De technologie achter ons cloud-gebaseerde portfolio

Ontdek hoe Priva uw gegevens beveiligt

Whitepaper

priva.com

Introductie

Bij Priva willen we producten en diensten ontwikkelen waarmee onze klanten hun bedrijf kunnen laten groeien. We gebruiken verschillende technologieën om onze producten en diensten zo krachtig mogelijk te maken en toch gebruiksvriendelijk te houden. De cloud speelt hierbij een centrale rol: dankzij deze technologie zijn geweldige gebruikerservaringen altijd, overal, en op elk apparaat mogelijk.

Onze technologie regelt functies die essentieel zijn voor de kernactiviteiten van de mensen die ze gebruiken. De beveiliging van deze producten en diensten, inclusief de gegevens die zij bevatten, is van cruciaal belang. In dit document maakt u kennis met de technologie achter ons cloud-gebaseerde portfolio en leggen wij uit welke stappen wij hebben ondernomen om de veiligheid van uw gegevens te waarborgen.

Inhoud

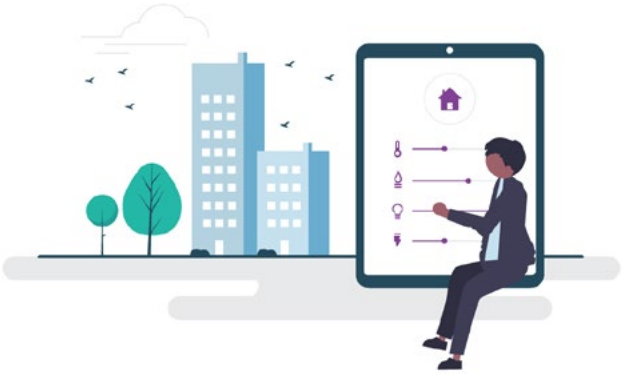
>

1.1 Waarom de cloud?

Het concept van de cloud is eenvoudig: in plaats van enorme IT-infrastructuren aan te schaffen en te onderhouden, kunnen bedrijven de cloud gebruiken voor de opslag, overdracht en verwerking van gegevens.

Voor eigenaren of beheerders van gebouwen is de toegang op afstand tot installatie-, comfort- en energiegegevens via de cloud bijzonder interessant. Het helpt namelijk om alles in het gebouw te optimaliseren en daarmee het comfort voor de bewoners te verbeteren. De mogelijkheid om uw gebouw altijd, overal en op elk apparaat te kunnen beheren is een belangrijke voorwaarde voor een goed comfortniveau in dat gebouw.

Met de big data-intelligentie die de cloud biedt, kunt u grote gegevensvolumes verwerken, analyseren en opslaan. Eventuele problemen worden daardoor snel en efficiënt opgespoord en opgelost. Deze efficiëntie resulteert in een hoger comfortniveau in het gebouw en een verbetering van de resultaten in het algemeen. Wij noemen dit een groeiklimaat.



>

1.2 Wat zijn de voordelen?

De cloud is een krachtig hulpmiddel om gebruikers in hun processen te ondersteunen en biedt gebruiksgemak. Bij Priva gebruiken we verschillende technologieën om onze producten en diensten zo krachtig mogelijk maken en toch gebruiksvriendelijk te houden.

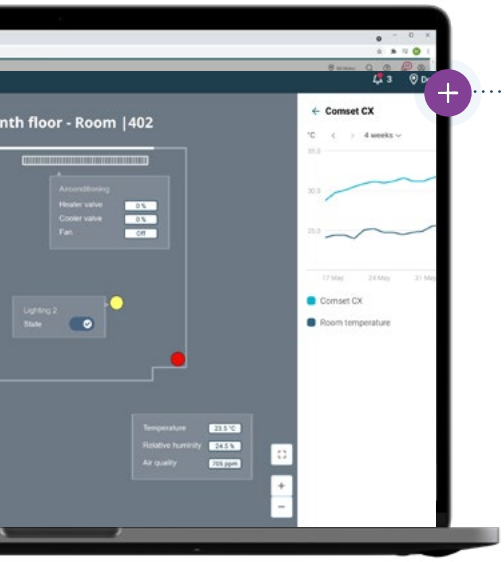
De cloud is een belangrijke technologie die waar dan ook geweldige gebruikerservaringen mogelijk maakt. Dat vertaalt zich in de volgende voordelen:

1. **Altijd, overal en vanaf elk apparaat verbonden zijn**
2. **Het comfort van de bewoners verhogen**
3. **Afhandeling van alarmmeldingen**
4. **Proactief onderhoud ondersteunen**
5. **Doorlopend verbeteringen aanbrengen**

Het beheren en optimaliseren van gebouwen is niet iets om vanachter een bureau te regelen. Het vraagt om betrokkenheid bij de gebruikers van het gebouw en om een directe aanpak als zich problemen voordoen. Met behulp van cloud-verbonden software kunt u een oogje in het zeil houden, aanpassingen doen, prestaties analyseren en waarschuwingsmeldingen beheren. Zo kunt u zich op uw taken concentreren en problemen snel en efficiënt oplossen.

Tegenwoordig is alles met elkaar verbonden. Dat roept ook vragen op over de beveiliging van gegevens. In de cloud kunnen beveiligingsupdates gecentraliseerd en geoptimaliseerd worden. Dit minimaliseert de risico's dat verouderde softwareoplossingen problemen veroorzaken.

Deze updates omvatten echter meer dan alleen beveiliging. Technologie verbetert sneller dan ooit. Wanneer u een BMS implementeert, wilt u niet dat dit systeem een jaar later verouderd is. Het is daarom noodzakelijk om compatibiliteit tussen de technologieën te creëren.



Door de cloud te gebruiken om het besturingssysteem los te koppelen van de toepassingen, kan elke nieuwe technologie in de cloud-omgeving worden geïntegreerd zonder het lokale besturingssysteem te veranderen. Dit betekent dat nieuwe technologieën moeiteloos in uw BMS geïntegreerd kunnen worden.
Op deze manier blijft de tijd niet stilstaan en is de technologie van uw gebouw vanaf de ontwerpfase tot aan een renovatie of verbouwing te allen tijde up-to-date.

Technologie is niet het enige dat in de loop van de tijd kan veranderen. Ook uw behoeften kunnen veranderen. In dat geval is het heel eenvoudig om uw dienstenpakketten aan te passen. Zonder kostbare of ingewikkelde aanpassingen in het lokale systeem waar verschillende experts aan te pas moeten komen. U bent veel flexibeler om het gebouw in te richten naar uw behoeften.

Datagegevens kun je vergelijken met een ruwe grondstof: ze zijn pas waardevol na verfijning en als ze gemakkelijk en op de juiste plaats toegankelijk zijn. Met behulp van de cloud bladert u door gegevens in een eenvoudige grafiek of voert u complexe analyses uit, zonder de enorme hoeveelheid rekenkracht en complexiteit op te merken die nodig is om meer gegevens te verwerken dan uw lokale toestel aankan.

>

1.3 Tot besluit

Het gebruik van de cloud verhoogt de gebouwwaarde door u en uw processen beter te ondersteunen en het volledige potentieel van uw gegevens te benutten, en is tegelijkertijd gebruikersvriendelijker, veiliger, flexibeler én toekomstbestendiger.

>

2. Beveiliging van de cloud

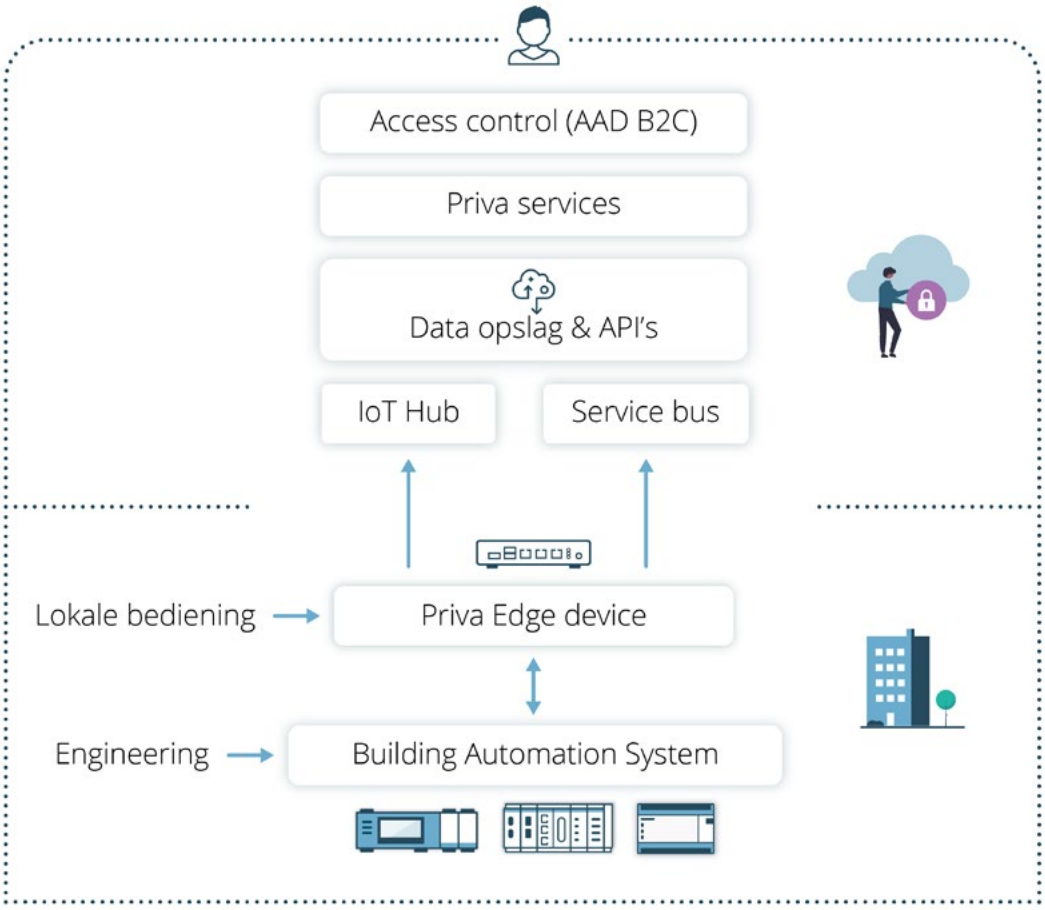
Het ontwikkelen van veilige clouddiensten is een uitdagend proces dat vraagt om expertise en een veilig en stabiel cloudplatform. Wij gebruiken het Microsoft Azure-platform als betrouwbare basis voor al onze clouddiensten. Microsoft Azure is een cloudplatform met een hoog beveiligingsniveau, zoals blijkt uit de meer dan 90 compliance-certificeringen die het platform bezit. Deze certificeringen staan vermeld op de website van Azure, bij de documentatie over compliance. Voor uitgebreide informatie over de beveiligingsmaatregelen van Microsoft kunt u terecht in het Microsoft Trust Center.

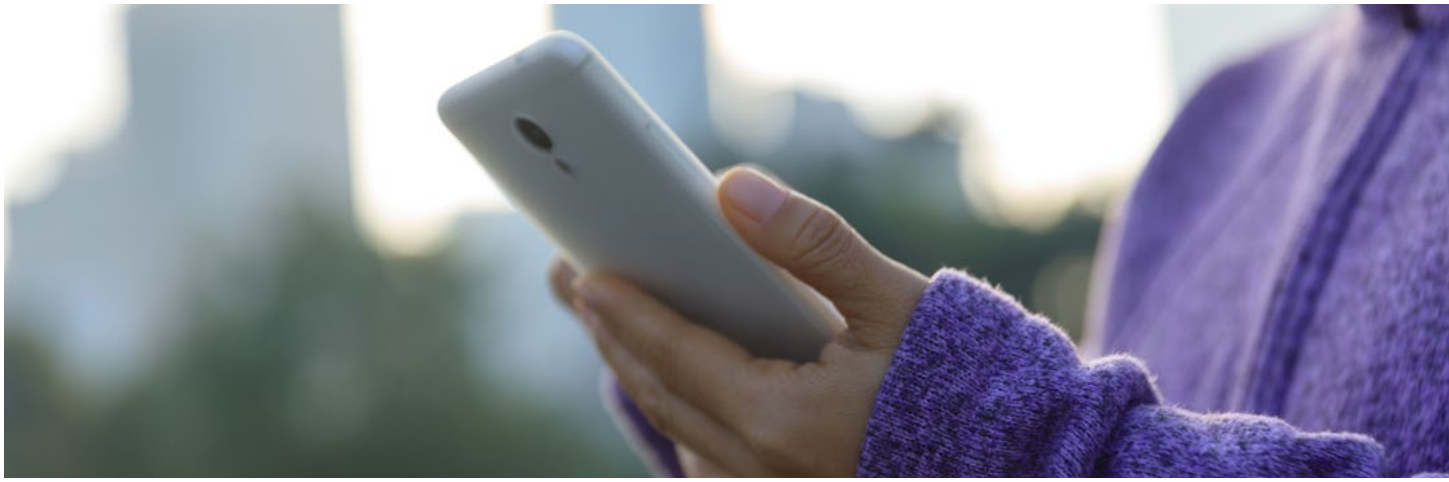
Naast het cloudplatform Microsoft Azure waarvan wij gebruikmaken, hebben wij onze Priva Digital Services ontwikkeld. Microsoft Azure biedt ons veiligheid op het vlak van datacenters, fysieke infrastructuur en standaardcomponenten. Dat betekent dat Priva zich qua veiligheid kan richten op het ontwerpen van software, coderen en de configuratie van onze digitale diensten. Voor de ontwikkeling en het gebruik van deze services passen wij bekende beveiligingsprincipes toe zoals ‘security by design’ en ‘defense in depth’.

Onze architecten en beveiligingsspecialisten werken nauw samen met de ontwikkelingsteams, zodat informatiebeveiliging een integraal onderdeel vormt van het ontwikkelingsproces. Tijdens de ontwikkelfase testen wij voortdurend of onze producten en diensten aan het vereiste veiligheidsniveau voldoen. Dit doen we aan de hand van risicobeoordelingen, geautomatiseerde tests en handmatige coderevisies, in overeenstemming met ons beleid inzake softwareontwikkeling en ander beleid voor informatiebeveiliging.

Om er zeker van te zijn dat (cloud)diensten van Priva veilig zijn, huurt Priva daarnaast onafhankelijke ethische hackers in om periodiek pentesten uit te voeren. De bevindingen worden onderzocht en problemen opgelost, zodat het beveiligingsniveau voortdurend toeneemt. Wanneer een dienst of hardware-apparaat voldoende beschermd is, verstrekken de ethische hackers een derdenverklaring (TPM, Third Party Memorandum) om hun bevindingen over het beveiligingsniveau formeel te bevestigen. Priva is bovendien ISO 9001 en ISO 27001 gecertificeerd.

Architectuur van Priva-services





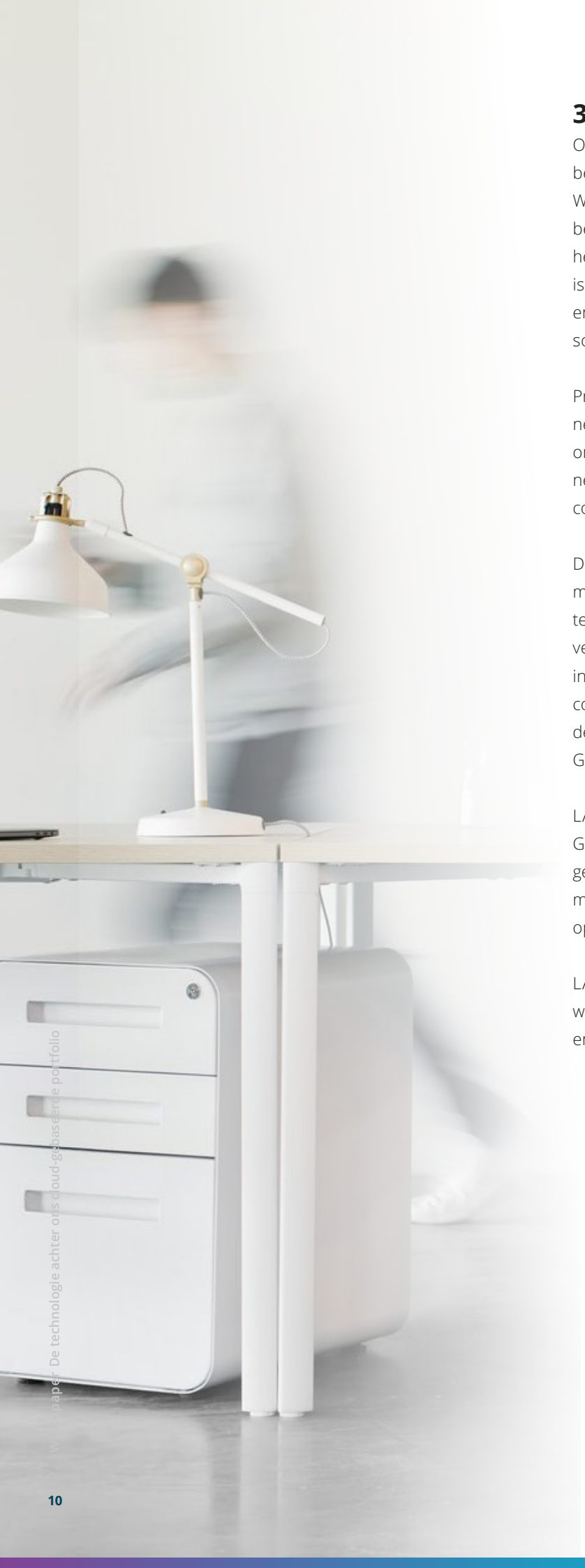
3. Meer over de beveiliging van Priva Services

Priva-services, en de infrastructuur erachter, kunnen in meerdere beveiligingslagen verdeeld worden. Het begint met het besturingssysteem. Het **besturingssysteem** maakt verbinding met de cloud via de **Priva Edge Gateway**. In de cloud worden de gegevens opgeslagen en de services gehost. Dit is ook de plaats waar gebruikers toegang krijgen tot hun services. De beveiliging van elk van deze onderdelen wordt hieronder besproken.

3.1 Het besturingssysteem

Het besturingssysteem is het netwerk van controllers dat de klimaatinstallatie regelt. Over het algemeen hebben controllers van gebouwautomatisering en andere verwante apparatuur te maken met een beperkte mate van beveiliging. Het netwerkverkeer tussen de onderdelen van het besturingssysteem is vaak ook onversleuteld. Apparatuur voor gebouwautomatisering functioneert naar verwachting meer dan tien jaar lang, dag en nacht; de reden waarom het ongelooflijk moeilijk is om het systeem tijdens de gehele levensduur up-to-date te houden en te beveiligen.

Systemen voor gebouwautomatisering dienen gebruik te maken van een gespecialiseerd technisch netwerk dat deze systemen op een veilige manier scheidt van alle mogelijke manieren van toegang van buitenaf. Systemen voor gebouwautomatisering mogen nooit draaien op netwerken die via het internet toegankelijk zijn.



3.2 Priva Edge Gateway

Om clouddiensten te kunnen gebruiken, moet het besturingssysteem verbinding maken met het internet. Wij maken gebruik van Priva Edge Gateway om een beveiligde interface tussen het besturingssysteem en het internet tot stand te brengen. De Priva Edge Gateway is een gesloten systeem dat alleen geconfigureerd is en gebruikt kan worden voor Priva-services. Niet-Priva software kan hier niet op draaien.

Priva Edge Gateway gebruikt drie afzonderlijke netwerkkaarten die niet overbrugd kunnen worden om het internet fysiek te scheiden van het technische netwerk dat onze controllers gebruiken. Zo blijven de controllers logisch gescheiden van het internet.

De eerste netwerkkaart, LAN1, is voor de verbinding met de buitenwereld. Om bescherming te bieden tegen mogelijke indringers, gebruikt de kaart uitgaande verbindingen en alleen de minimaal noodzakelijke inkomende verbindingen (zie de tabel hiernaast). Elke communicatie tussen het gebouwbeheersysteem en de cloud wordt altijd geïnitieerd door de Priva Edge Gateway.

LAN2 is voor het verbinden van de Priva Edge Gateway met het netwerk waar het systeem voor gebouwautomatisering op staat. Om verbinding te maken met de andere apparaten, heeft LAN2 poorten openstaan voor inkomend verkeer.

LAN3 is voor service. LAN3 geeft toegang tot de lokale webinterface waarmee de instellingen van de apparatuur en het netwerk gewijzigd kunnen worden.

	Accepteert inkomend verkeer	UDP-poort	TCP-poort	Doel
LAN 1 /LAN 2/ LAN 3	Ja	68		DHCP (Client)
LAN 3	Ja		80	Lokale webinterface
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	Functies van Building Operator Local of Building Operator Local Fallback
LAN 2	Ja	5353		mDNS
LAN 2	Ja	7650/ 7651/ 7660/ 7661		DDS
LAN 2	Ja	9508		PTP
LAN 2	Ja	15000/15001		Comprinet

Voor de communicatie tussen het gebouw en de cloud gebruiken wij standaard Microsoft-componenten. Meer specifiek maken onze services gebruik van IoT Hub en Service Bus van Microsoft Azure. Het netwerkverkeer tussen Priva Edge Gateway en de cloud is versleuteld. In tegenstelling tot sommige andere methoden om toegang te krijgen tot onderhoudssystemen voor gebouwen zoals VPN, maakt deze architectuur gebruik van een op berichten gebaseerd systeem. Op deze manier is er geen volledige gegevensverbinding tussen het gebouw en de buitenwereld.
Er worden slechts zeer beperkte relevante gegevens uitgewisseld.

> *Het netwerkverkeer tussen Priva Edge Gateway en de cloud is versleuteld.*

Het concept van de cloud is eenvoudig: bedrijven kunnen de cloud gebruiken voor de opslag, overdracht en verwerking van gegevens...

3.3 Beveiliging van de cloud

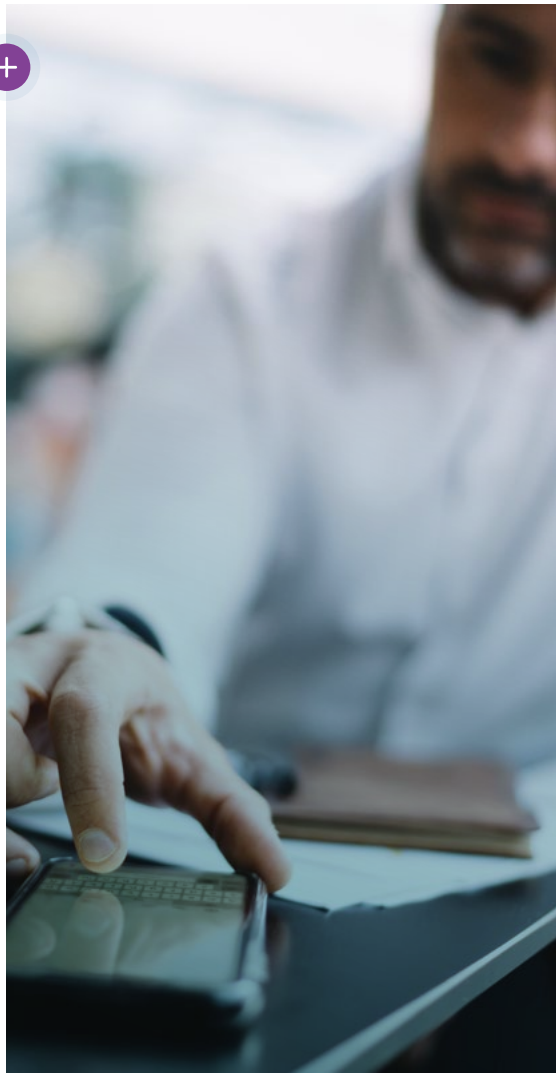
De primaire verdediging tegen onbevoegde gebruikerstoegang tot onze clouddiensten is een authenticatielaag op basis van het OAuth2-protocol. Wij gebruiken Azure Active Directory B2C (AAD B2C) als onze identiteitsprovider en een implementatie van de Identity Server die de autorisatieregels voor deze identiteiten levert. Wij zorgen ervoor dat de communicatie met al onze services verloopt via HTTPS (TLS v1.2 of hoger).

Nadat een gebruiker zich bij AAD B2C heeft geauthenticeerd, worden zijn rechten gecodeerd in een JSON Web Token en ondertekend met een privésleutel. Telkens wanneer een van onze toepassingen toegang wil tot uw gegevens, moet hij het token voorleggen aan de service die ze opslaat. De service zal dan controleren of er niet met het token is geknoeid met behulp van een openbare sleutel, en of de gebruiker toestemming heeft om toegang te krijgen tot de gevraagde bron.

Gebruikers van Priva-services zijn bekend met Access Control, het systeem waarmee administratieve gebruikers van een organisatie kunnen bepalen welke accounts toegang hebben tot welke functies en gebouwen. Op het moment van aanschaf geven wij toegangsrechten aan de koper van de service, waarna hij anderen kan uitnodigen en hun rechten kan bepalen.

Standaard is MFA (Multi-Factor Authentication) ingeschakeld voor nieuwe gebruikers, wat de veiligheid tijdens het inloggen verhoogt. Naast het wachtwoord van de gebruiker vereist MFA een tweede authenticatiefactor zoals een sms met een eenmalige code om toegang te krijgen tot de cloudservices.

Bovendien ondersteunen onze services ook het gebruik van de AAD van de klant, waarmee de klant een uitgebreidere controle over het beveiligingsbeleid heeft.



3.4 Beveiligde communicatie

Priva Digital Services hebben verschillende grote veiligheidsvoordelen ten opzichte van de traditionele verbindingsmethoden. Met Priva Digital Services is er geen tunnel – die veel belangrijke functies met elkaar verbindt, misschien over gebouwen heen of buiten uw eigen controle – waarin ingebroken kan worden. De Priva-services maken gebruik van een op berichten gebaseerd systeem. Ook is er geen ingewikkelde installatie of configuratie nodig, wat de kans op fouten en potentiële zwakke punten verkleint. Toegang geven of intrekken met behulp van Access Control is zo veel gemakkelijker voor meerdere gebouwen; geen dubbele logincodes of meerdere wachtwoorden of mensen op één account (voor veiligheidsdoeleinden).

3.5 Welke eindpunten gebruiken Priva services?

Om verbinding te maken met de diensten in de cloud gebruikt onze Priva Edge Gateway volledig gekwalificeerde domeinnamen (Fully Qualified Domain Names, FQDN's). Het complete overzicht van specifieke FQDN's is beschikbaar in de documentatie. Hieronder vindt u een beknopt overzicht van FQDN's met wildcards:

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

3.6 Wie is de eigenaar van de gegevens?

Ons beleid is dat de gegevens toebehoren aan degene die eigenaar is van het systeem dat ze genereert. Wij behouden ons echter het recht voor om deze gegevens voor ontwikkelingsdoeleinden te gebruiken nadat ze anoniem zijn gemaakt. Het volledige beleid van Priva ten aanzien van het gebruik van gegevens staat beschreven in onze algemene en servicegerelateerde voorwaarden en ons privacybeleid.

3.7 Waar worden uw gegevens opgeslagen?

Al onze clouddiensten worden gehost in de regio West-Europa van Microsoft Azure. De datacenters in deze regio zijn momenteel fysiek gevestigd in/bij Amsterdam. Voor doeleinden met betrekking tot herstel na noodgevallen worden deze datacenters van Microsoft echter gekoppeld aan de gegevens in de regio Noord-Europa van Microsoft Azure, die zich fysiek in/bij Dublin, Ierland bevinden. In noodsituaties kunnen uw gegevens tussen deze twee datacenterlocaties worden overgebracht. Voor deze gegevensoverdrachten wordt altijd gebruikgemaakt van de communicatie-infrastructuur waarvan Microsoft eigenaar is.

PRIVA 10-2022

Neem contact op

We horen graag van u!

Priva
Zijlweg 3
2678 LC De Lier

P.O. Box 18
2678 ZG De Lier
Netherlands

priva.com

#creatingaclimateforgrowth