SYS.2: Desktop-Systeme

SYS.bd.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 Eigen-schaften verfügen:

- Einsatzzweck: mit einem vordefinierten Satz von einer oder mehreren isolierten Anwendun-gen, 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 Betriebssys-temen wie Linux (Fedora, Debian) oder Windows basieren.
- Vertrauensebenen: von vollständig bis nicht existent. Alle Fenster werden in einer einheitli-chen 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 genann-ten Qubes, ausgeführt, die voneinander isoliert sind („Sicherheit durch Abschottung“). Nicht jede An-wendung 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 lö-schen. Es gibt auch einige sogenannte Service Qubes im System. Jeder Qube, der eine Verbindung zum Internet herstellt, tut dies über einen Service Qube, der ein Netzwerk bereitstellt. Wenn man auf USB-Geräte zugreifen muss, erledigt das ein anderer Service Qube.

Standardmäßig basieren alle Anwendungs-VMs (AppVMs) auf einer einzigen, gemeinsamen Tem-plateVM, 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 Tem-plateVM in keiner Weise verändern und damit möglicherweise sie und damit auch alle davon abhän-gigen AppVMs kompromittieren kann.

Nur die privaten Dateien, die sich in der Regel in einem Ordner wie /home oder Dokumente befin-den, werden in der AppVM selbst gespeichert und sind somit permanent und stehen nach Herunter-fahren 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 Datei-en erforderlich ist. Für Operationen, die potenziell bösartige Daten betreffen, kann ein spezieller Typ von AppVM namens DisposableVM („Wegwerf-VM“) verwendet werden, der keinen perma-nenten privaten Speicherplatz besitzt und daher beim Herunterfahren vollständig zerstört wird.

Gängige Angriffsvektoren wie das Missbrauchen 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. Inte-grierte Kopier- und Einfügeoperationen für Dateien und die Zwischenablage machen es einfach, mit ver-schiedenen 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.bd.2.8 *Clients unter Qubes OS* ist für alle Client-Systeme anzuwenden, die mit Qubes OS be-trieben werden.

Dieser Baustein enthält Anforderungen für Clients, die mit Qubes OS betrieben werden. Allgemeine Anfor-derungen an Client-Systeme werden in diesem Baustein nicht behandelt. Sie sind im Baustein SYS.2.1 *Allgemeiner Client* zu finden. Die Besonderhei-ten der Betriebssysteme, die in den einzelnen VMs laufen, wer-den in den jeweiligen Bausteinen für diese Sys-teme 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.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.bd.2.8 *Clients unter Qubes OS* von besonderer Bedeutung.

2.1 Schadsoftware

Schadsoftware wird in der Regel heimlich und ohne Wissen oder Erlaubnis des Benutzers aktiviert. 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 Schadsoftware, die Veränderung an den Systemdaten vorgenommen hat, beseitigt, während Schadsoftware, die in den privaten Daten der AppVM gespeichert wurde, auch nach einem Neustart noch vorhanden ist und bei einem neuen Zugriff auf die betreffenden Daten wieder aktiviert wird.

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 ggf. zu kompilieren. Werden fertige Softwarepakete verwendet, so werden diese oft nicht immer aus den vorhandenen Paketquellen des einer bestimmten VM zugrundeliegenden Betriebssystems 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.

2.3 Geräte-basierte Angriffe

Das Anschließen eines PCI-Geräts an einen Qube kann ernsthafte Auswirkungen auf die Sicherheit haben. 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 ausnutzen und so diese Hardware kompromittieren. Umgekehrt ist es auch möglich, dass auf diesem Weg die Sicherheit des Hostsystems durch gezielte Einwirkung über dieses Gerät kompromittiert wird.

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. Eine Manipulation des USB-Stacks kann daher ebenfalls zu Angriffen auf die Integrität von Dom0 genutzt werden.

2.4 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. Sie kann daher vom anderen Betriebssystem böswillig modifiziert werden, 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

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.bd.2.8 *Clients unter Qubes OS* aufgeführt. Der ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt.

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.bd.2.8.A1 Sichere Installation (B)

Das IT-System, auf dem Qubes OS betrieben werden soll, MUSS IOMMU-basierte Virtualisierung unterstützen. Diese MUSS im BIOS des IT-Systems zusammen mit den Standard-Virtualisierungs- (Intel VT-x) und AMD-Virtualisierungs- (AMD-V) Erweiterungen aktiviert werden.

Die digitale Signatur der heruntergeladenen ISO MUSS vor der Installation überprüft werden.

Auf dem Laufwerk, auf dem Qubes OS installiert ist, SOLLTE kein anderes Betriebssystem installiert sein.

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

Vor der Installation zusätzlicher Software in Dom0 MUSS eine gründliche Analyse der möglichen Folgen für die Sicherheit von Dom0 durchgeführt werden. Zusätzliche Software DARF NUR dann in Dom0 installiert werden, wenn dies unbedingt erforderlich ist und keine sichere Alternative dazu besteht.

SYS.bd.2.8.A4 Keine Ausführung von Anwendungen auf einer TemplateVM [Benutzer] (B)

In TemplateVMs DÜRFEN NUR Anwendungen ausgeführt werden, die benötigt werden, um Konfigurationsdateien zu ändern. TemplateVMs DÜRFEN NUR verwendet werden, um Software zu installieren oder zu aktualisieren. Alle Anwendungen MÜSSEN auf AppVMs ausgeführt werden.

SYS.bd.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 unter Nutzung der konfigurierten Proxy VM (in der Regel sys-firewall) aus erfolgen. Dazu SOLLTE das Update-Widget der TemplateVM verwendet werden. Alternativ kann für Fedora-basierte Linux-Systeme das Kommando dnf bzw. für Debian-basierte Systeme wie etwa ubuntu das Kommando apt-get verwendet werden, da diese Kommandos ebenfalls den Zugriff der Installation über die Proxy VM unterstützen.

SYS.bd.2.8.A6 Installation von Aktualisierungen und Patches (B)

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. Vor der Installation potentiell riskanter Patches SOLLTE zuerst die betroffene TemplateVM geklont werden und die Patches in diesem Klon installiert werden, um sie dort zu testen.

SYS.bd.2.8.A7 Firewall-Konfiguration (B)

Die Firewall-VMs für AppVMs MÜSSEN möglichst restriktiv konfiguriert werden. Die Adressen, zu denen eine AppVM Verbindungen herstellen kann, MÜSSEN soweit wie möglich eingeschränkt sein. Falls zusätzliche Regeln für eingehende Verbindungen definiert werden, MÜSSEN diese ebenfalls auf notwendige Fälle beschränkt werden. Für AppVMs, die keinen Netzwerkzugriff erhalten sollen, MUSS die Netzwerk-VM none zugeordnet werden.

SYS.bd.2.8.A19 Installation von Nicht-Standard-Software in TemplateVMs (B)

Während bei den in Qubes integrierten Templates die Aktualisierung und Installation von Software normalerweise über eine vorgeschaltete Proxy VM (in der Regel sys-firewall) erfolgt, so dass die TemplateVM selbst keinen Netzwerkzugriff benötigt, existiert Anwendungssoftware, wie z.B. der Zoom-Client oder der Google Chrome Browser, die nicht als Pakete in den Standard Repositories gängiger Software-Distributionen vorhanden sind, sondern als eigenständige Pakete vom Server des betreffenden Herstellers heruntergeladen und dann manuell installiert werden müssen. Derartige Software, die nicht über den Aktualisierungsserver verfügbar ist, wie auch z.B. spezielle Gerätetreiber, DARF NUR nach einer gründlichen Analyse der möglichen Folgen in einer TemplateVM installiert werden.

Die Installation derartiger Software MUSS so erfolgen, dass keine sensiblen TemplateVMs mit den Internet verbunden werden. Dazu bestehen die beiden folgenden Möglichkeiten:

- Die notwendigen Software-Pakete werden in eine AppVM heruntergeladen und zur Installation in die TemplateVM kopiert.
- Es wird eine, dann als weniger vertrauenswürdig betrachtete, Kopie der TemplateVM erzeugt, die dann nur für solche AppVMs verwendet wird, die die betreffende Anwendung benötigen. Sicherheitskritische Service VMs wie sys-net, sys-firewall und sys-usb DÜRFEN nicht auf einer solchen TemplateVM basieren.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.bd.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.bd.2.8.A9 Verwendung eines USB-Qube (S)

Wenn externe USB-Geräte an das Client-System angeschlossen werden sollen, SOLLTE ein USB-Qube installiert werden. Dies ist allerdings nur dann möglich, wenn das System nicht von einem USB-Laufwerk aus gestartet wird, da in diesem Fall die Verwendung eines USB-Qube zu einem nicht mehr verwendbaren System führt.

SYS.bd.2.8.A10 Beschränkung von Windows 10/11 AppVMs auf das lokale Netzwerk (S)

Die Firewall-Regeln für Windows 10 und 11 AppVMs SOLLTEN so restriktiv angegeben werden, dass der Zugriff auf das lokale Netz und ggf. selektierte, genau festgelegte Adressen beschränkt ist, damit unerwünschte Telemetrie-Datenverbindungen blockiert werden.

SYS.bd.2.8.A11 Verwendung von DisposableVMs [Benutzer] (S)

Von externen Quellen (z.B. als Mail-Anhänge aus unbekannten Quellen) erhaltene Dokumente in den gängigen Office- und Graphik-Formaten bergen ein hohes Risiko, mit Schadsoftware infiziert zu sein. Sie SOLLTEN daher nicht in VMs geöffnet werden, die wichtige Daten enthalten. Falls möglich, SOLLTEN sie ungeöffnet in eine VM übertragen werden, in der sie keinen Schaden anrichten können.

Alternativ SOLLTEN sie mit Hilfe der für DisposableVMs angebotenen Funktionen in andere Datenformate umgewandelt werden, ehe sie in eine produktive Umgebung übernommen werden. Dies kann durch Löschen von Makros in Office-Dokumenten mit Hilfe der Funktion Edit in DisposableVM oder durch ihre Umwandlung in PDF in einer DisposableVM erfolgen, Für PDF- und Bild-Dateien SOLLTEN die Funkionen Convert To Trusted PDF bzw. Convert To Trusted Img verwendet werden. Für Operationen, die keinen Netzzugang benötigen, SOLLTE die Verwendung von DisposableVMs auf Basis einer TemplateVM ohne Netzzugang in Betracht gezogen werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

Die Verwendung eines YubiKey SOLLTE in Betracht gezogen werden, um eine erhöhte Sicherheit bei der Anmeldung zu erreichen.

SYS.2.3.A13 Zwei-Faktor-Authentifizierung mit U2F Proxy (H)

Die U2F-Spezifikation („Universal 2nd Factor“) für eine Authentisierung über Hardware-Tokens 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. Die token-basierte Zwei-Faktor-Authentifizierung durch Installation des Qubes U2F-Proxy SOLLTE bei sensiblen Webzugriffen verwendet werden.

SYS.bd.2.8.A14 Konfiguration von Windows 10/11 TemplateVM und AppVM (H)

Windows 10 und 11 Clients SOLLTEN grundsätzlich als Kombination aus TemplateVM und davon abhängigen AppVMs und nicht als StandaloneVMs installiert werden, da nur so eine sichere Trennung zwischen System- und Benutzerdaten zu gewährleisten ist. Eine für die periodische Überprüfung der Lizenzaktivierung notwendige Verbindung zum offenen Internet SOLLTE deshalb nur für die TemplateVM, die keine Benutzerdaten enthält, erlaubt sein und zeitlich auf diese Lizenzaktivierung beschränkt bleiben. Diese Verbindung SOLLTE nach Möglichkeit durch die zugeordnete Firewall-VM auf den Update-Server des Herstellers beschränkt und nach der Lizenzprüfung/-aktualisierung sofort wieder getrennt werden. Verbindungen der AppVM in das offene Internet SOLLTEN blockiert werden, insbesondere wenn personenbezogene Daten verarbeitet werden, deren mögliche Übertragung durch die Telemetrie unzulässig ist.

SYS.bd.2.8.A15 Schutz gegen Evil Maid Angriffe (H)

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 (AEM) (oder anderen Boot-Schutzverfahren wie etwa Heads) in Erwägung gezogen werden, wenn die Hardware-Voraussetzungen erfüllt sind. Dadurch wird bei jedem Boot-Vorgang überprüft, ob es unerlaubte Änderungen an der Boot-Konfiguration des IT-Systems gab.

SYS.bd.2.8.A16 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. Bei Verwendung von GNU Privacy Guard SOLLTE Split GPG verwendet werden.

SYS.bd.2.8.A17 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.bd.2.8.A18 Verschlüsselte AppVMs (H)

Bei AppVMs, die sensible Informationen enthalten, SOLLTE das private Laufwerk verschlüsselt werden. Bei Windows-AppVMs SOLLTE dies mit BitLocker oder Tools wie VeraCrypt zur Verschlüsselung von Laufwerk D: geschehen. Bei Linux-basierten AppVMs SOLLTE 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., Eine Installation ohne Auslagerungsdatei SOLLTE in Betracht gezogen werden, um Situationen zu vermeiden, in denen sensible Daten dort verbleiben könnten.

SYS.bd.2.8.A20 Ausführung von Windows-Anwendungen in einer Linux-Umgebung (H)

Es ist möglich, einen relativ großen Teil existierender Windows-Anwendungen mit Hilfe der WINE-Schnittstelle in Linux-Systemen auszuführen. Um Angriffe über solche Anwendungen, insbesondere im Office-Bereich, zu erschweren oder abzuwehren, SOLLTE geprüft werden, ob die betreffenden Anwendungen statt unter Windows in einer Linux-basierten VM ausgeführt werden können. Dazu ist in der zugeordneten TemplateVM das Paket WINE zu installieren, während die Anwendung selbst in einer AppVM zu installieren ist. Sofern das Windows-Kommando zum Start dieser Anwendung Leerzeichen („Blanks“) enthält, sind ggf. weitere Schritte notwendig, um den Start dieser Anwendung über die Menüstruktur von Qubes zu ermöglichen.

SYS.bd.2.8.A21 Nutzung nicht unterstützter Betriebssysteme als TemplateVMs (H)

Es ist möglich, andere als die im Qubes-Umfeld unterstützten Betriebssysteme, wie z.B. Android, Q4OS oder ReactOS, zu installieren und diese mit eingeschränkter Integration in ihre Umgebung zu nutzen. Werden solche Systeme als TemplateVM installiert, so SOLLTEN sie als weniger vertrauenswürdig behandelt werden und insbesondere keine sicherheitskritischen Aktionen in ihnen und in eventuell zugeordneten AppVMs ausgeführt werden. Insbesondere ist zu beachten, dass für diese Systeme kein Dateiaustausch mit anderen VMs und keine durch Proxy geschützte Software-Aktualisierung und -Installation zur Verfügung steht und dass alle auf einem

derartigen Template basierenden AppVMs sich als DisposableVMs verhalten, also bei Herunterfahren alle während der betreffenden Sitzung gespeicherten Daten wieder verlieren.

4. Weiterführende Informationen

Weitere Informationen über Gefährdungen und Sicherheitsanforderungen und -maßnahmen für Baustein SYS.bd.2.8 *Clients unter Qubes OS* sind u.a. in den folgenden Publikationen zu finden, auf die zuletzt am 13.07.2022 zugegriffen wurde:

- Dokumentation der Installation, Konfiguration und Verwendung von Qubes OS
  https://www.Qubes-os.org/doc/,
- Installationsanleitung für Qubes OS
  https://www.Qubes-os.org/doc/installation-guide/
- Regeln zur Konfiguration der Netzübergänge zwischen VMs
  https://www.Qubes-os.org/doc/firewall/
- Installationsanweisungen für Windows Clients unter Qubes
  https://github.com/Qubes-Community/Contents/blob/master/docs/os/windows/windows.md
- Entwicklerdokumentation, Diskussion aktueller / zukünftiger Erweiterungen
  https://github.com/QubesOS/Qubes-issues/issues
  https://dev.qubes-os.org/en/latest/
- Google Benutzergruppe, Diskussion von Anwendungsproblemen
  https://groups.google.com/g/qubes-users
- Benutzerforum, Diskussion von Anwendungsproblemen und aktuellen Entwicklungen
  https://forum.qubes-os.org/