Häufig gestellte Fragen

In diesem Kapitel finden Sie Antworten auf häufig gestellte Fragen zu den Funktionen von Cisco Business Dashboard und potenziellen Problemen. Die Themen sind in die folgenden Kategorien unterteilt:

Allgemeine häufig gestellte Fragen

Q. Welche Sprachen werden von Cisco Business Dashboard unterstützt?

A. Cisco Business Dashboard ist in den folgenden Sprachen verfügbar:

- Chinesisch
- Englisch
- Französisch
- Deutsch
- Japanisch
- Spanisch

Häufig gestellte Fragen zur Netzwerkerkennung

Q. Welche Protokolle verwendet Cisco Business Dashboard für das Management meiner Geräte?

A. Cisco Business Dashboard verwendet zur Erkennung und für das Management des Netzwerks verschiedene Protokolle. Welche Protokolle für ein bestimmtes Gerät verwendet werden, hängt vom Gerätetyp ab.

Zu den verwendeten Protokollen gehören die folgenden:

- Multicast DNS und DNS Service Discovery (d. h. *Bonjour*, siehe *RFCs 6762 bzw. 6763*)

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (siehe *Spezifikation IEEE 802.1AB*)
- Simple Network Management Protocol (SNMP)
- RESTCONF (siehe *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Proprietäre APIs für Webdienste

Q. Wie erkennt Cisco Business Dashboard mein Netzwerk?

A. Cisco Business Dashboard Probe erstellt durch Abhören von CDP-, LLDP- und mDNS-Bekanntmachungen eine vorläufige Liste von Geräten im Netzwerk. Network Probe stellt dann über die unterstützten Protokolle eine Verbindung zu jedem einzelnen Gerät her und fragt weitere Informationen ab, z. B. die CDP- und LLDP-Tabellen für Nachbargeräte, MAC-Adresstabellen und Listen zugeordneter Geräte. Anhand dieser Angaben werden weitere Geräte im Netzwerk identifiziert, und der Prozess wird so oft wiederholt, bis alle Geräte erfasst wurden.

Q. Führt Cisco Business Dashboard Netzwerkscans durch?

A. Cisco Business Dashboard führt nicht aktiv Netzwerkscans durch. Die Network Probe-Software scannt das IP-Subnetz, mit dem sie direkt verbunden ist, jedoch keine anderen Adressbereiche. Der Scan erfolgt auf Basis des ARP-Protokolls. Zusätzlich prüft die Network Probe-Software bei jedem erkannten Gerät, ob ein Webserver und ein SNMP-Server auf den betreffenden Standardports konfiguriert sind.

Häufig gestellte Fragen zur Konfiguration

Q. Was passiert, wenn ein neues Gerät erfasst wird? Wird die Konfiguration geändert?

A. Neue Geräte werden zur Standard-Gerätegruppe hinzugefügt. Wurden der Standard-Gerätegruppe Konfigurationsprofile zugewiesen, wird diese Konfiguration für neu erfasste Geräte übernommen.

Q. Was passiert, wenn ich ein Gerät aus einer Gerätegruppe in eine andere verschiebe?

A. VLAN- oder WLAN-Konfigurationen für Profile, die auf die Original-Gerätegruppe angewendet und nicht für die neue Gerätegruppe übernommen wurden, werden entfernt. VLAN- oder WLAN-Konfigurationen für Profile, die auf die neue Gruppe angewendet werden, aber nicht zur Originalgruppe gehören, werden zum Gerät hinzugefügt. Die Systemkonfigurationseinstellungen werden von Profilen überschrieben, die für die neue Gruppe übernommen werden. Wenn Sie für eine neue Gruppe keine Systemkonfigurationsprofile festgelegt haben, wird die Systemkonfiguration des Geräts nicht geändert.

Häufig gestellte Fragen zu Sicherheitsmaßnahmen

Q. Welche Portbereiche und Protokolle werden für Cisco Business Dashboard benötigt?

A. In der folgenden Liste sind die von Cisco Business Dashboard verwendeten Protokolle und Ports aufgeführt:

Tabelle 1: Cisco Business Dashboard Protokolle und Ports

Port	Richtung	Protokolle	Einsatzbereiche
TCP 22	Inbound	SSH	Zugriff auf das Dashboard über die Kommandozeile SSH ist im von Cisco bereitgestellten VM-Image standardmäßig deaktiviert.
TCP 80	Inbound	HTTP	Web-Zugriff auf das Dashboard Weiterleitung auf sicheren Webserver (Port 443)
TCP 443	Inbound	HTTPS Multiplex-TCP	Sicherer Web-Zugriff auf das Dashboard Kommunikation zwischen Probe und Dashboard
UDP 1812	Eingehend	RADIUS	Gerätezugriff auf das Dashboard bei der Authentifizierung des Benutzerzugriffs.
TCP 50000–51000 (Systeme, die über den Microsoft Azure-Marktplatz bereitgestellt werden, verwenden TCP 50000–50049)	Inbound	HTTPS	Remotezugriff auf Geräte Dieser Bereich kann über die Seite System > Platform Settings (System > Plattformeinstellungen) gesteuert werden.
UDP 53	Outbound	DNS	Domain-Namenauflösung
UDP 123	Outbound	NTP	Zeitsynchronisation.
TCP 443	Outbound	HTTPS	Zugriff auf Cisco Webservices zum Abrufen von Informationen wie Softwareupdates, Support-Status und End-of-Life-Ankündigungen Zugriff auf die Update-Services für Betriebssysteme und Anwendungen.
UDP 5353	Outbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk zum Bekanntmachen des Dashboards.

Q. Welche Portbereiche und Protokolle werden für Cisco Business Dashboard benötigt?

A. In der folgenden Liste sind die von Cisco Business Dashboard Probe verwendeten Protokolle und Ports aufgeführt:

Tabelle 2: Cisco Business Dashboard Protokolle und Ports

Port	Richtung	Protokolle	Einsatzbereiche
TCP 22	Inbound	SSH	Befehlszeilenzugriff auf die Probe SSH ist im von Cisco bereitgestellten VM-Image standardmäßig deaktiviert.
TCP 80	Inbound	HTTP	Web-Zugriff auf die Probe Weiterleitung auf sicheren Webserver (Port 443)
TCP 443	Inbound	HTTPS	Sicherer Web-Zugriff auf die Probe
UDP 5353	Inbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk. Wird für die Geräteerkennung verwendet.
UDP 53	Outbound	DNS	Domain-Namenauflösung
UDP 123	Outbound	NTP	Zeitsynchronisation
TCP 80	Outbound	HTTP	Gerätemanagement ohne sichere Webservices
UDP 161	Outbound	SNMP	Management von Netzwerkgeräten
TCP 443	Outbound	HTTPS Multiplex-TCP	Gerätemanagement über sichere Webservices, Zugriff auf Cisco Webservices zum Abrufen von Informationen wie Softwareupdates, Support-Status und End-of-Life-Ankündigungen Zugriff auf die Update-Services für Betriebssysteme und Anwendungen. Kommunikation zwischen Probe und Dashboard
UDP 5353	Outbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk zum Bekanntmachen von Network Probe

Q. Mit welchen Cisco Servern kommuniziert Cisco Business Dashboard und warum?

A. In der folgenden Tabelle sind die Cisco Server aufgeführt, mit denen Cisco Business Dashboard kommuniziert, sowie der Zweck dieser Kommmunikation:

Tabelle 3: Cisco Business Dashboard - Cisco Server

Hostname	Zweck
tools.cisco.com	Wird von Smart Licensing verwendet, um zu überprüfen, ob genügend Lizenzen für das Dashboard in Ihrem Smart Account verfügbar sind. Dieser Server wird nur verwendet, wenn die Dashboard-Instanz bei Cisco Smart Licensing registriert ist.
api.cisco.com	Dient zum Abrufen von Informationen zu Softwareupdates und Produktlebenszyklen. Dieser Server wird nur verwendet, wenn die Berichterstellung zu Softwareupdates oder Lebenszyklen unter System > Privacy Settings (System > Datenschutzeinstellungen) aktiviert ist.
dl.cisco.com download-ssc.cisco.com	Wird verwendet, um Softwareupdatedateien von Cisco herunterzuladen. Diese Server werden nur verwendet, wenn Softwareupdates unter **System> Privacy Settings** (System > Datenschutzeinstellungen) aktiviert sind und Sie einen Upgradevorgang für ein Netzwerkgerät oder für Cisco Business Dashboard ausführen.
cloudsso.cisco.com	Wird zur Authentifizierung von Cisco Business Dashboard vor der Kommunikation mit api.cisco.com verwendet. Dieser Server wird nur verwendet, wenn die Berichterstellung zu Softwareupdates oder Lebenszyklen unter **System > Privacy Settings** (System > Datenschutzeinstellungen) aktiviert ist.
ciscoactiveadvisor.cisco.com	Wird verwendet, um Daten zur Produktverbesserung zu sammeln und die Funktion „Upload to CAA“ (In CAA hochladen) zu unterstützen. Dieser Server wird nur verwendet, wenn die Produktverbesserung unter **System > Privacy Settings** (System > Datenschutzeinstellungen) aktiviert ist oder wenn Sie die Funktion „Upload to CAA“ (In CAA hochladen) verwenden.
www.cisco.com	Wird verwendet, um Aktualisierungen der Signaturzertifikate der Stammzertifizierungsstelle abzurufen, die zur Verifizierung von X509-Zertifikaten verwendet werden, die von Cisco und Drittanbieterservices zur Sicherung der Netzwerkkommunikation verwendet werden.

Q. Welche Prozesse und Systemservices benötigt Cisco Business Dashboard?

A. In der folgenden Tabelle sind die von Cisco Servern verwendeten Prozesse und Systemservices aufgeführt, die Cisco Business Dashboard:

Tabelle 4: Cisco Business Dashboard - Prozesse und Systemservices

Prozessen	Weitere Details
Dashboard Essential Processes	
/usr/lib/jvm/java-8-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	Die wichtigste Dashboardanwendung
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	Webserver
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod /usr/lib/postgresql/xx/bin/postgres postgres: xx/main:	Datenbankservices
/bin/bash /usr/lib/ciscobusiness/dashboard/bin/freeradiussvc /usr/lib/ciscobusiness/dashboard/bin/freeradius	Benutzerauthentifizierungsservices
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	In-Memory-Cache-Services
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	Nachrichten-Broker
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	Multicast-DNS-Ankündigungen
/bin/sh /usr/share/contuit/contuit /bin/sh /usr/share/contuit-computations/contuit-computations /bin/sh /usr/share/contuit-monorepo/contuit-mop /bin/sh /usr/share/contuit-scheduler/contuit-scheduler /bin/sh /usr/share/contuit-shim/contuit-shim	Nur erforderlich, wenn die Integration mit externen Anwendungen aktiviert ist
Dashboard Essential System Services	
/usr/sbin/rsyslog	Protokollierungsservices
/usr/sbin/cron	Planungsservices
systemd-timesyncd	Zeitdienste

Prozessen	Weitere Details
Dashboard Essential Processes	
avahi-daemon	Multicast-DNS-Listener

Q. Welche Prozesse und Systemservices benötigt Cisco Business Dashboard Probe?

A. In der folgenden Tabelle sind die von Cisco Servern verwendeten Prozesse und Systemservices aufgeführt, die Probe Cisco Business Dashboard:

Tabelle 5: Cisco Business Dashboard - Prozesse und Systemservices

Prozessen	Weitere Details
Probe Essential Processes	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	Die wichtigste Probe-Anwendung
/usr/lib/ciscobusiness/probe/bin/fpscan	Gerätescanner-Tool
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	Multicast-DNS-Ankündigungen
nginx	Webserver Wenn sich Probe auf dem Dashboardserver befindet, wird der Dashboardwebserver genutzt
Probe Essential System Services	
/usr/sbin/rsyslogd	Protokollierungsservices
/usr/sbin/cron	Planungsservices
systemd-timesyncd	Zeitdienste
avahi-daemon	Multicast-DNS-Listener
lldpd	Erkennung von LLDP-Nachbarn

Q. Wie sicher ist die Kommunikation zwischen Cisco Business Dashboard und Probe?

A. Die gesamte Kommunikation zwischen dem Dashboard und Probe wird über eine TLS1.2-Sitzung mit authentifizierten Client- und Serverzertifikaten verschlüsselt. Die Sitzung wird von Probe initiiert. Wenn die Zuordnung zwischen dem Dashboard und Probe zum ersten Mal hergestellt wurde, muss sich der Benutzer beim Dashboard über Probe anmelden.

Q. Gibt es für Cisco Business Dashboard eine „Hintertür“ für den Zugriff auf meine Geräte?

A. Nein. Wenn Cisco Business Dashboard ein unterstütztes Cisco Gerät erkennt, werden für den Zugriff die werkseitigen Standard-Anmeldeinformationen für dieses Gerät verwendet. Benutzername und Kennwort lauten dann jeweils `cisco` und die SNMP-Community lautet `public`. Wurde die

Standard-Gerätekonfiguration geändert, muss der Benutzer die korrekten Anmeldeinformationen in Cisco Business Dashboard angeben.

Q. Sind die Anmeldeinformationen in Cisco Business Dashboard sicher gespeichert?

A. Die Anmeldeinformationen für den Zugriff auf Cisco Business Dashboard werden mit dem SHA512-Hash-Algorithmus verschlüsselt. Dieser Vorgang ist nicht umkehrbar. Die Anmeldeinformationen für Geräte und andere Services, wie **Cisco Active Advisor**, werden mit dem AES-128-Algorithmus verschlüsselt. Diese Verschlüsselung ist umkehrbar.

Q. Wie kann ich ein verloren gegangenes Kennwort für die Webbenutzeroberfläche wiederherstellen?

A. Wenn Sie das Kennwort für alle Administratorkonten in der Web-Benutzeroberfläche verloren haben, können Sie es wiederherstellen, indem Sie sich bei der Konsole der Probe-Instanz anmelden und das Tool **cbdprobe recoverpassword** ausführen. Alternativ können Sie sich bei der Konsole der Dashboard-Instanz anmelden und das Tool **cisco-business-dashboard recoverpassword** ausführen. Mit diesem Tool können Sie das Kennwort für das Benutzerkonto „cisco“ auf das Standardkennwort „cisco“ zurücksetzen. Wurde das Benutzerkonto „cisco“ entfernt, können Sie das Konto mit dem Standardkennwort wiederherstellen. Nachfolgend finden Sie ein Beispiel der Befehle, mit denen Sie in diesem Tool das Kennwort wiederherstellen können.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

Hinweis Wenn Sie Cisco Business Dashboard für AWS verwenden, ist das Kennwort die AWS-Instanz-ID.

Q. Wie lauten der Standardbenutzername und das Kennwort für den Bootloader der virtuellen Maschine?

A. Die Standard-Anmeldeinformationen für den Bootloader der virtuellen Maschine sind: Benutzername: **root**, Kennwort: **cisco**. Diese können mit dem config_vm-Tool geändert werden. Wenn Sie gefragt werden, ob Sie das Bootloader-Passwort ändern möchten, antworten Sie mit „Ja“.

Q. Wie authentifiziert das Dashboard Netzwerkzugriffsgeräte?

A. Das Dashboard verwendet zwei Authentifizierungsebenen.

- Zunächst wird die Quell-IP-Adresse der eingehenden Anfrage mit den externen IP-Adressen der vom Dashboard gemanagten Netzwerke verglichen, wenn NAT verwendet wird, bzw. mit den internen Subnetzen der Netzwerke, wenn kein NAT verwendet wird.
- Danach wird nach dem Zufallsprinzip ein eindeutiger geheimer RADIUS-Schlüssel für jede Organisation erstellt, der vom Netzwerkzugriffsgerät in seiner Anfrage verwendet werden muss.

Häufig gestellte Fragen zum Remote-Zugriff

Q. Verwende ich eine sichere Sitzung, wenn ich mich über Cisco Business Dashboard mit der Verwaltungsoberfläche eines Geräts verbinde?

A. Cisco Business Dashboard stellt die Remotesitzung zwischen dem Gerät und dem Benutzer per Tunneling bereit. Das zwischen Probe und dem Gerät verwendete Protokoll hängt von der Konfiguration des

Endgeräts ab, aber Cisco Business Dashboard wählt immer ein sicheres Protokoll für die Sitzung, sofern verfügbar (z. B. wird HTTPS gegenüber HTTP bevorzugt). Verbindet sich der Benutzer über das Dashboard mit dem Gerät, wird die Sitzung über einen verschlüsselten Tunnel zwischen dem Dashboard und Probe abgewickelt, unabhängig von den auf dem Gerät aktivierten Protokollen. Für die Verbindung zwischen dem Webbrowser des Benutzers und dem Dashboard wird immer HTTPS genutzt.

Q. Warum wird meine Remotesitzung zu einem Gerät immer sofort unterbrochen, wenn ich eine Remotesitzung auf einem anderen Gerät starte?

A. Wenn Sie mit Cisco Business Dashboard auf ein Gerät zugreifen, registriert der Browser jede Verbindung als Kommunikation mit einem Webserver (Dashboard) und sendet Cookies von einem Gerät zum anderen. Wenn mehrere Geräte denselben Cookienamen verwenden, wird eventuell das Cookie eines Geräts von einem anderen Gerät überschrieben. Dies tritt häufig bei Sitzungscookies auf. Aus diesem Grund ist ein Cookie immer nur für das zuletzt verwendete Gerät gültig. Alle anderen Geräte, die denselben Cookienamen verwenden, identifizieren das Cookie als ungültig und beenden die Sitzung.

Q. Warum tritt bei meiner Remotesitzung der folgende Fehler auf? **Access Error: Request Entity Too Large HTTP Header Field exceeds Supported Size** (Zugriffsfehler: Anforderungsentität zu groß – HTTP-Header-Feld übersteigt die unterstützte Größe.)

A. Nach zahlreichen Remotesitzungen zu unterschiedlichen Geräten sind im Browser viele Cookies für die Dashboard-Domain gespeichert. Um dieses Problem zu umgehen, löschen Sie mithilfe der Browserfunktionen die Cookies für diese Domain, und laden Sie dann die Seite erneut.

Häufig gestellte Fragen zu Softwareupdates

Q. Wie sorge ich dafür, dass das Betriebssystem des Dashboards auf dem neuesten Stand ist?

A. Das Dashboard verwendet die Ubuntu Linux-Verteilung für ein Betriebssystem Die Pakete und der Kernel lassen sich mit den Ubuntu-Standardprozessen aktualisieren. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle `sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System darf nicht auf eine neue Ubuntu-Version aktualisiert werden. Wir raten davon ab, zusätzliche Pakete zu installieren. Verwenden Sie nur die Pakete, die im von Cisco bereitgestellten VM-Image enthalten sind, oder die Pakete, die im Rahmen einer Minimalinstallation von Ubuntu installiert werden.

Q. Wie aktualisiere ich Java auf dem Dashboard?

A. Cisco Business Dashboard verwendet die OpenJDK-Pakete aus den Ubuntu-Repositorys. OpenJDK wird automatisch aktualisiert, wenn das Kernbetriebssystem aktualisiert wird.

Q. Wie sorge ich dafür, dass das Betriebssystem von Network Probe auf dem neuesten Stand ist?

A. Cisco Business Dashboard verwendet die Ubuntu Linux-Verteilung für ein Betriebssystem Die Pakete und der Kernel lassen sich mit den Ubuntu-Standardprozessen aktualisieren. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle `sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System darf nicht auf eine neue Ubuntu-Version aktualisiert werden. Wir raten davon ab, zusätzliche Pakete zu installieren. Verwenden Sie nur die Pakete, die im von Cisco bereitgestellten VM-Image enthalten sind, oder die Pakete, die im Rahmen einer Minimalinstallation von Ubuntu installiert werden.

Q. Wie sorge ich dafür, dass das Betriebssystem von Network Probe auf dem neuesten Stand bleibt, wenn ich einen Raspberry Pi nutze?

A. Die Raspbian-Pakete und der Kernel können mit den Standardprozessen aktualisiert werden, die für Debian-basierte Linux-Distributionen verwendet werden. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle

`sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System sollte nicht auf eine neue Raspbian-Hauptversion aktualisiert werden. Es wird empfohlen, keine Pakete außer den zur „Lite“-Version der Raspbian-Distribution gehörenden und den vom Probe-Installationsprogramm hinzugefügten Pakete zu installieren.

Q. Cisco Business Dashboard 2.3.0 unterstützt nun Ubuntu 20.04 (Focal Fossa). Wenn ich mein System auf 2.3.0 aktualisiert habe, kann ich dann das Betriebssystem von Ubuntu 16.04 auf Ubuntu 20.04 aktualisieren?

A. Leider sind die Änderungen zwischen den beiden Betriebssystemversionen zu groß, um ein direktes Upgrade zu ermöglichen. Wenn auf einem vorhandenen System Ubuntu 16.04 ausgeführt wird, sollten Sie das Dashboard auf Version 2.3.0 aktualisieren und dann ein Backup des Dashboards über die Seite **System** > **Backup**(Systemsicherung) erstellen. Sie können dann entweder Ihr Dashboard mit Ubuntu 20.04 neu aufbauen oder eine neue Dashboardinstallation basierend auf Ubuntu 20.04 erstellen. Anschließend können Sie das Backup von dem alten Dashboard im neuen Dashboard wiederherstellen.

Q. Cisco Business Dashboard 2.3.0 unterstützt nun Ubuntu 20.04 (Focal Fossa). Wenn ich mein System auf 2.3.0 aktualisiert habe, kann ich dann das Betriebssystem von Ubuntu 16.04 auf Ubuntu 20.04 aktualisieren?

A. Leider sind die Änderungen zwischen den beiden Betriebssystemversionen zu groß, um ein direktes Upgrade zu ermöglichen. Wenn auf einem vorhandenen System Ubuntu 16.04 ausgeführt wird, sollten Sie das Dashboard auf Version 2.3.0 aktualisieren und dann ein Backup des Dashboards über die Seite **System** > **Backup**(Systemsicherung) erstellen. Sie können dann entweder Ihr Dashboard mit Ubuntu 20.04 neu aufbauen oder eine neue Dashboardinstallation basierend auf Ubuntu 20.04 erstellen. Anschließend können Sie das Backup von dem alten Dashboard im neuen Dashboard wiederherstellen.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.