Die Technologie hinter unserem cloud-basierten Portfolio

Finden Sie heraus, wie Priva Ihre Daten schützt

Whitepaper

priva.com

Einleitung

Priva ist bestrebt, Produkte und Dienstleistungen zu entwickeln, mit denen unsere Kunden ihr Business ausbauen können. Wir verwenden eine Vielzahl von Technologien, um diese Produkte und Dienstleistungen so leistungsstark wie möglich zu machen und dennoch eine einfache Bedienung zu gewährleisten. Die Cloud ist eine Schlüsseltechnologie, die auf jedem Gerät großartige Benutzererlebnisse ermöglicht, unabhängig von Ort und Zeitpunkt.

Unsere Technologie steuert Funktionen, die für das Kerngeschäft derjenigen, die sie nutzen, von hohem Stellenwert sind. Die Sicherheit dieser Produkte und Dienstleistungen – und der darin enthaltenen Daten – ist von entscheidender Bedeutung. In diesem Dokument wird die Technologie hinter unserem cloud-basierten Portfolio vorgestellt und die Schritte erläutert, die wir zum Schutz Ihrer Daten unternommen haben.

Index

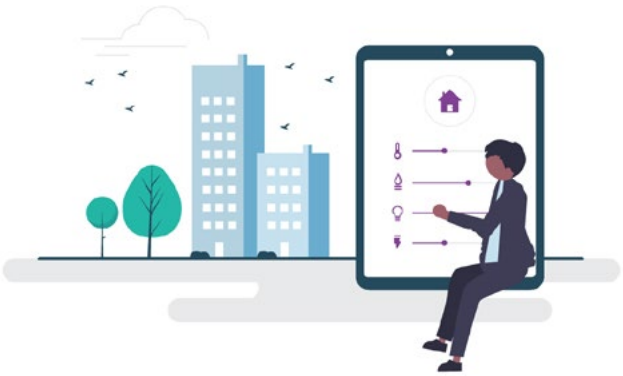
>

1.1 Warum die Cloud?

Das Konzept der Cloud ist simpel: Anstatt riesige IT-Infrastrukturen zu kaufen und zu warten, können Unternehmen die Cloud nutzen, um Datenspeicherung, -kommunikation und -verarbeitung auszulagern.

Für Gebäudeeigentümer oder Facility Manager ist der Fernzugriff auf Installations-, Komfort- und Energiedaten über die Cloud von besonderem Interesse, da er zur allgemeinen Optimierung und zu einem besseren Komfort der Nutzer*innen beiträgt. In der Lage zu sein, Ihr Gebäude jederzeit, überall und auf jedem Gerät zu verwalten, ist ein Hauptkriterium, um einen guten Komfort in diesem Gebäude zu erreichen.

Die Cloud bietet Big-Data-Intelligenz, mit der Sie große Datenmengen verarbeiten, analysieren und speichern können. Auf diese Art werden Probleme schnell und effizient erkannt und behoben. Diese Effizienz führt zu einem höheren Komfort im Gebäude und einer allgemeinen Leistungssteigerung: Wir nennen dies ein Wachstumsklima.



>

1.2 Was sind die Vorteile?

Die Cloud ist ein leistungsstarkes und benutzerfreundliches Tool, um Benutzer bei ihren Prozessen zu unterstützen. Wir von Priva verwenden eine Vielzahl von Technologien, um unsere Produkte und Dienstleistungen so leistungsstark wie möglich zu machen und dennoch eine einfache Bedienung zu gewährleisten.

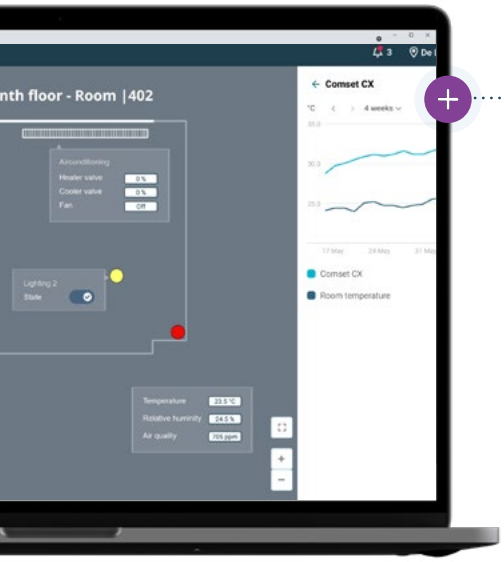
Die Cloud ist eine Schlüsseltechnologie, die auf jedem Gerät großartige Benutzererlebnisse ermöglicht, unabhängig von Ort und Zeitpunkt. Daraus ergeben sich folgende Vorteile:

1. **Verbindung und Zugriff jederzeit, überall und von jedem Gerät aus**
2. **Höherer Komfort für Nutzer*innen**
3. **Aktivierung Alarmhandhabung**
4. **Unterstützung proaktiver Wartung**
5. **Kontinuierliche Verbesserung**

Gebäudemanagement und -optimierung ist kein theoretischer Prozess. Es erfordert die Zusammenarbeit mit den Gebäudenutzern und die direkte Behebung von Problemen. Mit der cloud-verbundenen Software können Sie Gebäudedaten überwachen, Anpassungen vornehmen, die Leistung analysieren und Warnungen verwalten.
Das ermöglicht Ihnen, sich auf Ihre Aufgaben zu konzentrieren – und Probleme schnell und effizient zu lösen.

Heute ist alles miteinander verbunden. Das wirft auch Fragen und Sorgen bezüglich der Datensicherheit auf. Mit der Cloud können Sicherheitsupdates zentralisiert und optimiert werden. Dies minimiert das Risiko von Problemen durch veraltete Softwarelösungen.

Bei diesen Updates geht es jedoch um mehr als nur um Sicherheit. Die Technologie verbessert sich schneller als je zuvor. Wenn Sie ein BMS implementieren, möchten Sie nicht, dass es im folgenden Jahr veraltet ist. Daher ist es notwendig, Kompatibilität zwischen Technologien zu schaffen.



Durch die Nutzung der Cloud zur Entkopplung des Steuerungssystems von den Anwendungen kann jede neue Technologie in die Cloud-Umgebung integriert werden, ohne das lokale Steuerungssystem zu ändern. So lassen sich neue Technologien problemlos in Ihr BMS integrieren.

Wo früher die Steuerungsmöglichkeiten eines Gebäudes von der Entwurfsphase bis zur Renovierung oder zum Wiederaufbau unveränderbar festgelegt waren, bleiben sie heute jederzeit und flexibel auf dem neuesten Stand.

Daten sind wie jede andere Ressource nur dann wertvoll, wenn sie präzisiert und am richtigen Ort einfach zugänglich sind. Mit der Cloud können Sie Daten in einem einfachen Diagramm durchsuchen oder komplexe Analysen durchführen - ohne die enorme Menge an Rechenleistung und Komplexität zu bemerken, die erforderlich ist, um mehr Daten zu verarbeiten, als Ihr lokales Gerät verarbeiten kann.

>

1.3 Zusammenfassend

Die Nutzung der Cloud stellt sicher, dass Gebäude wertvoller werden, indem Sie und Ihre Prozesse besser unterstützt und das volle Potenzial Ihrer Daten ausgeschöpft werden. Gleichzeitig ist das System einfacher zu bedienen, sicherer, flexibler und zukunftssicher.

>

2. Cloud-Sicherheit

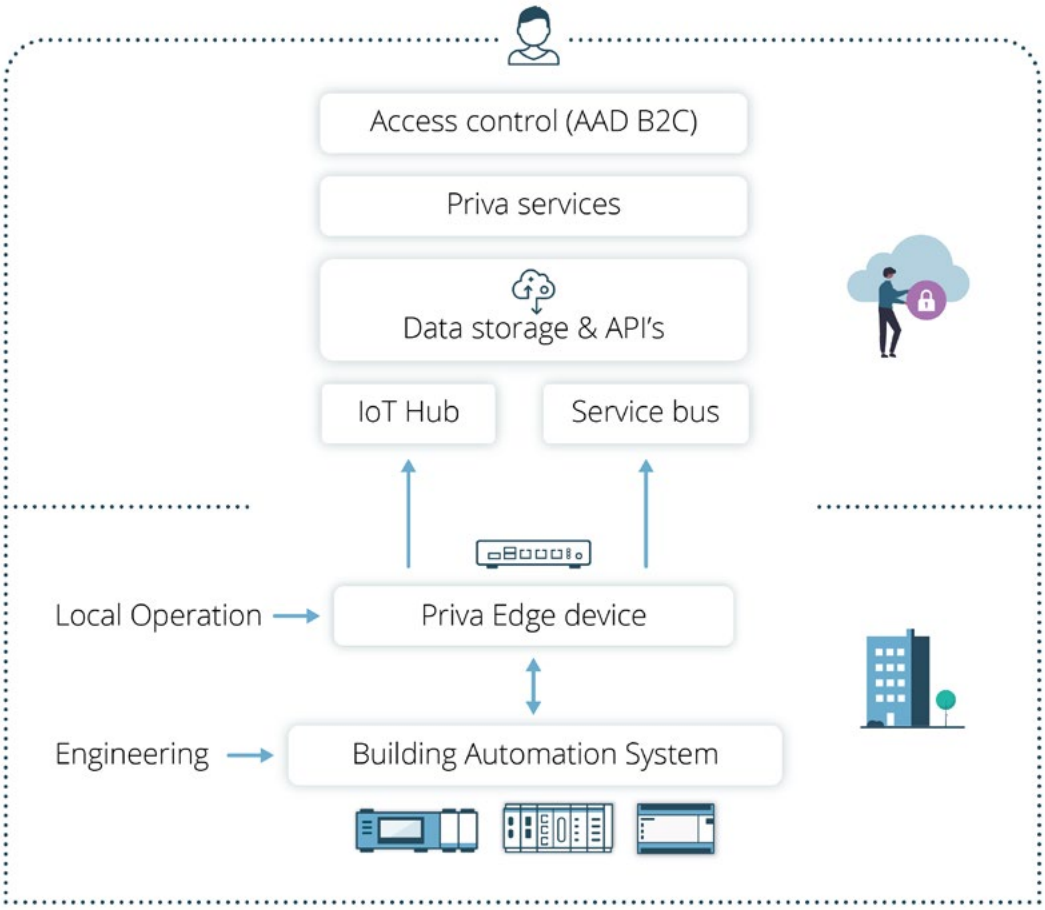
Die Entwicklung sicherer Cloud Services ist ein herausfordernder Prozess, der erhebliches Fachwissen und eine sichere und stabile Cloud-Plattform erfordert. Wir nutzen die Microsoft Azure Cloud-Plattform als zuverlässige Grundlage für alle unsere Cloud Services. Microsoft Azure ist eine Cloud-Plattform, die ein hohes Maß an Sicherheit bietet, wie die über 90 Compliance-Zertifizierungen bestätigen. Diese Zertifizierungen sind auf der Compliance-Dokumentationswebsite von Azure aufgeführt. Detaillierte Informationen zu den Sicherheitsmaßnahmen von Microsoft finden Sie im Microsoft Trust Center.

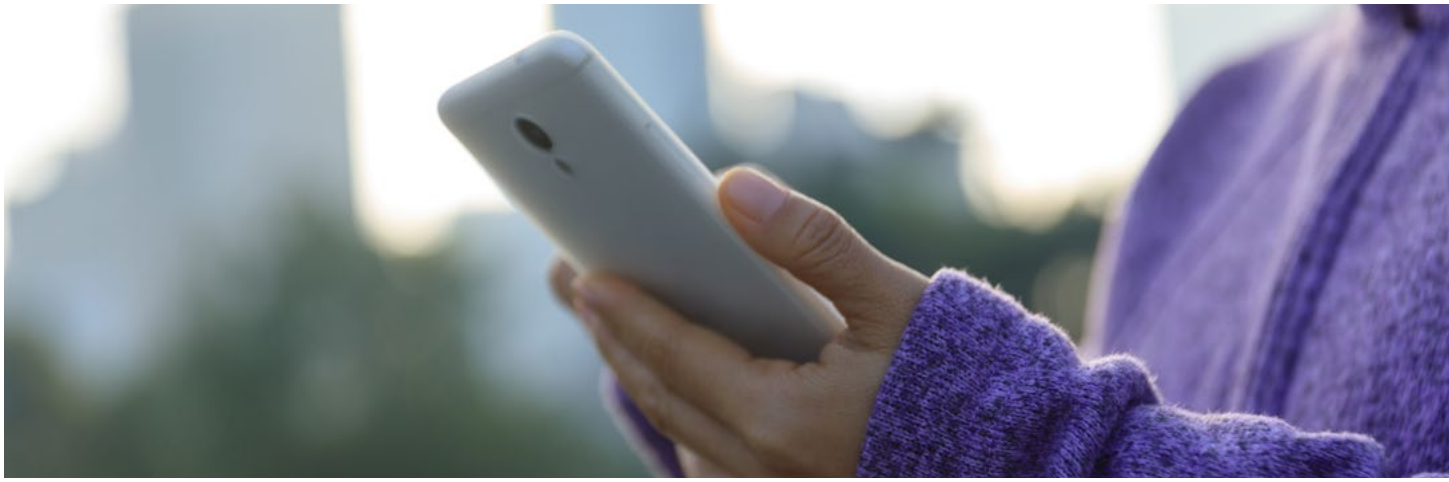
Zusätzlich zu Microsoft Azure haben wir unsere Priva Digital Services entwickelt. Microsoft Azure bietet uns sichere Rechenzentren, eine sichere physische Infrastruktur und Standardkomponenten. Dies bedeutet, dass sich Priva auf sicheres Softwaredesign, sichere Codierung und sichere Konfiguration unserer digitalen Dienstleistungen konzentrieren kann. Bei der Entwicklung und Nutzung dieser Dienstleistungen wenden wir bekannte Sicherheitsprinzipien wie „Security by Design“ und „Defense in Depth“ an.

Unsere Architekten und Sicherheitsspezialisten arbeiten eng mit den Entwicklungsteams zusammen, so dass Informationssicherheit ein integraler Bestandteil des Entwicklungsprozesses ist. Während der Entwicklung testen wir kontinuierlich, ob unsere Produkte und Dienstleistungen das erforderliche Sicherheitsniveau erfüllen. Dies geschieht mithilfe von Risikobewertungen, automatisierten Tests und manuellen Codeüberprüfungen in Übereinstimmung mit unserer Softwareentwicklungsrichtlinie und anderen Informationssicherheitsrichtlinien.

Um sicherzustellen, dass Priva (Cloud) Services sicher sind, stellt Priva auch unabhängige ethische Hacker ein, um regelmäßige Penetrationstests durchzuführen. Die Ergebnisse werden untersucht und ausgewertet, damit sich das Sicherheitsniveau kontinuierlich erhöht. Wenn ein Dienstleistungs- oder Hardwaregerät angemessen geschützt ist, stellen die ethischen Hacker ein TPM (Third Party Memorandum) zur Verfügung, um ihre Erkenntnisse über das Sicherheitsniveau formell zu bestätigen. Des Weiteren ist Priva zertifiziert nach ISO9001 und ISO27001.

Privas Dienstleistungs-Architektur





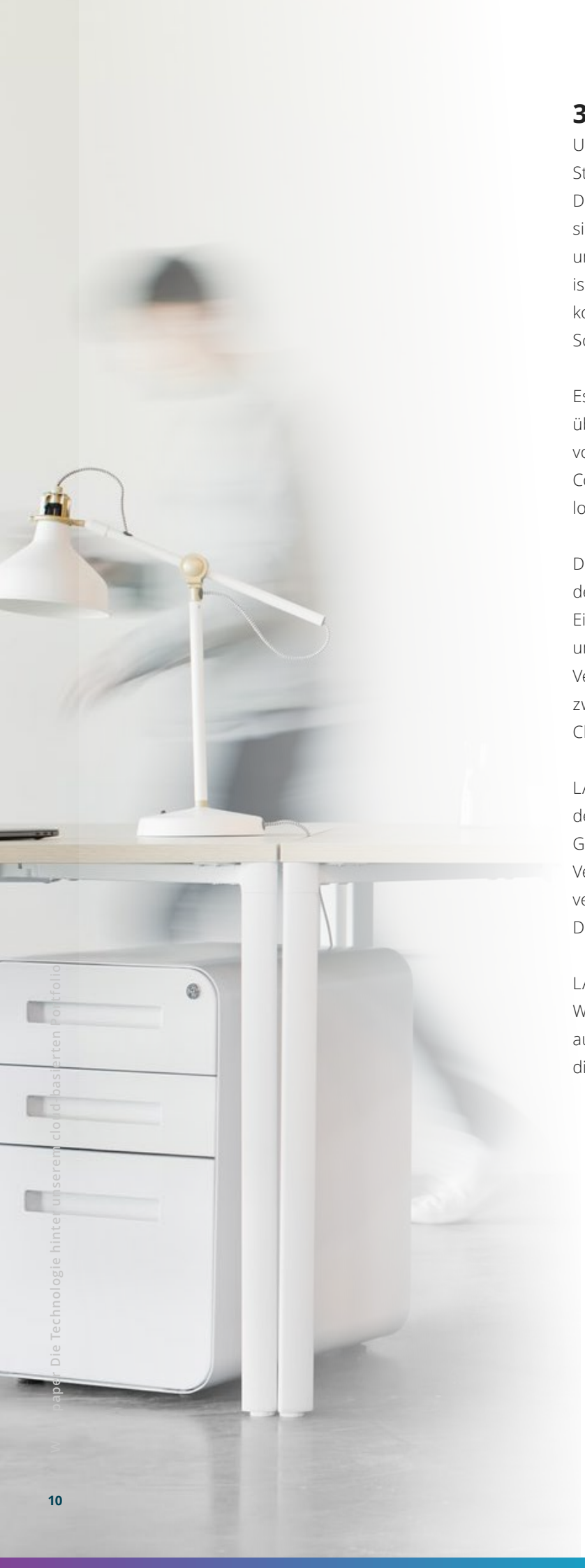
3. Ein detaillierter Blick auf die Sicherheit der Priva Services

Priva Services – und die Infrastruktur dahinter – können in mehrere Sicherheitsebenen unterteilt werden. Es beginnt beim Steuerungssystem. Das **Steuerungssystem** verbindet sich über das **Priva Edge Gateway** mit der Cloud. In der Cloud werden die Daten gespeichert und die Dienstleistungen gehostet. Hier haben Benutzer Zugang zu ihren Dienstleistungen. Im Folgenden wird die Sicherheit der einzelnen Komponenten behandelt.

3.1 Das Steuerungssystem

Das Steuerungssystem besteht aus dem Controller-Netzwerk, das die Klimainstallation steuert. Im Allgemeinen haben Gebäudeautomationssteuerungen und ähnliche Geräte eine begrenzte Sicherheit. Der Netzwerkverkehr zwischen den Komponenten des Steuerungssystems ist ebenfalls unverschlüsselt. Es wird erwartet, dass Gebäudeautomationsgeräte mehr als ein Jahrzehnt lang rund um die Uhr funktionieren und sind als solche während ihrer gesamten Lebensdauer unglaublich schwer auf dem neuesten Stand und sicher zu halten.

Gebäudeautomationssysteme sollten immer ein dediziertes technisches Netzwerk verwenden, das Sicherheit bietet und das Gebäudeautomationssystem vor allen Zugangsmöglichkeiten von außen schützt. Gebäudeautomationssysteme sollten niemals in Netzwerken mit Internetzugang betrieben werden.



3.2 Das Priva Edge Gateway

Um Cloud Services zu nutzen, muss das Steuerungssystem mit dem Internet verbunden sein. Daher verwenden wir das Priva Edge Gateway, um eine sichere Schnittstelle zwischen dem Steuerungssystem und dem Internet zu generieren. Das Priva Edge Gateway ist ein geschlossenes System, das nur für Priva Services konfiguriert und genutzt werden kann. Non-Priva-Software ist nicht kompatibel.

Es verwendet drei separate Netzwerkkarten, die nicht überbrückt werden können, um das Internet physisch von dem technischen Netzwerk zu trennen, das unsere Controller verwenden. Dadurch bleiben die Controller logisch vom Internet getrennt.

Die erste Netzwerkkarte, LAN1, ist für die Verbindung mit der Außenwelt bestimmt. Zum Schutz vor potenziellen Eindringlingen verwendet es ausgehende Verbindungen und nur die minimal notwendigen eingehenden Verbindungen (siehe Tabelle unten). Jede Kommunikation zwischen dem Gebäudemanagementsystem und der Cloud wird immer vom Priva Edge Gateway initiiert.

LAN2 dient dazu, das Priva Edge Gateway mit dem Netzwerk zu verbinden, auf dem sich das Gebäudeautomationssystem befindet. Um eine Verbindung mit den anderen Geräten herzustellen, verfügt LAN2 über Ports, die für eingehenden Datenverkehr geöffnet sind.

LAN3 ist für den Service. Über LAN3 kann auf die lokale Web-Benutzeroberfläche zugegriffen werden, über die auf Geräte- und Netzwerkeinstellungen zugegriffen und diese geändert werden können.

	Akzeptiert eingehenden Datenverkehr	UDP Port	TCP Port	Zweck
LAN 1 /LAN 2/ LAN 3	Ja	68		DHCP (Client)
LAN 3	Ja		80	Lokale Web-Benutzer-oberfläche
LAN 2	Ja	123		NTP
LAN 2	Ja	514		Rsyslog
LAN 2	Ja		1883	MQTT
LAN 2	Ja	1900		SSDP
LAN 2	Ja		5000/ 5001/ 5002/ 5003/ 5004	Funktionen des lokalen Gebäudebetreibers oder des lokalen Reservesystems des Gebäudebetreibers
LAN 2	Ja	5353		mDNS
LAN 2	Ja	7650/ 7651/ 7660/ 7661		DDS
LAN 2	Ja	9508		PTP
LAN 2	Ja	15000/15001		Comprinet

Wir verwenden Standardkomponenten von Microsoft, um zwischen dem Gebäude und der Cloud zu kommunizieren. Insbesondere für unsere Dienstleistungen nutzen wir den IoT Hub und Service Bus von Microsoft Azure. Der Netzwerkverkehr zwischen dem Priva Edge Gateway und der Cloud wird verschlüsselt. Im Gegensatz zu einigen anderen Methoden des Zugriffs auf Gebäudewartungssysteme wie VPN, verwendet diese Architektur ein nachrichtenbasiertes System, so dass es keine vollständige Datenverbindung zwischen dem Gebäude und der Außenwelt gibt. Es werden nur sehr begrenzte relevante Daten ausgetauscht.

Der Netzwerkverkehr zwischen dem Priva Edge Gateway und der Cloud wird verschlüsselt.

Das Konzept der Cloud ist einfach. Unternehmen können die Cloud nutzen, um Datenspeicherung, -kommunikation und -verarbeitung auszulagern...

3.3 Sicherheit der Cloud

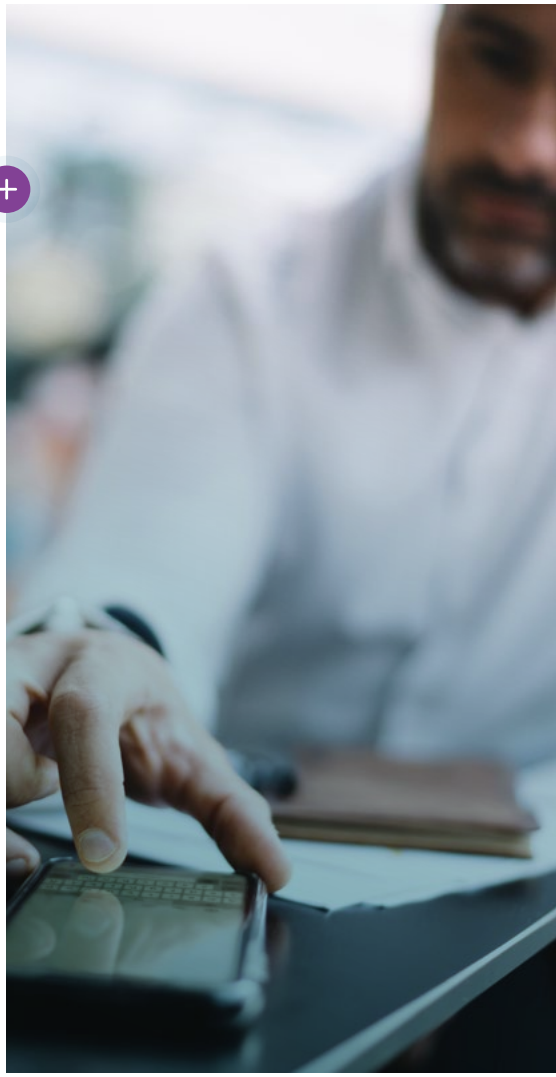
Der primäre Schutz gegen unbefugten Benutzerzugriff auf unsere Cloud Services ist eine Authentifizierungsschicht, die auf dem OAuth2-Protokoll basiert. Wir verwenden Azure Active Directory B2C (AAD B2C) als Identitätsanbieter und eine Identitätsserver-Implementierung, welche die Autorisierungsregeln für diese Identitäten bereitstellt. Wir stellen sicher, dass die Kommunikation mit allen unseren Diensten über HTTPS (TLS v1.2 oder höher) erfolgt.

Nachdem sich ein Benutzer mit AAD B2C authentifiziert hat, werden seine Berechtigungen in einem JSON-Webtoken codiert und mit einem privaten Schlüssel signiert. Wann immer eine unserer Anwendungen auf Ihre Daten zugreifen möchte, muss sie das Token dem Service präsentieren, der sie speichert. Der Service überprüft dann, ob das Token nicht manipuliert wurde, indem er einen öffentlichen Schlüssel verwendet, und ob der Benutzer über die Berechtigung zum Zugriff auf die angeforderte Ressource verfügt.

Benutzer von Priva Services sind mit der Zugriffskontrolle vertraut, mit der Administratoren einer Organisation steuern können, welche Konten Zugriff auf welche Funktionen und Gebäude haben. Am Point of Sale erteilen wir dem Käufer des Dienstes Zugriffsrechte, sodass er andere einladen und ihre Rechte kontrollieren kann.

Standardmäßig ist MFA (Multi-Factor Authentication) für neue Benutzer aktiviert, was die Sicherheit während des Anmeldevorgangs erhöht. Zusätzlich zum Kennwort des Benutzers verwendet MFA einen zweiten Authentifizierungsfaktor wie eine Textnachricht mit einem einmaligen Code, um Zugriff auf die Cloud-Dienstleistungen zu erhalten.

Darüber hinaus unterstützen unsere Dienstleistungen auch die Nutzung des Kunden-AAD, die dem Kunden eine umfassendere Kontrolle über die Sicherheitsrichtlinien ermöglichen.



3.4 Gesicherte Kommunikation

Die Digital Services von Priva bieten gegenüber herkömmlichen Verbindungsmethoden mehrere große Sicherheitsvorteile. Mit den Digital Services von Priva gibt es keinen sicherheitsgefährdeten Tunnel, der viele wichtige Funktionen verbindet, etwa über Gebäude oder außerhalb Ihrer eigenen Kontrolle. Priva Services verwenden ein nachrichtenbasiertes System. Außerdem ist keine schwierige Einrichtung oder Konfiguration erforderlich, was die Fehlerquote und potenzielle Schwachstellen reduziert. Das Erteilen oder Widerrufen des Zugangs mit der Zugangskontrolle über mehrere Gebäude zugleich ist so viel einfacher: keine doppelten Logins, mehrfache Passwörter oder mehrere Personen auf einem einzigen Konto (aus Sicherheitsgründen).

3.5 Welche Endpunkte verwenden Priva services?

Um sich mit den Dienstleistungen in der Cloud zu verbinden, verwendet unser Priva Edge Gateway vollqualifizierte Domänennamen (Fully Qualified Domain Names, FQDNs). Die vollständige Übersicht der einzelnen FQDNs finden Sie in der Dokumentation. Nachfolgend ein Auszug aus FQDNs mit Platzhaltern::

***.servicebus.windows.net**
***.azure-devices.net**
***.azurewebsites.net**
***.blob.core.windows.net**
***.priva.com**

3.6 Wem gehören die Daten?

Unser Grundprinzip besteht darin, dass die Daten dem Eigentümer des Systems gehören, das sie generiert. Wir behalten uns jedoch das Recht vor, diese Daten nach einer Anonymisierung für Entwicklungszwecke zu verwenden. Die vollständige Richtlinie von Priva in Bezug auf die Verwendung von Daten ist in unseren allgemeinen und servicespezifischen Geschäftsbedingungen und unserer Datenschutzrichtlinie beschrieben.

3.7 Wo werden Ihre Daten gespeichert?

Alle unsere Cloud Services werden in der Region Westeuropa von Microsoft Azure gehostet. Die Rechenzentren in dieser Region befinden sich derzeit physisch in/in der Nähe von Amsterdam, Niederlande. Für die Notfallwiederherstellung werden diese Microsoft-Rechenzentren jedoch mit denen in der Azure-Region Nordeuropa zusammengeführt, die sich physisch in/in der Nähe von Dublin, Irland, befinden. In Notsituationen können Ihre Daten zwischen diesen beiden Rechenzentrumsstandorten übertragen werden. Für diese Datenübertragungen wird stets die private Kommunikationsinfrastruktur von Microsoft genutzt.

PRIVA 01-2023

Kontaktieren Sie uns

Wir freuen uns auf Sie!

Priva Building Intelligence GmbH
Tackweg 35
47918 Tönisvorst
Deutschland

T +49 2151 650 590
E info.de@priva.com

priva.com

#creatingaclimateforgrowth