Benutzerdefinierter Baustein

SYS.2: Desktop-Systeme

SYS.2.8: Clients unter Qubes OS

1 Beschreibung

1.1 Einleitung

Qubes OS ist ein freies und sicherheitsorientiertes Open-Source-Betriebssystem, das für Einzelplatz-Desktop-Computer gedacht ist. Qubes OS nutzt die Xen-basierte Virtualisierung, um die Erstellung und Verwaltung isolierter virtueller Maschinen (VMs) zu ermöglichen, die über spezifische Eigenschaften verfügen:

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

In Qubes werden alle Programme in leichtgewichtigen virtuellen Maschinen (VMs), den so genannten Qubes, ausgeführt, die voneinander isoliert sind („Sicherheit durch Abschottung“). Nicht jede Anwendung läuft in einem eigenen Qube. Statt dessen repräsentiert jeder Qube eine Sicherheitsdomäne. Eine spezielle Verwaltungsdomäne namens Dom0 wird verwendet, um die in einer Qubes-Installation definierten virtuellen Maschinen zu verwalten, d.h. zu erstellen, zu starten, anzuhalten und zu löschen.

Standardmäßig basieren alle Anwendungs-VMs (AppVMs) auf einer einzigen, gemeinsamen TemplateVM, obwohl mehrere TemplateVMs erstellt und verwendet werden können. Jede AppVM teilt sich das Dateisystem des Betriebssystems mit ihrer jeweiligen TemplateVM. Eine AppVM hat nur Lesezugriff auf das Dateisystem der TemplateVM, auf der sie basiert, so dass eine AppVM eine TemplateVM in keiner Weise verändern kann. Dies ist wichtig, da es bedeutet, dass, falls eine AppVM jemals kompromittiert wird, die ihr zugrundeliegende TemplateVM (und alle anderen AppVMs, die auf dieser TemplateVM basieren) immer noch sicher sind.

Nur die privaten Dateien, die sich in der Regel in einem Ordner wie `/home` oder `Dokumente` befinden, werden in der AppVM selbst gespeichert und sind somit permanent und stehen nach Herunterfahren und Neustart wieder zur Verfügung. Die Erstellung einer großen Anzahl von Domänen ist also billig: Jede Domäne benötigt nur so viel Speicherplatz, wie für die Speicherung ihrer privaten Dateien erforderlich ist. Für Operationen, die potenziell bösartige Daten betreffen, kann ein spezieller Typ von AppVM namens Disposable VM („Wegwerf-VM“) verwendet werden, der keinen permanenten privaten Speicherplatz besitzt und daher beim Herunterfahren vollständig zerstört wird, wodurch das Risiko einer Infizierung des Systems mit Schadsoftware verringert wird.

Gängige Angriffsvektoren wie Missbrauch von Netzwerkkarten und USB-Controllern sind durch exklusiven Zugriff über eigene Hardware-Qubes isoliert, während die Funktionalität dieser Komponenten durch sichere Vernetzung, Firewalls und USB-Geräteverwaltung aufrechterhalten wird. Integrierte Kopier- und Einfügeoperationen für Dateien und die Zwischenablage machen es einfach, mit verschiedenen Qubes zu arbeiten, ohne die Sicherheit zu beeinträchtigen.

1.2 Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen, die auf Qubes OS-Clients erstellt, verarbeitet, gespeichert oder gesendet werden. Die Anforderungen des Bausteins beziehen sich hauptsächlich auf Linux- und Windows-Clients, die als virtuelle Maschinen unter der Kontrolle des Xen-Hypervisors und der Qubes OS-Betriebsumgebung laufen.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.2.8 *Clients unter Qubes OS* ist für alle Client-Systeme anzuwenden, auf denen als zentrales System Qubes OS eingesetzt wird.

Dieser Baustein enthält grundlegende Anforderungen für den Betrieb von Clients unter der Kontrolle von Qubes OS auf kommerziell erhältlichen IT-Systemen. Es spezifiziert und ergänzt die im Baustein SYS.2.1 *Allgemeiner Client* behandelten Aspekte um die Besonderheiten von Qubes OS-Systemen. Die Besonderheiten der Betriebssysteme, die in den einzelnen VMs laufen, werden in den jeweiligen Bausteinen für diese Systeme behandelt, z.B. SYS.2.2.3 *Clients unter Windows 10* oder SYS.2.3 *Clients unter Linux und Unix*.

Der Baustein umfasst keine Software, die auf den Konfigurationen der in den einzelnen Qubes betriebenen Betriebssysteme aufbaut, wie z.B. E-Mail-Clients oder Office-Software; die diesbezüglichen Anforderungen finden sich in der Schicht APP.1 *Client-Anwendungen* des IT-Grundschutz-Kompendiums. Verfügt der Client über Schnittstellen zum Datenaustausch (z.B. CD/DVD, USB, Bluetooth oder WLAN), müssen die Sicherheitsspezifikationen des Bausteins SYS.4.5 *Wechseldatenträger* erfüllt werden.

Im Rahmen dieses Bausteins wird davon ausgegangen, dass neben dem Administrator nur eine unveränderliche Person ein interaktives Benutzerkonto ständig aktiv nutzt. Clients, die von mehreren Personen nacheinander oder gleichzeitig benutzt werden, erfordern zusätzliche Sicherheitsvorkehrungen, die im Rahmen dieses Bausteins nicht angesprochen werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für Baustein SYS.2.8 *Clients unter Qubes OS* von besonderer Bedeutung:

2.1 Schadsoftware

Schadsoftware wird mit dem Ziel entwickelt, unerwünschte und in der Regel schädliche Funktionen auszuführen. Schadsoftware wird in der Regel heimlich und ohne Wissen oder Erlaubnis des Benutzers aktiviert. Heutzutage bietet Schadsoftware einem Angreifer umfangreiche Kommunikations- und Kontrollmöglichkeiten sowie eine Reihe von Funktionen. Schadsoftware kann unter anderem dazu verwendet werden, an bestimmte Passwörter zu gelangen, Systeme aus der Ferne zu steuern, Schutzsoftware zu deaktivieren und unbefugt an Daten zu gelangen. In Qubes OS ist Schadsoftware auf den Qube beschränkt, in dem die infizierende Datei ausgeführt wurde; wenn es sich dabei um eine AppVM handelt, kann sie die TemplateVM, auf der diese AppVM basiert, nicht ändern. Nach einem Neustart der infizierten AppVM ist also die meiste Schadsoftware beseitigt.

2.2 Nicht vertrauenswürdige oder fehlerhafte Software aus Drittanbieter-Quellen

In Qubes OS ist es leicht möglich, unabhängig von den vom System bereitgestellten Softwarepaketen zusätzliche Software herunterzuladen und zu kompilieren. Werden fertige Softwarepakete verwendet, so werden diese oft nicht immer aus den vorhandenen Paketquellen des einer bestimmten VM zugrundeliegenden Be-

triebssystems installiert; sie können auch ohne weitere Prüfung aus fremden Quellen beschafft werden. Jede dieser alternativen Möglichkeiten der Software-Installation birgt zusätzliche Risiken, da falsche oder inkompatible Software und Schadsoftware installiert werden kann. Wenn diese Software in einer TemplateVM installiert wird, werden sofort alle AppVMs, die auf dieser TemplateVM basieren, kompromittiert. Wenn andererseits solche Software in einer AppVM installiert wird, wird sie beim Herunterfahren dieser AppVM automatisch entfernt.

2.3 Geräte-basierte Angriffe

Das Anschließen eines PCI-Geräts an einen Qube hat ernsthafte Auswirkungen auf die Sicherheit. Es setzt den Gerätetreiber, der im Qube läuft, einem externen Gerät aus. In vielen Fällen kann ein böswilliges Gerät wählen, welcher Treiber geladen werden soll (z.B. durch Manipulation von Geräte-Metadaten wie Hersteller- und Produktkennungen) – selbst wenn der beabsichtigte Treiber ausreichend sicher ist, kann das Gerät versuchen, einen anderen, weniger sicheren Treiber anzugreifen. Darüber hinaus hat diese VM die volle Kontrolle über das Gerät und kann Fehler oder eine böswillige Implementierung der Hardware sowie einfache Sicherheitsprobleme, die die Hardware verursachen kann, ausnutzen.

Der Anschluss eines nicht vertrauenswürdigen USB-Geräts an die Xen-Management-VM Dom0 stellt ein Sicherheitsrisiko dar, da das Gerät einen beliebigen USB-Treiber angreifen, Fehler beim Partition-Table-Parsing ausnutzen oder einfach vorgeben kann, eine Tastatur zu sein. Der gesamte USB-Stack wird eingesetzt, um die vom USB-Gerät präsentierten Daten zu analysieren, um festzustellen, ob es sich um ein USB-Massenspeichergerät handelt, um seine Konfiguration auszulesen usw.

2.4 Evil Maid Angriffe

Ein Evil Maid Angriff ist ein Angriff auf ein unbeaufsichtigtes Gerät, bei dem ein Angreifer mit physischem Zugriff dieses Gerät in einer nicht erkennbaren Weise verändert, so dass er später auf das Gerät oder die Daten darauf zugreifen kann. Der Name bezieht sich auf das Szenario, in dem ein Zimmermädchen ein unbeaufsichtigt in einem Hotelzimmer zurückgelassenes Gerät unterwandern könnte – aber das Konzept selbst gilt auch für Situationen, in denen ein Gerät während des Transports abgefangen oder vorübergehend von Flughafen- oder Strafverfolgungspersonal mitgenommen wird.

Der Angriff beginnt, wenn das Opfer sein Gerät unbeaufsichtigt lässt. Der Angreifer kann dann beginnen, das Gerät zu manipulieren. Wenn das Gerät des Opfers keinen Passwortschutz oder keine Authentifizierung hat, kann ein Eindringling den Computer einschalten und sofort auf die Informationen des Opfers zugreifen. Wenn das Gerät jedoch passwortgeschützt ist, wie bei der Verschlüsselung der gesamten Festplatte, muss die Firmware des Geräts kompromittiert werden, was normalerweise mit einem externen Laufwerk geschieht. Die kompromittierte Firmware liefert dem Opfer oft eine gefälschte Passwortabfrage, die mit dem Original identisch ist. Sobald das Passwort eingegeben wird, sendet die kompromittierte Firmware das Passwort an den Angreifer und entfernt sich nach einem Neustart selbst. Um den Angriff erfolgreich abzuschließen, muss der Angreifer, nachdem er ein zweites Mal unbeaufsichtigt war, zum Gerät zurückkehren, um die jetzt zugänglichen Daten zu stehlen.

2.5 Unvollständige Trennung von Windows 10 VMs

Um eine klare Trennung zwischen TemplateVMs, die die Software enthalten, und AppVMs, die die Benutzerdaten enthalten, zu gewährleisten, müssen die Benutzerdaten auf einem anderen als dem Systemlaufwerk gespeichert werden. Bei Windows 7 wird dies erreicht, indem bei der Vorlagenkonfiguration das Verzeichnis `C:\Users` nach `D:\Users` verschoben wird. Für Windows 10 ist dies aufgrund undokumentierter Merkmale des NTFS-Dateisystems nicht möglich und funktioniert ohnehin nicht. Außerdem wird eine solche Konfiguration laut der Windows-Dokumentation nicht mehr unterstützt.

2.6 Multiboot-Systeme

Dual- oder Multiboot-Systeme stellen besondere Risiken für die Sicherheit eines Qubes OS-Systems dar. Ein Problem ist, dass bei Dual- oder Multiboot, selbst wenn bei der Installation von Qubes OS Verschlüsselung

verwendet wird, die – in der Regel unverschlüsselte – Boot-Partition immer noch ungeschützt ist und vom anderen Betriebssystem böswillig modifiziert werden könnte, was möglicherweise dazu führt, dass Qubes OS selbst modifiziert wird. Das andere Problem ist die Sicherheit der Firmware – z.B. könnte das andere System die BIOS-Firmware infizieren, was zu einer schädlichen Modifikation von Qubes OS selbst führen könnte.

3 Anforderungen

Die spezifischen Anforderungen des Bausteins SYS.2.8 *Clients unter Qubes OS* sind unten aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen verantwortlich. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.2.8 *Clients unter Qubes OS* vorrangig erfüllt werden.

SYS.2.8.A1 Sichere Installation (B)

Qubes OS hat sehr spezifische Systemanforderungen. Auch auf unterstützter Hardware MUSS sichergestellt werden, dass die IOMMU-basierte Virtualisierung im BIOS aktiviert ist. Ohne sie kann Qubes OS keine Isolierung erzwingen. Bei Intel-basierten Boards wird diese Einstellung Intel Virtualization for Directed I/O (Intel VT-d) genannt und bei AMD-basierten Boards AMD I/O Virtualization Technology (oder einfach AMD-Vi). Dieser Parameter MUSS im BIOS des Computers zusammen mit den Standard-Virtualisierungs- (Intel VT-x) und AMD-Virtualisierungs- (AMD-V) Erweiterungen aktiviert werden.

Die Entwickler von Qubes OS haben absolut keine Kontrolle über die Server, die die Installations-ISO-Datei bereitstellen, daher ist es möglich, dass diese kompromittiert werden oder einfach nur kompromittierte ISOs zum Download zur Verfügung stellen, weil ihre Betreiber dies beschlossen haben, aus welchem Grund auch immer. Daher MUSS die digitale Signatur auf der heruntergeladenen ISO immer vor der Installation überprüft werden.

Qubes OS kann nicht als virtuelle Maschine unter einem anderen Hypervisor wie z.B. VirtualBox, VMware oder Hyper-V installiert werden, da der Hypervisor Xen, auf dem Qubes OS basiert, vom Typ 1 (Hardware-Hypervisor) ist und keine verschachtelte Virtualisierung unterstützt.

Qubes OS SOLLTE auf einem separaten Laufwerk installiert werden, vorzugsweise auf einer SSD mit mindestens 40 GB freiem Speicherplatz, ohne dass ein anderes Betriebssystem auf diesem Laufwerk installiert ist. Zu Testzwecken kann das System auf einem schnellen USB 3.0-Stick installiert werden; die ausschließliche Verwendung von USB 2.0 führt zu einem inakzeptabel langsamen System.

SYS.2.8.A2 Authentifizierung von Administratoren und Benutzern [Benutzer] (B)

Um den Client nutzen zu können, MÜSSEN die Benutzer durch das IT-System authentifiziert werden.

SYS.2.8.A3 Keine zusätzliche Software in Dom0 (B)

Normalerweise sollte es nur wenige Gründe für die Aktualisierung von Software in der Verwaltungsdomäne Dom0 geben. Dies liegt daran, dass es in Dom0 kein Netzwerk gibt, was bedeutet, dass, selbst wenn einige Fehler z.B. im Dom0 Desktop Manager entdeckt werden, dies kein echtes Problem für Qubes darstellt, da die gesamte in Dom0 laufende Software von Drittanbietern in keiner Weise von VMs oder dem Netzwerk aus zugänglich ist. Zusätzliche Software DARF in Dom0 erst nach einer gründlichen Analyse der möglichen Fol-

gen für die Sicherheit von Dom0 installiert werden, da dies mit hoher Wahrscheinlichkeit die Sicherheit des gesamten Systems durch die Installation von Fehlern oder sogar Schadsoftware in Dom0 gefährdet. Software-Installationen in Dom0 MÜSSEN eine seltene Ausnahme sein.

SYS.2.8.A4 Keine Ausführung von Anwendungen auf einer TemplateVM [Benutzer] (B)
Mit Ausnahme eines Texteditors, der zum Ändern von Konfigurationsdateien verwendet wird, DARF man Benutzeranwendungen wie Mail- oder Office-Software NICHT in TemplateVMs oder in Dom0 ausführen. Nur die Installation und Aktualisierung von Software ist als Verwendung einer TemplateVM akzeptabel. Alle Anwendungen MÜSSEN auf AppVMs ausgeführt werden.

SYS.2.8.A5 Kein Netzwerkzugriff von TemplateVMs (B)
TemplateVMs DÜRFEN NICHT standardmäßig Zugriff auf Netzwerk-VMs (z.B. `sys-firewall`) haben. Stattdessen MUSS die zugeordnete Netzwerk-VM als „`none`“ angegeben werden. Jegliche Software-Installation und -Aktualisierung SOLLTE nur vom dedizierten Update-Server aus erfolgen, vorzugsweise über das Update-Widget der TemplateVM. Software, die nicht über den Aktualisierungsserver verfügbar ist, wie z.B. spezielle Gerätetreiber, DARF erst nach einer gründlichen Analyse der möglichen Folgen in einer TemplateVM installiert werden, da dies mit hoher Wahrscheinlichkeit die Sicherheit der TemplateVM und aller von dieser TemplateVM abhängigen AppVMs gefährdet.

SYS.2.8.A6 Installation von Aktualisierungen und Patches (B)
Die Verantwortlichen MÜSSEN Informationen über bekannt gewordene Schwachstellen erhalten. Updates und Patches für Dom0 MÜSSEN so schnell wie möglich installiert werden, sobald der Qubes Updater anzeigt, dass solche Patches verfügbar sind. Patches für TemplateVMs MÜSSEN installiert werden, wenn dies zweckmäßig ist; normalerweise ist es nicht notwendig, sie sofort zu installieren, wenn sie verfügbar sind. Es kann ratsam sein, zuerst eine TemplateVM zu klonen und riskante Patches in diesem Klon zu installieren, um sie dort zu testen. Nach dem Herunterfahren einer gepatchten TemplateVM werden deren Patches automatisch auf die abhängigen AppVMs angewendet, sobald diese wieder gestartet werden.

SYS.2.8.A7 Firewall-Konfiguration (B)
Jeder Qube in Qubes ist über eine Firewall-VM mit dem Netzwerk verbunden, die zur Durchsetzung von Richtlinien auf Netzwerkebene verwendet wird. Standardmäßig gibt es eine Standard-Firewall-VM, aber es steht dem Benutzer frei, bei Bedarf weitere zu erstellen. Die Firewall für eine AppVM wird durch geeignete `iptables`-Regeln gesteuert, die die Adressen einschränken, mit denen sich diese AppVM verbinden kann. Diese Adressen MÜSSEN so restriktiv wie möglich gewählt werden, um Datenlecks von empfindlichen AppVMs zu vermeiden; es kann sogar notwendig sein, von einigen AppVMs keine Netzwerkverbindungen zuzulassen, indem für diese AppVMs als zugeordnete Netzwerk-VM „`none`“ angegeben wird..

Ohne explizite zusätzliche Regeln ist kein Zugriff von außen oder von anderen VMs erlaubt. Diese Regeln MÜSSEN so restriktiv wie möglich spezifiziert werden, z.B. nur den Zugriff auf ein lokales Netz und keinen Zugriff von anderen Qubes oder von außerhalb des System auf eine AppVM erlauben. Die AppVM kann die Regeln, denen sie unterworfen ist, nicht ändern.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.2.8 *Clients unter Qubes OS*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.8.A8 Festplattenverschlüsselung (S)
Wenn die physische Sicherheit des Systems, auf dem Qubes OS läuft, nicht immer gewährleistet werden kann, SOLLTE die Festplattenverschlüsselung als Installationsoption gewählt werden.

SYS.2.8.A9 Verwendung eines USB-Qube (S)
Wenn externe USB-Geräte während der Installation oder zu einem späteren Zeitpunkt an das Client-System angeschlossen werden sollen, SOLLTE ein USB-Qube installiert werden. Ein USB-Qube fungiert als sicherer Schnittstelle zu potenziell bösartigen USB-Geräten und verhindert, dass diese mit Dom0 in Kontakt kommen (was andernfalls für die Sicherheit des gesamten Systems fatal sein könnte). Dadurch werden einige der Sicherheitsauswirkungen der Verwendung von USB-Geräten gemildert.

Die Möglichkeit der Umsetzung dieser Anforderung muss besonders geprüft werden, wenn das System eine USB-Tastatur verwendet, da keine Eingabe darüber möglich ist, wenn die Tastatur an einen nicht laufenden USB-Qube angeschlossen ist.

SYS.2.8.A10 Beschränkung von Windows 10 VMs auf das lokale Netzwerk (S)

Die Firewall-Regeln für Windows 10 VMs SOLLTEN so angegeben werden, dass der Zugriff auf das lokale Netz beschränkt ist. Dies blockiert effektiv jede Übertragung von Telemetriedaten, da keine VM die für sie festgelegten Firewall-Regeln ändern kann. Die Firewall-Regeln werden von der für diese VM ausgewählten Firewall-VM (normalerweise `sys-firewall`) durchgesetzt.

SYS.2.8.A11 Verwendung von Disposable VMs [Benutzer] (S)

Wenn verdächtige Daten (z.B. Mail-Anhänge aus unbekannten Quellen) verarbeitet werden müssen, SOLLTE dies mit den Funktionen geschehen, die für Disposable VMs vorgesehen sind. Für Operationen, die keinen Netzzugang benötigen, SOLLTE die Verwendung von Disposable VMs auf Basis einer TemplateVM ohne Netzzugang in Betracht gezogen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.2.8 *Clients unter Qubes OS* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

SYS.2.8.A12 Schutz gegen unautorisierte Anmeldungen (H)

Ein YubiKey kann verwendet werden, um die Benutzer-Authentifizierung in Qubes zu verbessern, z.B. um das Risiko zu verringern, dass jemand das Passwort ausspioniert. Dies kann auch die Sicherheit etwas verbessern, wenn eine USB-Tastatur eingesetzt wird. Die Verwendung eines YubiKey SOLLTE in Betracht gezogen werden, um eine erhöhte Sicherheit bei der Anmeldung zu erreichen.

SYS.2.3.A13 Zwei-Faktor-Browser-Authentifizierung (H)

Die Zwei-Faktor-Authentifizierung SOLLTE durch Installation des Qubes U2F-Proxy verwendet werden. Die U2F-Spezifikation („Universal 2nd Factor“) definiert Protokolle für mehrere Schichten von USB bis zur Browser-API, und der gesamte Stack ist für die Verwendung mit Webanwendungen (meist Websites) in Browsern vorgesehen.

SYS.2.8.A14 Konfiguration des eingehenden Netzwerkzugriffs auf VMs (H)

Normalerweise ist jeglicher Netzwerkverkehr zwischen den virtuellen Maschinen aus Sicherheitsgründen verboten. In besonderen Situationen kann es jedoch sinnvoll sein, bestimmten virtuellen Maschinen selektiv zu erlauben, eine Netzwerkverbindung untereinander herzustellen. Um die Vernetzung zwischen zwei VMs zu erlauben, müssen in der Firewall-VM, mit der beide VMs verbunden sind, entsprechende `iptables`-Regeln angegeben werden. Zusätzlich muss in jeder virtuellen Maschine eine `iptables`-Regel angegeben werden, die den Zugriff von der anderen VM erlaubt. Um diese Regeln dauerhaft zu machen, müssen sie in die Konfigurationsdateien all dieser Qubes eingetragen werden. Diese Regeln SOLLTEN so restriktiv wie möglich spezifiziert werden, um die Freigabe des Zugriffs auf ganze Teilnetze zu vermeiden.

Damit auf einen in einer virtuellen Maschine vorhandenen Dienst in der Standardeinstellung (in der die VM `sys-firewall` als Netzwerk-VM hat, die wiederum `sys-net` als Netzwerk-VM hat) von außerhalb des Qubes OS-Systems zugegriffen werden kann, muss Folgendes getan werden:

- In der `sys-net` VM:
  - Pakete von der Außenwelt zur `sys-firewall` VM leiten
  - Zulassen der Übertragung von Paketen von `sys-net` nach `sys-firewall`
- In der `sys-firewall` VM:
  - Pakete von der `sys-net` VM zur Ziel-VM leiten
  - Zulassen der Übertragung von Paketen durch `sys-firewall` zur Ziel-VM
- In der Ziel-VM:
  - aus `sys-firewall` empfangenen Paketen erlauben, den Dienst zu erreichen

SYS.2.8.A15 Konfiguration von Windows 10 TemplateVM und AppVM (H)

Die einzelnen Benutzerdatenverzeichnisse `C:\Benutzer\username\Dokumente` MÜSSEN nach der Installation der Windows 10 TemplateVM manuell von Laufwerk `C:` auf Laufwerk `D:` verschoben werden. Damit werden dann alle in diesen Verzeichnissen gespeicherten Benutzerdaten in den AppVMs statt in der TemplateVM aufbewahrt.

Konfigurationsdaten, wie sie in Verzeichnissen wie `AppData` gespeichert sind, verbleiben weiterhin in der TemplateVM, so dass ihre Änderungen bei jedem Herunterfahren der AppVM verloren gehen. Um dauerhafte Änderungen an diesen Konfigurationsdaten vorzunehmen, müssen sie in der TemplateVM geändert werden, d.h. Anwendungen müssen dort gestartet werden, was die Sicherheit der TemplateVM verletzt und vielleicht sogar gefährdet. Solche Änderungen SOLLTEN nur bei absoluter Notwendigkeit und mit großer Sorgfalt vorgenommen werden. Es ist eine gute Idee, sie zuerst in einer geklonten TemplateVM zu testen, bevor sie in der Produktions-VM angewendet werden.

Datei-Kopieroperationen in eine Windows 10 VM sind möglich, wenn die in Qubes OS definierte Eigenschaft `default_user` auf den für den Zugriff auf diese VM verwendeten Benutzernamen gesetzt ist, was in der Verwaltungsdomäne Dom0 über den Befehl
`qvm-prefs VMname default_user username`
erfolgen kann. Wenn diese Eigenschaft nicht oder auf einen falschen Wert gesetzt ist, werden die auf diese VM kopierten Dateien im Ordner
`C:\Windows\System32\config\systemprofile\Documents\QubesIncoming\srcVM`
gespeichert. Wenn die Ziel-VM eine AppVM ist, hat dies zur Folge, dass die Dateien in der entsprechenden TemplateVM gespeichert werden und somit beim Herunterfahren der AppVM verloren gehen.

SYS.2.8.A16 Windows 10-Verwendung gemäß DSGVO (H)

Wenn Windows 10 zur Verarbeitung personenbezogener Daten verwendet wird, ist keine automatische Datenübermittlung in Länder außerhalb der EU ohne ausdrückliche Zustimmung der betroffenen Person(en) oder ggf. eine andere gesetzliche Zustimmung zulässig. Da kein zuverlässiger Weg gefunden wird, um das Senden von Telemetrie von Windows 10 aus vollständig zu kontrollieren, muss das System, das personenbezogene Daten enthält, vollständig vom Internet abgeschirmt werden.

Dies SOLLTE durch die Installation von Windows 10 auf einer TemplateVM erreicht werden, wobei das Verzeichnis der Benutzerdaten auf ein separates Laufwerk (normalerweise `D:`) verschoben wird. Personenbezogene Daten DÜRFEN NICHT innerhalb der TemplateVM gespeichert werden, sondern in AppVMs, die von dieser TemplateVM abhängen. Der Netzwerkzugriff durch diese AppVMs MUSS auf das lokale Netz beschränkt sein. Jeglicher Datenaustausch der AppVMs MUSS auf Datei- und Zwischenablageoperationen zu und von anderen VMs im selben Qubes OS-System beschränkt sein.

SYS.2.8.A17 Schutz gegen Evil Maid Angriffe (H)

Anti Evil Maid (AEM) ist eine Implementierung eines TPM-basierten dynamischen vertrauenswürdigen Bootvorgangs für `dracut/initramfs`-basierte Betriebssysteme (Fedora, Qubes usw.) mit dem primären Ziel, Evil Maid Angriffe zu verhindern. Kurz gesagt, AEM verlässt sich auf TPM und eine Funktion, die in Intels vPro-CPUs (TXT) zu finden ist, um Manipulationen an verschiedenen Boot-Komponenten zu erkennen. Bei mobilen Systemen wie Notebooks oder wenn die Gefahr besteht, dass sich jemand physischen Zugang zum Computer verschafft, wenn dieser ausgeschaltet bleibt, oder wenn Qubes im Dual-Boot-Modus verwendet wird, sollte die Installation von Anti Evil Maid (oder anderen Boot-Schutzverfahren wie etwa Heads) in Erwägung gezogen werden, wenn die Hardware-Voraussetzungen erfüllt sind. AEM wird den Benutzer über alle nicht autorisierten Änderungen am BIOS oder der Boot-Partition informieren.

SYS.2.8.A18 Split GPG (H)

Split GPG implementiert ein ähnliches Konzept wie eine Smart Card mit den privaten GPG-Schlüsseln des Anwenders, mit der Ausnahme, dass die Rolle der „Smart Card“ eine andere Qubes AppVM spielt. Auf diese Weise kann eine nicht so vertrauenswürdige Domäne alle Krypto-Operationen, wie Ver-/Entschlüsselung und Signierung, an eine andere, vertrauenswürdigere, vom Netz isolierte Domäne delegieren. Auf diese Weise ermöglicht die Kompromittierung der Domäne, in der eine Client-Anwendung ausgeführt wird, dem Angreifer

nicht, automatisch auch alle Schlüssel zu stehlen. Für hohe Sicherheitsanforderungen SOLLTE Split GPG verwendet werden.

SYS.2.8.A19 Zentralisierte Verwaltung über SALT (H)

Qubes OS enthält die Salt (auch SaltStack genannte) Management-Engine in Dom0 als Standard (wobei einige Zustände bereits vorkonfiguriert sind). Salt ermöglicht es Administratoren, ihre Systeme einfach zu konfigurieren. In einer verwalteten Umgebung SOLLTE Salt verwendet werden, um die Rollen von Administrator und Benutzer zu trennen, wobei die VM-Verwaltung von Administratoren ohne Zugriff auf Benutzerdaten und die VM-Nutzung von Benutzern ohne Zugriff auf VM-Verwaltungsfunktionen durchgeführt wird. Alle Richtlinien, die zur Kontrolle von Salt festgelegt werden, sollten so restriktiv wie möglich sein.

SYS.2.8.A20 Verschlüsselte AppVMs (H)

Bei AppVMs, die sensible Informationen enthalten, SOLLTE das private Laufwerk verschlüsselt werden. Bei Windows-AppVMs könnte dies mit BitLocker oder Tools wie VeraCrypt zur Verschlüsselung von Laufwerk D: geschehen, bei Linux-basierten AppVMs könnte LUKS/dm-crypt-Verschlüsselung für das Verzeichnis /rw (das /home und /usr/local enthält) verwendet werden. Dies kann auch verwendet werden, um den Zugriff auf solche AppVMs auf ausgewählte Benutzer zu beschränken, die die Verschlüsselungspassphrase kennen oder Zugriff auf ein Token haben, das den Schlüssel enthält.

Solange das System nicht unbeaufsichtigt gelassen wird, während eine verschlüsselte AppVM läuft, besteht keine Notwendigkeit, die entsprechende TemplateVM zu verschlüsseln, da alle möglicherweise sensiblen Daten, die von der AppVM in die TemplateVM kopiert werden, beim Herunterfahren der AppVM zerstört werden.

Wenn verschlüsselte AppVMs verwendet werden, SOLLTE die Verschlüsselung der Systemplatte während der Installation von Qubes OS als Option ausgewählt werden, und eine Installation ohne Auslagerungsdatei SOLLTE in Betracht gezogen werden, um Situationen zu vermeiden, in denen sensible Daten dort verbleiben könnten.

4 Weiterführende Informationen

Weitere Informationen über Gefährdungen und Sicherheitsanforderungen und -maßnahmen für Baustein SYS.2.8 *Clients unter Qubes OS* sind u.a. in den folgenden Publikationen zu finden, auf die zuletzt am 26.08.2020 zugegriffen wurde:

[QubesDoc]	Dokumentation der Installation, Konfiguration und Verwendung von Qubes OS https://www.Qubes-os.org/doc/,
[QubesInstall]	Installationsanleitung für Qubes OS https://www.Qubes-os.org/doc/installation-guide/
[QubesDevelopment]	Entwicklerdokumentation, Diskussion aktueller / zukünftiger Erweiterungen https://github.com/QubesOS/Qubes-issues/issues
[QubesUsers]	Google Benutzergruppe, Diskussion von Anwendungsproblemen https://groups.google.com/forum/?nomobile=true#!forum/Qubes-users
[QubesForum]	Benutzerforum, Diskussion von Anwendungsproblemen und aktuellen Entwicklungen https://qubes-os.discourse.group/

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird

den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein SYS.2.8 *Qubes OS Clients* relevant:

- G 0.14 Abfangen von Informationen / Spionage
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation mit Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Vorschriften
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	CIA	G 0.14	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.38	G 0.39	G 0.46
SYS.2.8.A1			X	X	X	X	X	X	X			X			X	X
SYS.2.8.A2		X	X				X				X		X			
SYS.2.8.A3		X	X	X	X	X	X		X			X			X	X
SYS.2.8.A4		X	X	X	X	X			X			X			X	X
SYS.2.8.A5		X	X		X	X			X			X			X	X
SYS.2.8.A6				X					X			X			X	X
SYS.2.8.A7		X	X						X						X	
SYS.2.8.A8		X				X				X				X		X
SYS.2.8.A9		X	X		X			X							X	X
SYS.2.8.A10		X	X							X					X	
SYS.2.8.A11			X	X											X	X
SYS.2.8.A12	CIA	X	X		X	X	X				X					X
SYS.2.8.A13	CIA	X				X			X				X	X		X
SYS.2.8.A14	CI	X	X		X	X						X				
SYS.2.8.A15	CI	X	X						X	X		X			X	X
SYS.2.8.A16	CI	X	X							X				X		
SYS.2.8.A17	CIA	X	X	X	X	X	X								X	X
SYS.2.8.A18	CI	X	X						X							
SYS.2.8.A19	CIA		X		X		X				X	X	X			
SYS.2.8.A20	CI	X	X			X							X	X		X