das bloße Vorhandensein einer PGP-Signatur nicht auf Autorität schließen lässt. Was zählt, ist die erfolgreiche Verifizierung.) Alle offiziellen Nachrichten können authentifiziert werden, indem die Signaturen der entsprechenden Tags oder Commits im Qubes-Posts Repository überprüft werden.

Angesichts der Tatsache, dass es Betrüger und andere gibt, die versuchen, Sie in die Irre zu führen, wie sollten Sie die guten von den schlechten Ratschlägen unterscheiden? Das muss jeder für sich selbst entscheiden, aber es ist hilfreich zu wissen, dass viele Mitglieder unserer Gemeinschaft sich durch ihre Beiträge zum Projekt als sachkundig erwiesen haben. Oft signieren diese Personen ihre Nachrichten mit demselben Schlüssel (oder einem anderen Schlüssel, der durch denselben authentifiziert wird), mit dem sie auch ihre Beiträge signieren.

Es fällt Ihnen zum Beispiel leichter, dem Rat von jemandem zu vertrauen, der nachweislich Software-Pakete beigesteuert oder zur Dokumentation beigetragen hat. Es ist unwahrscheinlich, dass Personen, die sich im Laufe der Jahre durch ihre Beiträge einen guten Ruf erarbeitet

haben, das Risiko eingehen würden, bösartige Ratschläge in signierten Nachrichten an öffentliche Mailinglisten zu geben. Da jeder Beitrag zum Qubes OS Projekt öffentlich einsehbar und kryptographisch signiert ist, könnte jeder überprüfen, ob er vom selben Schlüsselinhaber stammt.

Leitlinien für die Diskussion

Qubes-Diskussionen finden hauptsächlich auf `qubes-users`, `qubes-devel` und im Forum statt, die alle unten erklärt werden. Die meisten Fragen sollten an `qubes-users` oder an `qubes-devel` oder das Forum gerichtet werden. **Bitte senden Sie keine Fragen an einzelne Qubes-Entwickler.** Indem Sie eine Nachricht an die entsprechende Mailingliste schicken, geben Sie nicht nur anderen die Möglichkeit, Ihnen zu helfen, sondern Sie können auch anderen helfen, indem Sie eine öffentliche Diskussion über ein gemeinsames Problem oder Interesse starten.

Es handelt sich um offene Treffpunkte, an denen Menschen aus freiem Willen zusammenkommen, um über Qubes zu diskutieren und sich aus gegenseitigem Interesse und gutem Willen gegenseitig zu helfen. Sie sind *nicht* Ihr persönlicher, bezahlter Unterstützungsdienst. **Keiner schuldet Ihnen eine Antwort.** Niemand hier ist dafür verantwortlich, Ihre Probleme für Sie zu lösen. Dennoch gibt es viele Dinge, die Sie tun können, um die Wahrscheinlichkeit zu erhöhen, dass Sie eine Antwort erhalten. Diese Gemeinschaft kann sich glücklich schätzen, eine außergewöhnlich große Anzahl freundlicher und sachkundiger Menschen zu haben, die sich gerne über diese Listen austauschen. Die große Mehrheit von ihnen wird Ihnen gerne helfen, wenn Sie diese einfachen Richtlinien befolgen.

Seien Sie höflich und respektvoll

Denken Sie daran, dass niemand hier verpflichtet ist, Ihnen zu antworten. Denken Sie an Ihre Leser. Die meisten von ihnen kommen nach einem langen, harten Arbeitstag nach Hause. Das Letzte, was sie brauchen, ist ein Wutanfall von jemandem. Wenn Sie unhöflich und respektlos sind, werden Sie mit großer Wahrscheinlichkeit ignoriert werden.

Prägnant sein

Fügen Sie nur wesentliche Informationen ein. Die meisten Ihrer Leser sind sehr beschäftigt und haben nur wenig Zeit. Wir *möchten* einen Teil dieser Zeit damit verbringen, Ihnen zu helfen, wenn wir können. Wenn Sie sich jedoch zu weit ausbreiten, wird es einfacher sein, Sie zu übergehen und jemandem zu helfen, der gleich zum Punkt kommt.

Helfen Sie uns, Ihnen zu helfen

Sagen Sie uns, was Sie bereits ausprobiert haben und welche Dokumentationsseiten Sie bereits gelesen haben. Versetzen Sie sich in die Lage Ihrer Leser. Welche wichtigen Informationen benötigen sie, um Ihnen helfen zu können? Stellen Sie sicher, dass Sie diese Informationen in Ihrer Nachricht angeben. Eine gute Möglichkeit, Ihre Hardware-Details anzugeben, ist Erstellung und Übermittlung eines Berichts zur Hardwarekompatibilitätsliste (HCL), und verlinken Sie dann in Ihrer Nachricht darauf. Stellen Sie Fragen auf die intelligente Art.

Geduldig sein

Verschieben Sie ein Thema nicht öfter als einmal alle drei Tage. Wenn Sie den Eindruck haben, dass Ihre Nachrichten an die Mailinglisten ständig ignoriert werden, vergewissern Sie sich, dass Sie die auf dieser Seite beschriebenen Richtlinien befolgen. Wenn Sie dies bereits getan haben, aber immer noch keine Antworten erhalten, ist es wahrscheinlich, dass niemand, der die Antwort kennt, bisher Zeit hatte, zu antworten. Denken Sie daran, dass die Entwickler sehr beschäftigt mit der Arbeit an Qubes sind. Sie haben normalerweise nur alle paar Tage die Möglichkeit, Fragen auf den Mailinglisten zu beantworten.

Seien Sie ein gutes Mitglied der Gemeinschaft

Wie in jeder sozialen Gemeinschaft erwerben sich die Mitglieder im Laufe der Zeit unterschiedliche Reputationen. Wir möchten, dass diese Diskussionsforen freundliche, produktive Orte sind, an denen Informationen und Ideen zum gegenseitigen Nutzen aller ausgetauscht werden. Wir wissen, dass dies am besten durch die Förderung und Pflege von Gleichgesinnten erreicht werden kann. Diejenigen, die sich durch ihre bisherigen Beiträge als gute Mitglieder der Gemeinschaft erwiesen haben, haben sich unser Wohlwollen verdient, und wir sind besonders darauf bedacht, ihnen zu helfen und mit ihnen zusammenzuarbeiten. Wenn Sie neu in der Gemeinschaft sind, sollten Sie verstehen, dass es einige Zeit dauern kann, bis Sie sich das Wohlwollen der anderen verdienen. Das bedeutet nicht, dass Sie keine Hilfe erhalten werden. Im Gegenteil, wir können uns glücklich schätzen, eine so hilfsbereite und verständnisvolle Gemeinschaft zu haben, dass viele von ihnen Stunden ihrer persönlichen Zeit damit verbringen, völlig Fremden zu helfen, einschließlich vieler, die anonym posten. (Angesichts der Integration von Qubes in Whonix verstehen wir die Komplexität von Privatsphäre und Anonymität besser als die meisten anderen, und wir wissen, dass viele Nutzer keine andere Wahl haben, als anonym zu posten). Weitere Informationen finden Sie im Verhaltenskodex und in den Datenschutzbestimmungen unseres Projekts.

Probleme melden und Änderungen an den richtigen Stellen einreichen

Die Mailinglisten und Forum sind gute Orte, um Fragen zu stellen und Dinge zu diskutieren. Wenn Sie jedoch einen formelleren Bericht einreichen, würden wir es bevorzugen, dass Sie ihn an unseren Issue Tracker senden, damit er nicht übersehen wird. (Bitte denken Sie jedoch daran, dass der Issue Tracker kein Diskussionsforum ist.) Ebenso sollten Sie, wenn Sie sehen, dass etwas in der Dokumentation geändert werden sollte, nicht einfach in einer Diskussion darauf hinweisen. Reichen Sie stattdessen die Änderung ein.

Moderation

Das Moderationsteam ist bestrebt, unseren Verhaltenskodex durchzusetzen. Darüber hinaus sollten die Nutzer keine besonderen Maßnahmen von dem Moderationsteam erwarten. Insbesondere sollten die Nutzer nicht verlangen, dass Beiträge oder Nachrichten von einem Moderator gelöscht oder bearbeitet werden. Die Nutzer werden darauf hingewiesen, dass in den meisten Fällen alle Beiträge als E-Mail an andere Nutzer verschickt werden und dass diese E-Mails nicht aus den Posteingängen anderer gelöscht werden können.

Besondere Regeln und Hinweise für Mailinglisten

Verwenden Sie die richtige Liste

Senden Sie Ihre Nachricht an die richtige Liste. Lesen Sie die folgenden Abschnitte, um herauszufinden, welche Liste die richtige für Ihre Nachricht ist.

Nicht nach oben posten

Top-Posting ist das Platzieren Ihrer Antwort über der zitierten Nachricht, auf die Sie antworten. Bitte unterlassen Sie dies. Stattdessen sollten Sie entweder Ihre Antwort, indem Sie Teile Ihrer Nachricht unmittelbar unter den zitierten Teil setzen, auf den Sie antworten, oder indem Sie Ihre gesamte Antwort unter der zitierten Nachricht platzieren, auf die Sie antworten.

Richtige Betreffzeilen verwenden

Fügen Sie eine präzise und informative Betreffzeile ein. So können andere Ihr Thema in Zukunft leicht finden und als Referenz verwenden. (Schlecht: „Hilfe! Qubes Probleme!“ Gut: „R2B2-Installationsproblem: Apple-Tastatur funktioniert nicht im Installationsprogramm.“)

Senden Sie keine Duplikate

Wenn Ihre Nachricht nicht erfolgreich an die Liste gesendet wurde, ist sie wahrscheinlich im Spam-Filter hängen geblieben. Wir überprüfen den Spam-Filter regelmäßig. Bitte haben Sie etwas Geduld, und Ihre Nachricht sollte innerhalb weniger Tage genehmigt werden (und Ihre E-Mail-Adresse in die Whitelist aufgenommen werden).

Verwenden Sie CC in der Liste

Lassen Sie die Mailingliste während der gesamten Konversation mit CC versehen, es sei denn, es besteht ein besonderes Bedürfnis nach Privatsphäre (in diesem Fall sollten Sie PGP-Verschlüsselung verwenden). Dies erhöht die Wahrscheinlichkeit, dass in Zukunft eine größere Menge nützlicher Informationen für alle verfügbar ist.

Angemessen zitieren

Wenn Sie auf ein Thema antworten (egal, ob es sich um Ihr eigenes oder das eines anderen handelt), sollten Sie darauf achten, dass Sie genügend frühere Nachrichten aus dem Thema zitieren, damit die Leser Ihrer Nachricht den Kontext verstehen können, ohne frühere Nachrichten aus diesem Thema suchen und lesen zu müssen. Jede Antwort sollte die Unterhaltung fortsetzen und im Idealfall als eigenständige Unterhaltung lesbar sein. Zitieren Sie keine Werbung in Signaturen oder in inline-PGP-Signaturblöcken. (Das Zitieren von letzteren beeinträchtigt die Fähigkeit von Programmen wie Enigmail, Antworten korrekt zu zitieren).

Englisch nicht erforderlich

Wenn Sie kein Englisch sprechen, können Sie gerne in Ihrer eigenen Sprache schreiben. Denken Sie jedoch daran, dass die meisten Mitglieder der Liste nur Englisch lesen können. Vielleicht möchten Sie aus Rücksicht auf diese Leser eine automatische Übersetzung in Ihre Nachricht einfügen. Wenn Sie sich dafür entscheiden, auf Englisch zu schreiben, entschuldigen Sie sich bitte nicht dafür, dass Sie es schlecht machen, denn das ist unnötig. Wir verstehen das und werden Sie bei Bedarf um eine Klarstellung bitten.

Vorschläge

Während wir generell offen für Vorschläge für neue Funktionen sind, beachten Sie bitte, dass wir bereits eine ziemlich gut definierte Roadmap haben und es eher unwahrscheinlich ist, dass wir unseren Zeitplan ändern werden, um Ihre Anfrage zu berücksichtigen. Wenn es eine bestimmte Funktion gibt, die Sie gerne in Qubes sehen würden, ist es viel effektiver, einen Patch beizusteuern, der diese Funktion implementiert. Wir nehmen solche Beiträge gerne an, sofern sie unseren Standards entsprechen. Bitte beachten Sie jedoch, dass es immer eine gute Idee ist, Ihre Idee auf der `qubes-devel` Liste zu diskutieren, bevor Sie eine Menge harter Arbeit in etwas stecken, das wir vielleicht nicht akzeptieren können oder wollen.

Google Gruppen

Obwohl die Mailinglisten als Google Group Webforen implementiert sind, wird ein Google-Konto in keiner Weise benötigt, erwartet oder gefördert. Viele Diskutanten (einschließlich der meisten Mitglieder des Qubes-Teams) behandeln diese Listen wie herkömmliche Mailinglisten und interagieren mit ihnen ausschließlich über reine Text-E-Mails mit MUAs wie Thunderbird und Mutt. Der Google Groups Dienst ist nur eine kostenlose Infrastruktur, und wir misstrauen der Infrastruktur. Aus diesem Grund ermutigen wir zum Beispiel die Diskutanten, Split GPG zu verwenden, um alle ihre Nachrichten an die Listen zu signieren, aber wir befürworten nicht die Verwendung dieser Google-Gruppen als Webforen. Hierfür haben wir ein separates, spezielles Forum.

Mailinglisten

In diesem Abschnitt werden die einzelnen Mailinglisten mit Einzelheiten zum Zweck jeder Liste und zu ihrer Nutzung beschrieben. Ein Google-Konto ist für keine dieser Mailinglisten erforderlich.

`qubes-announce`

Dies ist eine Nur-Lese-Liste für diejenigen, die nur sehr wichtige, seltene Nachrichten erhalten möchten. Nur das Qubes-Kernteam kann auf dieser Liste posten. Nur Qubes Security Bulletins (QSBs), neue stabile Qubes OS Releases und Qubes OS Release End-of-Life Mitteilungen werden hier angekündigt.

Um sich anzumelden, senden Sie eine leere E-Mail an
qubes-announce+subscribe@googlegroups.com.
(Hinweis: Ein Google-Konto ist **nicht** erforderlich, jede beliebige E-Mail-Adresse funktioniert.) Um sich abzumelden, senden Sie eine leere E-Mail an
qubes-announce+unsubscribe@googlegroups.com.
Diese Liste verfügt auch über ein herkömmliches E-Mail-Archiv und eine optionale Google Groups-Webschnittstelle.

`qubes-users`

Diese Liste soll Benutzern bei der Lösung verschiedener täglicher Probleme mit Qubes OS helfen. Beispiele für Themen oder Fragen, die sich für diese Liste eignen, sind:

- HCL Berichte

- Probleme bei der Installation
- Probleme mit der Hardware-Kompatibilität
- Fragen der Form: „Wie kann ich...?“

Bitte versuchen Sie, sowohl die Qubes-Website als auch die Archive der Mailinglisten zu durchsuchen, bevor Sie eine Frage stellen. Vergewissern Sie sich außerdem, dass Sie die folgende grundlegende Dokumentation gelesen und verstanden haben, bevor Sie eine Nachricht an die Liste senden:

- Das Installationshandbuch, die Systemanforderungen und die HCL (für Probleme im Zusammenhang mit der Installation von Qubes OS)
- Die Benutzer-FAQ
- Die Dokumentation (für Fragen zur Verwendung von Qubes OS)

Sie müssen angemeldet sein, um Beiträge zu dieser Liste schreiben zu können. Um sich anzumelden, senden Sie eine leere E-Mail an
qubes-users+subscribe@googlegroups.com.
(Hinweis: Ein Google-Konto ist **nicht** erforderlich, jede E-Mail-Adresse funktioniert.) Um eine Nachricht an die Liste zu senden, richten Sie Ihre E-Mail an
qubes-users@googlegroups.com.
Wenn Ihr Beitrag nicht sofort erscheint, nehmen Sie sich bitte etwas Zeit für die Moderation.
Um sich abzumelden, senden Sie eine leere E-Mail an
qubes-users+unsubscribe@googlegroups.com.
Diese Liste verfügt auch über ein herkömmliches E-Mail-Archiv und eine optionale Google Groups-Webschnittstelle.

`qubes-devel`

Diese Liste ist in erster Linie für Personen gedacht, die daran interessiert sind, einen Beitrag zu Qubes zu leisten oder die mehr über die Architektur und Implementierung von Qubes erfahren möchten. Beispiele für Themen und Fragen, die sich für diese Liste eignen, sind:

- Fragen dazu, warum wir bestimmte Architektur- oder Implementierungsentscheidungen getroffen haben.
  - Zum Beispiel: „Warum haben Sie XYZ auf diese Weise implementiert und nicht auf die andere Weise?“
- Fragen zum Code-Layout und zur Position des Codes für bestimmte Funktionen.
- Diskussionen über vorgeschlagene neue Funktionen, Patches usw.
  - Zum Beispiel: "Ich möchte die Funktion XYZ einführen."
- Beigetragener Code und Patches.
- Sicherheitsdiskussionen, die in irgendeiner Weise für Qubes relevant sind.

Sie müssen angemeldet sein, um Beiträge zu dieser Liste zu schreiben. Um sich anzumelden, senden Sie eine leere E-Mail an
qubes-devel+subscribe@googlegroups.com.
(Hinweis: Ein Google-Konto ist **nicht** erforderlich, jede E-Mail-Adresse funktioniert.) Um eine Nachricht an die Liste zu senden, richten Sie Ihre E-Mail an
qubes-devel@googlegroups.com.

Wenn Ihr Beitrag nicht sofort erscheint, nehmen Sie sich bitte etwas Zeit für die Moderation . Um sich abzumelden, senden Sie eine leere E-Mail an qubes-devel+unsubscribe@googlegroups.com.
Diese Liste verfügt auch über ein herkömmliches E-Mail-Archiv und eine optionale Google Groups-Webschnittstelle.

qubes-project

Diese Liste ist für nicht-technische Diskussionen und Koordination rund um das Qubes OS Projekt gedacht.

Beispiele für Themen oder Fragen, die sich für diese Liste eignen, sind:

- Teilnahme (Vorträge, Workshops usw.) an kommenden Veranstaltungen
- Projektfinanzierungsanträge und -strategien
- Diskussionen über FOSS-Governance
- Die meisten Github-Themen, die mit business oder project management getaggt sind

Sie müssen angemeldet sein, um Beiträge zu dieser Liste schreiben zu können. Um sich anzumelden, senden Sie eine leere E-Mail an qubes-project+subscribe@googlegroups.com.
(Hinweis: Ein Google-Konto ist **nicht** erforderlich, jede beliebige E-Mail-Adresse funktioniert.) Um eine Nachricht an die Liste zu senden, richten Sie Ihre E-Mail an qubes-project@googlegroups.com.
Wenn Ihr Beitrag nicht sofort erscheint, nehmen Sie sich bitte etwas Zeit für die Moderation. Um sich abzumelden, senden Sie eine leere E-Mail an qubes-project+unsubscribe@googlegroups.com.
Diese Liste verfügt auch über ein herkömmliches E-Mail-Archiv und eine optionale Google Groups-Webschnittstelle.

qubes-translation

Diese Liste ist für Diskussionen rund um die Lokalisierung und Übersetzung von Qubes OS, seiner Dokumentation und der Website gedacht.

Beispiele für Themen oder Fragen, die sich für diese Liste eignen, sind:

- Fragen zu oder Probleme mit Transifex, der von uns verwendeten Übersetzungsplattform
- Wer verwaltet die Lokalisierung für eine bestimmte Sprache?
- Die meisten Github-Themen mit dem Stichwort Lokalisierung

Sie müssen angemeldet sein, um Beiträge zu dieser Liste schreiben zu können. Um sich anzumelden, senden Sie eine leere E-Mail an qubes-translation+subscribe@googlegroups.com.
(Hinweis: Ein Google-Konto ist **nicht** erforderlich, jede E-Mail-Adresse funktioniert.) Um eine Nachricht an die Liste zu senden, richten Sie Ihre E-Mail an qubes-translation@googlegroups.com.
Wenn Ihr Beitrag nicht sofort erscheint, nehmen Sie sich bitte etwas Zeit für die Moderation. Um sich abzumelden, senden Sie eine leere E-Mail an

qubes-translation+unsubscribe@googlegroups.com.
Diese Liste hat auch eine optionale Google Groups-Webschnittstelle.

Forum

Das offizielle Qubes-Forum ist ein Ort, an dem Sie Fragen stellen, Hilfe erhalten, Tipps und Erfahrungen austauschen können und vieles mehr! Seit langem wünschen sich die Mitglieder unserer Community ein Forum, das die Privatsphäre respektiert und moderne Funktionen bietet, die traditionelle Mailinglisten nicht unterstützen. Die Open-Source-Plattform Discourse erfüllt dieses Bedürfnis für uns, wie auch für viele andere Open-Source-Projekte.

Warum wurde dieses Forum eingerichtet?

Bisher bestand die einzige Möglichkeit, mit unseren Mailinglisten über Google Groups zu interagieren, aber wir wissen nur zu gut, dass die Auswirkungen auf den Datenschutz und die Benutzerfreundlichkeit für viele Mitglieder unserer Gemeinschaft inakzeptabel waren, vor allem, weil seit kurzem eine Anmeldung erforderlich ist, um Themen anzuzeigen. Viele von Ihnen schätzen die niedrigere Einstiegshürde, die Organisation, die Benutzerfreundlichkeit und die modernen sozialen Funktionen, die die heutigen Foren unterstützen. Außerdem bietet Discourse eine E-Mail-Integration für diejenigen, die das traditionelle Mailinglistenformat bevorzugen.

Was ist der Unterschied zu unseren Mailinglisten?

Um es klar zu sagen: Dies ist *kein* Ersatz für die Mailinglisten. Dieses Forum ist einfach ein *zusätzlicher* Ort für Diskussionen. Bestimmte Arten von Diskussionen eignen sich natürlich besser für Mailinglisten oder Foren, und verschiedene Arten von Benutzern bevorzugen unterschiedliche Orte. Wir haben von einigen Benutzern gehört, die die Mailinglisten als etwas einschüchternd empfinden oder die das Gefühl haben, dass ihre Nachricht nicht wichtig genug ist, um eine neue E-Mail zu erstellen, die in Tausenden von Posteingängen landet. Andere wünschen sich eine selektivere Kontrolle über die Themenbenachrichtigungen. Einige Benutzer schätzen einfach die Möglichkeit, eine „Reaktion“ zu einer Nachricht hinzufügen zu können, anstatt eine völlig neue Antwort verfassen zu müssen. Was auch immer Ihre Gründe sind, es liegt an Ihnen zu entscheiden, wo und wie Sie sich an der Konversation beteiligen möchten.

Wird dadurch die Gemeinschaft gespalten?

Viele Open-Source-Projekte (wie Fedora und Debian) haben sowohl Mailinglisten als auch Foren (und zusätzliche Diskussionsforen). In der Tat hatte das Qubes OS Projekt bereits vor der Einführung dieses Forums Diskussionsforen, die nicht auf Mailinglisten basieren, wie z.B. Reddit. Wir glauben, dass dieser zusätzliche Ort das kontinuierliche Wachstum der Community-Beteiligung fördert und die Erfahrungen aller Beteiligten verbessert. Außerdem gehen wir davon aus, dass viele Community-Mitglieder – vor allem die aktivsten – sich für die Teilnahme an beiden Foren entscheiden werden. (Für diejenigen, die es vorziehen, per E-Mail zu kommunizieren, unterstützt Discourse auch das).

Soziale Medien

Das Qubes OS Projekt ist auf den folgenden Social Media Plattformen vertreten:

- Twitter
- Reddit
- Facebook
- LinkedIn

Im Allgemeinen sind diese Foren nicht als primäre Anlaufstellen für den Support gedacht. (Diese wären `qubes-users` und das Forum.) Vielmehr sollen sie in erster Linie dazu dienen, die auf der Newsseite veröffentlichten Artikel weiter zu verbreiten. Wenn Sie eine dieser Plattformen benutzen, können Sie das Qubes OS Projekt auch dort verfolgen, um Neuigkeiten über Qubes zu erhalten.

Inoffizielle Kanäle

Wenn Sie einen anderen Treffpunkt im Internet finden, der oben nicht aufgeführt ist, handelt es sich um einen **inoffiziellen Treffpunkt**, was bedeutet, dass das Qubes-Team ihn **nicht** überwacht oder moderiert. Bitte seien Sie an inoffiziellen Orten besonders vorsichtig.

(Hinweis: Wenn ein Mitglied des Qubes-Teams den Treffpunkt entdeckt und beschließt, dort vorbeizuschauen, sollte dies nicht als Verpflichtung verstanden werden, den Treffpunkt zu überwachen oder zu moderieren. Er bleibt weiterhin inoffiziell. Bitte vergewissern Sie sich auch, dass jemand, der behauptet, ein Qubes-Teammitglied zu sein, auch wirklich eines ist. Es könnte ein Hochstapler sein!)

Hier sind zum Beispiel einige uns bekannte **inoffizielle** Chat-Kanäle, die von der Community unterhalten werden:

- Matrix, Qubes-bezogen: https://matrix.to/#/#cybersec-qubes_os:matrix.org
- `#qubes` Kanal auf `libera.chat` über herkömmliche IRC-Clients

DATENSCHUTZBESTIMMUNGEN

Die Kurzversion ist, dass wir versuchen, Ihre Privatsphäre so weit wie möglich zu respektieren. Wir verkaufen absolut keine Nutzerdaten. Tatsächlich tun wir alles, um Ihnen zu helfen, Ihre Daten vor allen zu schützen, auch vor uns. Zum Beispiel bieten wir dir an, Whonix von dem Moment an, in dem Sie Qubes OS installieren, so einzurichten, dass alle Ihre Updates durch Tor geleitet werden.

Website

Den gesetzlich vorgeschriebenen Text finden Sie in der Datenschutzrichtlinie der Website.

Dies ist nur eine statische Website, die mit Jekyll erstellt und von GitHub Pages gehostet wird. Wir versuchen, so wenig JavaScript wie möglich zu verwenden. Wir hosten alle Ressourcen lokal (keine CDNs von Drittanbietern), so dass Sie dich nur mit einer Domain verbinden müssen. Diese Seite sollte mit dem Tor-Browser und mit blockierten Skripten einfach zu durchsuchen sein. Wir haben auch einen Onion-Service (der Zugriff wird nicht protokolliert). Wir haben sogar dafür gesorgt, dass Sie das Git-Repository dieser Website, einschließlich des gesamten Quellcodes, einfach herunterladen können, so dass Sie die gesamte Website von deinem eigenen lokalen Rechner aus offline betreiben können. Noch besser ist, dass wir die gesamte Dokumentation in Markdown geschrieben haben, so dass Sie den Klartext bequem von Ihrem Terminal aus genießen können. Hier ist das Repo. (Übrigens sind die Git-Tags unserer Repos PGP-signiert, damit Sie die Authentizität des Inhalts überprüfen können). Natürlich verwenden wir keine Werbung oder Tracker, aber dies ist immer noch eine öffentliche Website, so dass Man-in-the-Middle-Angriffe und dergleichen immer eine Möglichkeit sind. Bitte seien Sie vorsichtig. Siehe Sollte ich der Qubes-Website vertrauen?

Server und Repositories aktualisieren

Wir bieten Repositories unter https://yum.qubes-os.org und https://deb.qubes-os.org/.

Wir sammeln und speichern Standard-Serverzugriffs- und Fehlerprotokolle, die IP-Adressen enthalten. Wir verwenden diese Daten für die Erstellung von Statistiken über die Qubes-Benutzerbasis und für die Reaktion auf Vorfälle.

Die Daten werden bis zu drei Monate lang aufbewahrt, damit wir die Statistiken der letzten zwei Monate neu berechnen können, falls etwas schief geht. Danach werden die Daten gelöscht. Wir verkaufen die Daten an niemanden und geben sie auch nicht an Dritte weiter.

Wenn Sie Ihre IP-Adresse vor uns verbergen möchten, empfehlen wir Ihnen dies und helfen Ihnen gerne dabei! Wählen Sie bei der Installation von Qubes OS einfach die Option Whonix, um alle Ihre Updates über Tor zu leiten.

Onion Services

Wir bieten einen Onion-Service für die Website und Onion-Service-Spiegel der Repositories. Der Zugang zu diesen Servern wird nicht protokolliert.

Spiegel (Mirrors)

Es gibt auch andere Spiegelserver von Drittanbietern, die von Freiwilligen betrieben werden. Diese werden sowohl für ISO-Downloads und Aktualisierungen verwendet. Wir haben keine Kontrolle darüber, welche Daten diese Mirrors sammeln oder mit wem sie sie teilen. Bitte lesen Sie die Datenschutzrichtlinien des jeweiligen Spiegelbetreibers.

Qubes OS

Wir haben Qubes OS speziell so entwickelt, dass es nicht möglich ist, Daten direkt von Qubes OS Installationen zu sammeln. Mit anderen Worten: Qubes OS hat nicht die Möglichkeit, „nach Hause zu telefonieren“ und ist absichtlich so konzipiert, dass dies nicht möglich ist. Dies liegt vor allem daran, dass wir sichergestellt haben, dass `dom0` keinen Netzwerkzugang hat.

Wir wollen nicht, dass Daten direkt von Qubes OS Installationen gesammelt werden können, denn wenn jemand diese Möglichkeit hat, ist das System nicht sicher. Wir selbst nutzen Qubes OS täglich für unsere Arbeit und unser Privatleben, daher sind unsere Interessen mit Ihren deckungsgleich. Auch wir wollen Privatsphäre! Zum Glück ist Qubes OS eine freie und quelloffene Software, so dass Sie sich nicht auf unser Wort verlassen müssen.

Natürlich kann es sein, dass Software von Drittanbietern (einschließlich anderer Betriebssysteme), die innerhalb von Qubes OS läuft, nicht so datenschutzfreundlich ist, also achten Sie bitte darauf, was Sie installieren. Wir haben keine Kontrolle über solche Drittanbieter-Software.

Für weitere Informationen, siehe Wie gewährleistet Qubes OS den Datenschutz?