DE TECHNOLOGIE ACHTER ONZE CLOUDGEBASEERDE PORTFOLIO

HOE BESCHERMT PRIVA UW DATA?

WAAROM DE CLOUD?

Het concept van de cloud is eenvoudig: in plaats van grote IT-organisaties te kopen en te onderhouden, kunnen bedrijven de cloud gebruiken om dataopslag, -communicatie en -verwerking uit te besteden. Externe toegang tot energie- en procesdata via de cloud is vooral voor gebouweigenaars of facilitair managers interessant, omdat daarmee het comfort van de gebouwgebruikers kan worden vergroot.

Hoewel comfort een van de belangrijkste vereisten is voor een sterk presterende organisatie, blijft het optimaliseren en onderhouden van klimaatsystemen zodat een optimaal comfortniveau kan worden geboden een complex proces dat veel aandacht vereist.

In staat zijn uw gebouw altijd, overal en op elk apparaat te beheren is een belangrijk onderdeel van het realiseren van comfort in het gebouw. Samenwerking met andere disciplines is een tweede belangrijk onderdeel. Tot slot kunnen we moderne technologie gebruiken om de gigantische hoeveelheid data die een gebouw genereert te gebruiken om het nut van het gebouw zo groot mogelijk te maken.

Met de cloud wordt dat mogelijk. De cloud heeft genoeg vermogen om de data te verwerken. En omdat het steeds toegankelijk is, is samenwerking en toegang tot het gebouw overal en op ieder moment mogelijk.

Als rechtstreeks gevolg daarvan worden problemen sneller en efficiënter opgespoord en opgelost. Die efficiëntie zorgt voor meer comfort in het gebouw en een algemene toename van de prestaties: Wij noemen dat een klimaat voor groei.

WAT ZIJN DE VOORDELEN?

Bij Priva streven we ernaar producten en services te ontwikkelen waarmee onze klanten hun bedrijf kunnen laten groeien. Om onze producten en services zo krachtig mogelijk te maken en toch zo eenvoudig mogelijk te houden, maken we gebruik van uiteenlopende technologieën. De cloud is daarbij cruciaal en stelt ons in staat gebruikers altijd, overal en op elk apparaat een fantastische ervaring te bieden. Dat komt neer op de volgende voordelen:

ALTIJD, OVERAL, ELK APPARAAT

GEBRUIKERS-COMFORT

REAL-TIME MELDINGEN

PROACTIEF ONDERHOUD

VOORTDURENDE VERBETERINGEN

VERBETERDE SERVICES

CLOUDPLATFORM:
MICROSOFT AZURE

Onze technologie stuurt functies aan die cruciaal zijn voor de kernactiviteiten van degenen die ze gebruiken. Het is zeer belangrijk dat die producten en services en de daarmee samenhangende data zijn beveiligd. Daarom leggen we u graag uit welke beveiligingsmaatregelen we hebben genomen:

We hebben al onze services vormgegeven op basis van het cloudplatform van Microsoft Azure. We hebben voor Azure gekozen vanwege de uitgebreide beveiligingsmaatregelen die Microsoft heeft genomen en de standaardcomponenten die Microsoft biedt. Zo kunnen wij ons richten op het scheppen van meerwaarde voor onze klanten en laten we de experts bij Microsoft zich bezighouden met de beveiliging van services en data. Het beveiligen van software is een reusachtige en dure taak waar specialistische kennis voor nodig is. Als vooraanstaande platformprovider is Microsoft in staat te investeren in de beveiliging van zoiets complex als softwareservices.

En dat is te merken. Azure voldoet in totaal aan meer dan 75 lokale, regionale en wereldwijde normen en biedt dus een mate van beveiliging en conformiteit die geen enkele organisatie ooit zelf zou kunnen bereiken met hun eigen ICT-afdeling.

De uitgebreide beveiligingsmaatregelen die Microsoft heeft getroffen, worden ook genomen voor de services van Priva. Gedetailleerde informatie over de beveiliging van Microsoft vindt u in het Microsoft Trust Center.

>

UW **GOUD** BEVEILIGEN

De beveiliging van de cloud kan worden vergeleken met een bankkluis. U kunt uw goud onder uw bed bewaren, waar u het dicht bij u kunt houden. Maar sloten houden alleen eerlijke mensen buiten. Als iemand echt bij u wil inbreken, hoeven ze alleen het juiste moment uit te kiezen en wat gereedschap mee te nemen.

U kunt er ook voor kiezen uw goud in een bankkluis te bewaren en een organisatie te betalen die als doel heeft uw waardevolle eigendommen veilig te stellen. Het resultaat? Het is nu moeilijker om uw goud te stelen.

WAAR ZOU U UW **GOUD** BEWAREN?

EEN BLIK OP DE BEVEILIGING VAN **PRIVA SERVICES**

De beveiliging van Priva-services en de infrastructuur achter deze services kan worden onderverdeeld in meerdere stappen. Het begint met het **beheersysteem**. De **Cloud Connector** zorgt ervoor dat het beheersysteem met de cloud is verbonden. In de cloud wordt data opgeslagen en zijn de services ondergebracht. Hier hebben gebruikers ook toegang tot de services. De beveiliging van elk van deze stappen wordt hieronder besproken:

HET BEHEERSYSTEEM

Het beheersysteem is het netwerk van controllers waarmee de klimaatinstallatie wordt aangestuurd. Over het algemeen zijn controllers voor gebouwautomation niet beveiligd en is er in de kernprotocollen voor gebouwautomatisering, zoals BACnet, geen mogelijkheid tot versleuteling. De controllers van Priva en de communicatie tussen de controllers zijn ook niet beveiligd.
Voor gebouwautomatiseringsystemen dient altijd gebruik te worden gemaakt van een speciaal technisch netwerk dat veiligheid biedt doordat het gebouwautomatiseringsysteem gescheiden wordt gehouden van middelen die toegang van buitenaf mogelijk maken. Gebouwautomatiseringsystemen mogen nooit op een netwerk met internettoegang draaien.

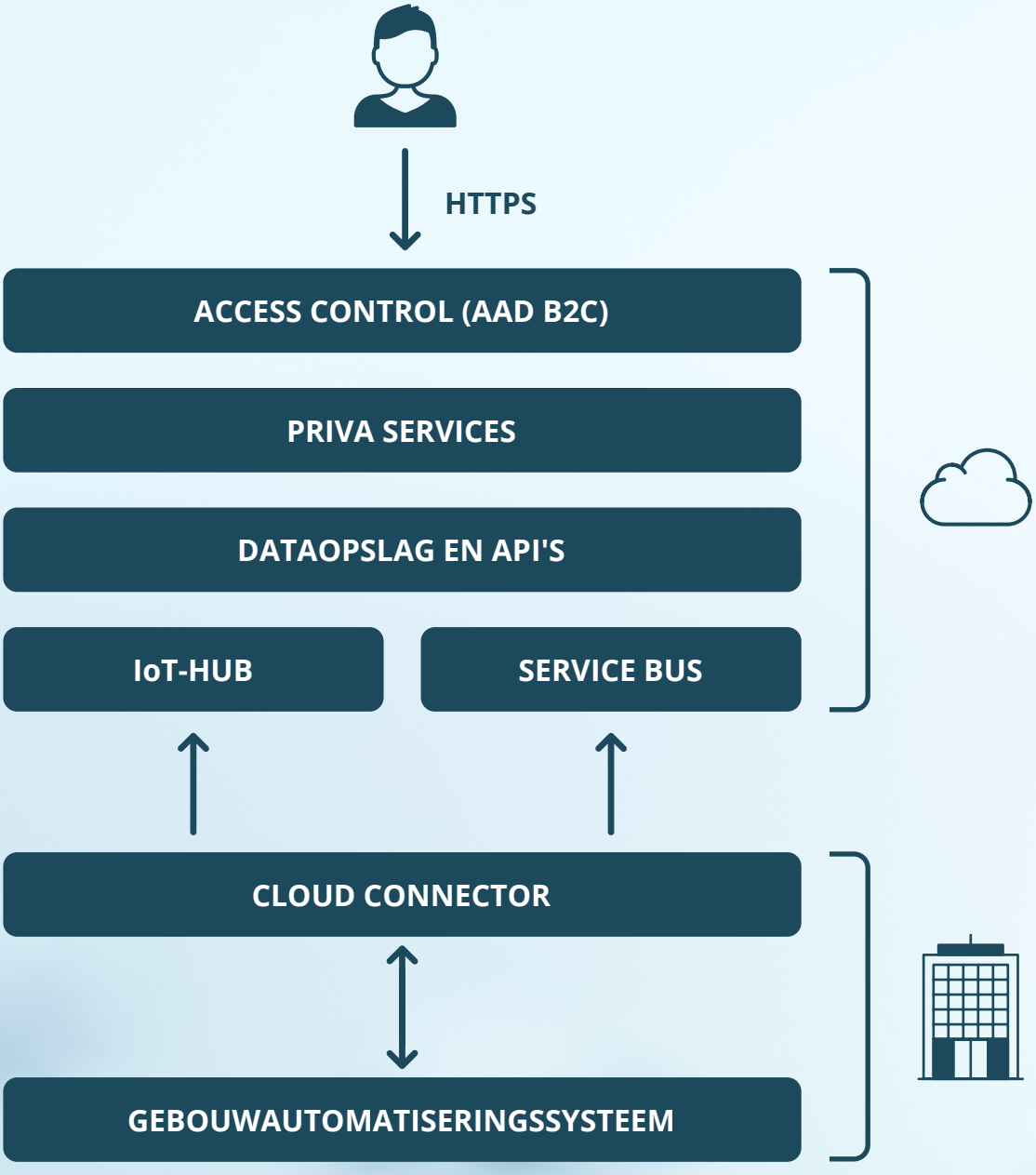
DE CLOUD CONNECTOR

Om cloudservices te kunnen gebruiken, moet het beheersysteem natuurlijk verbinding kunnen maken met het internet. Daarom gebruiken we de Cloud Connector voor een veilige interface tussen het controlesysteem en het internet. Om dat mogelijk te maken, heeft de Cloud Connector alleen uitgaande en geen inkomende verbindingen. Communicatie tussen het gebouw en de buitenwereld wordt daarom altijd door de Cloud Connector gestart. Vanuit het internet gezien bestaat de Cloud Connector dus eigenlijk niet. En iets wat niet bestaat, kan ook niet worden aangevallen.

Dit betekent ook dat er geen binnenkomende poorten hoeven te worden geopend. Uitgaande poorten moeten dan wer wel worden geopend. De poorten die worden gebruikt zijn de volgende: **Port 443 (HTTPS), Port 5671/5672 (AMQP) en 8883 (MQTT), Port 9354 (SBMP)**.

We maken gebruik van standaardcomponenten van Microsoft voor de communicatie tussen het gebouw en de cloud. Dat zijn de IoT-hub en Service Bus van Microsoft Azure. De data die wordt overgedragen tussen de Cloud Connector en de cloud is beveiligd aan de hand van versleuteling. In tegenstelling tot andere methoden voor toegang tot gebouwautomatiseringssystemen, zoals een VPN, maakt deze architectuur gebruik van een systeem op basis van berichten, dus is er geen volledige datalink tussen het gebouw en de buitenwereld. Er wordt slechts in heel beperkte mate data uitgewisseld.

PRIVA SERVICES
ARCHITECTUUR



EEN BLIK OP DE BEVEILIGING VAN **PRIVA SERVICES**

BEVEILIGING VAN DE CLOUD

De voornaamste bescherming tegen toegang door onbevoegden tot onze cloudservices is een verificatiestap op basis van het OAuth2-protocol. We gebruiken Azure Active Directory B2C (AAD B2C) als onze id-provider en een implementatie van een Identity Server die autorisatieregels voor deze identiteiten levert. We zorgen ervoor dat communicatie met al onze services verloopt via HTTPS (TLS v1.2 of hoger) en onze verificatielaag is geen uitzondering.

Nadat een gebruiker is geverifieerd via AAD B2C, worden de rechten van die gebruiker versleuteld in een JSON Web token en ondertekend met een privésleutel. Wanneer een van onze applicaties toegang tot uw data wil, moet de token worden aangeleverd aan de service die de data bewaart. De service controleert vervolgens aan de hand van een openbare sleutel of er niet met de token is geknoeid en of de gebruiker toegang heeft tot de aangevraagde resource.

Gebruikers van Priva services zijn bekend met Access Control, het overzicht dat we hebben gebouwd op basis van die verificatielaag. Hiermee kunnen gebruikers met beheerdersrechten van een organisatie bepalen welke accounts toegang hebben tot bepaalde functies en gebouwen. Op het moment van aankoop geven we de volledige rechten aan de koper van de service, waarna ze anderen kunnen uitnodigen en hun rechten kunnen beheren.

Microsoft heeft wat betreft conformiteit uitgebreide maatregelen getroffen om te voldoen aan normen en wetgeving. Normen als ISO/ICE 27018 en de AVG zorgen ervoor dat persoonsgegevens en wachtwoorden worden beveiligd. Er wordt regelmatig op de naleving hiervan gecontroleerd. Omdat we AAD B2C als onze ID-provider gebruiken, wordt data met betrekking tot die identiteit opgeslagen bij Microsoft en wordt er aan deze normen voldaan.

ONZE OPLOSSING VERSUS VPN

VPN's worden vaak gebruikt in de gebouw-automatisering om beheersystemen op afstand te beheren of daartoe toegang te verkrijgen. De services van Priva bieden een aantal grote voordelen ten opzichte van een traditioneel VPN. VPN's zijn tunnels door het internet, maar de communicatie in deze tunnels is vaak niet beveiligd en bestaat in veel gevallen uit een volledige datalink. Als iemand de tunnel binnendringt of op een andere manier toegang krijgt, loopt alles op het netwerk gevaar.

Voor de services van Priva wordt geen tunnel gebruikt die kan worden binnengedrongen, wat de oplossing veel veiliger maakt. Onze oplossing is veel veiliger. Bovendien is er geen moeilijke installatie of configuratie nodig, dus is er minder kans op fouten en zijn er minder potentieel zwakke plekken.

> WELKE EINDPUNTEN WORDEN VOOR PRIVA SERVICES GEBRUIKT?

Onze Cloud Connector maakt gebruik van Fully Qualified Domain Names (FQDN's) om verbinding te maken met de services in de cloud. De documentatie bevat het volledige overzicht van specifieke FQDN's. Hieronder vindt u een fragment van FQDN's met wildcards, zodat u een idee krijgt:

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

HET LEVEN VAN ONZE KLANTEN EENVOUDIGER MAKEN

Al onze (online) services en producten zijn onderhevig aan de **algemene voorwaarden van de Priva Cloud**, die u kunt vinden op www.priva.com/general-conditions.

VAN WIE IS DE DATA?

Wie de eigenaar is van data, is overal ter wereld een lastig onderwerp omdat het juridisch gezien niet mogelijk is om data te bezitten. Data bestaat uit enen en nullen en heeft geen duidelijk gedefinieerde grenzen, waardoor de eigenaar niet kan worden bepaald. Maar u kunt wel het recht op het gebruik van data hebben.

De data in onze systemen bestaat voornamelijk uit meetresultaten en instellingen voor klimaatregeling. Het volledige beleid van Priva inzake het gebruik van die data wordt beschreven in de algemene voorwaarden. Kort gezegd is ons beleid dat de data het eigendom is van degene die het systeem bezit dat de data genereert. We hebben wel het recht om deze data te gebruiken voor R&D-doeleinden nadat de data is geanonimiseerd.

WAAR WORDT UW DATA OPGESLAGEN?

Al onze cloudservices zijn ondergebracht in de regio West-Europa van Microsoft Azure. De datacenters in deze regio zijn momenteel fysiek gevestigd in/nabij Amsterdam. Voor het herstellen van data in geval van een ramp zijn de datacenters echter gekoppeld aan datacenters in de regio Noord-Europa, die zich fysiek bevinden in/nabij Dublin, Ierland.
In noodsituaties kan uw data worden overgedragen tussen deze twee datacenterlocaties. Voor deze dataoverdracht wordt altijd gebruikgemaakt van de privécommunicatie-infrastructuur van Microsoft.

HEEFT DE AMERIKAANSE OVERHEID TOEGANG TOT COMMERCIËLE - OF CONSUMENTENDATA?

Volgens de AVG is het delen van data die is opgeslagen in de EU op basis van een besluit van een buitenlandse overheid of rechterlijke instantie uitsluitend toegestaan als er een verdrag bestaat met die overheid, dus binnen een wettelijk kader waarmee de EU heeft ingestemd.
Niet-naleving kan grote boetes voor de organisatie tot gevolg hebben. Dit blijft een moeilijk vraagstuk tussen de EU en de Amerikaanse overheid. Afgezien van de wetgevingskant heeft Microsoft keer op keer laten zien dat het bedrijf ernaar streeft de data van haar klanten veilig te bewaren en heeft het verzoeken om data te delen vaak met succes aangevochten.


#CLIMATE-AS-A-SERVICE

CREATING
> A CLIMATE
FOR GROWTH

PRIVA

Zie www.priva.com voor contactgegevens van een Priva-kantoor of -partner in uw regio.

Volg **Priva Building Automation** op LinkedIn en Twitter