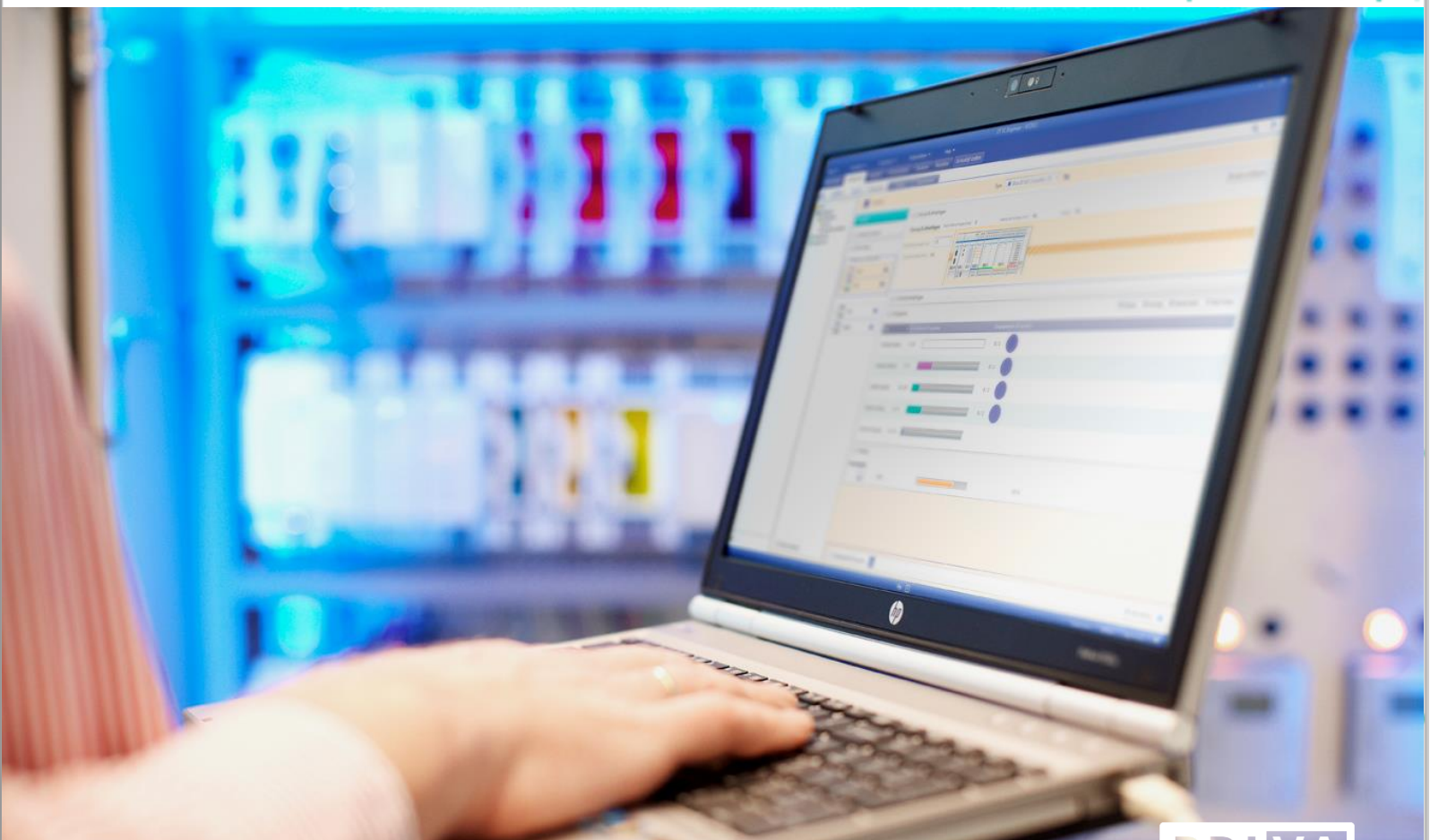
>

Cloudbeveiliging

Ontdek hoe Priva uw gegevens in de cloud beveiligt

Whitepaper



Deze whitepaper over cloudbeveiliging (cloud security) biedt een algemeen overzicht van de informatiebeveiligingsmaatregelen die Priva voor haar Clouddiensten heeft genomen.

Dit is een openbaar document om duidelijkheid te geven aan de klanten en partners van Priva, en om transparant te zijn over de informatiebeveiligingsmaatregelen die geïmplementeerd zijn en onderhouden worden binnen Priva Clouddiensten. Indien u aanvullende vragen heeft, kunt u contact opnemen met Priva's SQC-team (Security, Quality & Compliance) via sqc@priva.com.

Inhoudsopgave

1. Voorwoord

Priva streeft ernaar producten en diensten te ontwikkelen waarmee onze klanten hun bedrijf kunnen laten groeien. We gebruiken verschillende technologieën om onze producten en diensten zo krachtig mogelijk en tegelijk gebruiksvriendelijk te maken. De cloud is een belangrijke technologie die het mogelijk maakt om overal, altijd en op elk apparaat prettige gebruikerservaringen te hebben.

Beveiliging van deze producten en diensten - en van de data die ze bevatten - is van cruciaal belang. Dit document schetst de technologie achter ons portfolio van Clouddiensten, en beschrijft de stappen die we hebben genomen om ervoor te zorgen dat uw gegevens veilig zijn.

2. Veilige Clouddiensten

Het ontwikkelen van veilige Clouddiensten is een uitdagend proces. Het vereist aanzienlijke expertise en een veilig en stabiel cloudplatform. Wij gebruiken het Microsoft Azure cloudplatform als betrouwbaar fundament voor al onze Clouddiensten. Het hoge beveiligingsniveau van het Microsoft Azure cloudplatform wordt bevestigd door de meer dan 90 certificeringen die hiervoor zijn afgegeven. Deze certificeringen staan vermeld in documentatie op de eigen website van Azure. Meer specifieke informatie over de beveiligingsmaatregelen van Microsoft is te vinden in het Microsoft Trust Center.

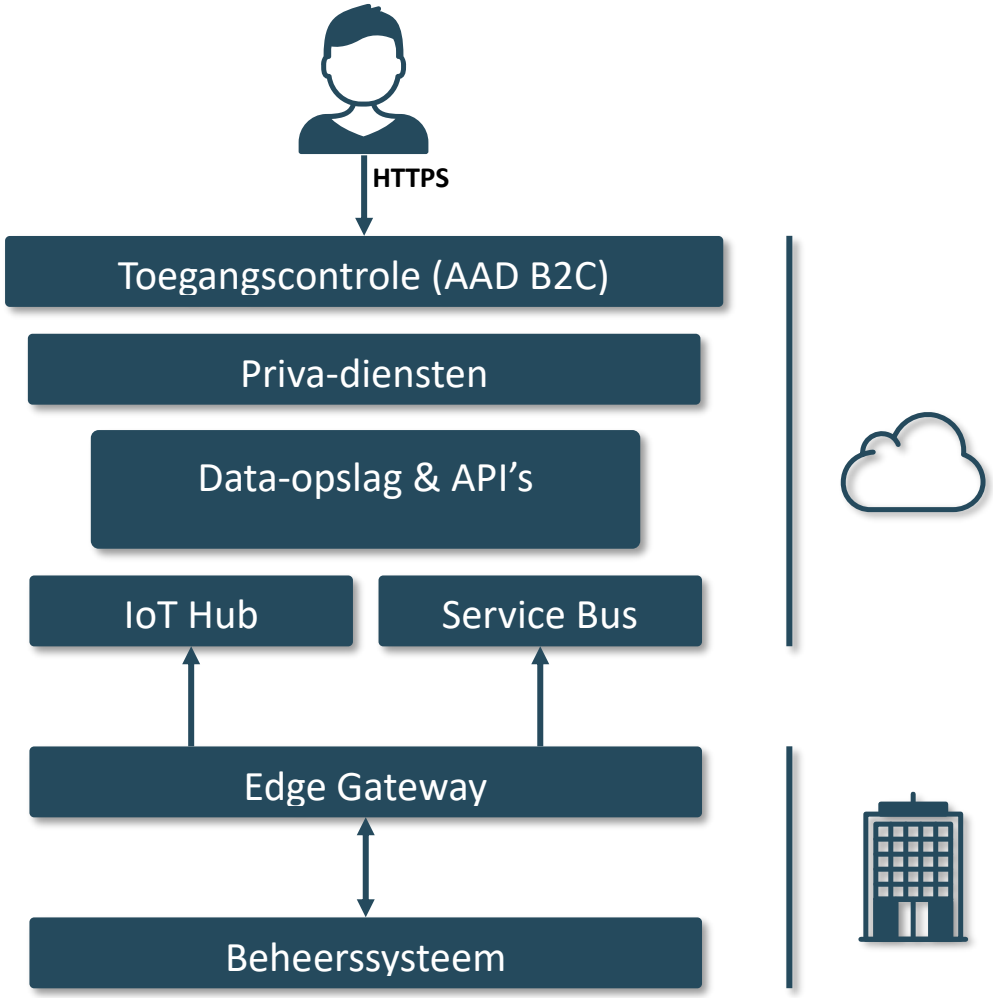
Onze Priva Clouddiensten zijn ontwikkeld op het Microsoft Azure-platform. Microsoft Azure biedt ons veilige datacenters, beveiligde fysieke infrastructuur en standaardcomponenten. Hierdoor kan Priva zich richten op veilig software-ontwerp, veilige codering en veilige configuratie van de eigen Clouddiensten. Bij de ontwikkeling en het gebruik van deze diensten passen wij bekende beveiligingsprincipes toe, zoals 'security by design' en 'defense in depth'.

Onze architecten en beveiligingsspecialisten werken nauw samen met de ontwikkelteams, zodat informatiebeveiliging een integraal onderdeel is van het ontwikkelproces. Tijdens de ontwikkeling testen we continu of onze producten en diensten voldoen aan het vereiste beveiligingsniveau. Dit gebeurt met behulp van risicobeoordelingen, geautomatiseerde testen en handmatige codebeoordelingen, in overeenstemming met ons softwareontwikkelingsbeleid en informatiebeveiligingsbeleid.

Om ervoor te zorgen dat Priva (Cloud)diensten veilig zijn, zet Priva ook onafhankelijke ethische hackers in om periodieke penetratietesten uit te voeren. Als hier bevindingen uit komen worden deze onderzocht en opgelost zodat het beveiligingsniveau continu wordt verbeterd. Wanneer een service of hardwarecomponent voldoende is beveiligd, verstrekken de ethische hackers een TPM (Third Party Memorandum) waarin zij hun bevindingen over het beveiligingsniveau formeel bevestigen. Ten slotte is Priva gecertificeerd volgens de normen ISO9001 en ISO27001.

3. Een nadere blik op de beveiliging van Priva-diensten

Priva-diensten, en de achterliggende infrastructuur, kunnen worden onderverdeeld in meerdere beveiligingslagen. Het begint bij het **beheerssysteem** dat verbinding maakt met de cloud via de **Edge Gateway**. In de cloud staan de gegevens opgeslagen en worden de diensten gehost. Dit is ook de locatie waar gebruikers toegang hebben tot hun diensten. Onderstaande afbeelding geeft een overzicht van de architectuur van de dienst. De beveiliging van elk van de onderdelen binnen de architectuur van de dienst wordt hierna toegelicht.



3.1 Het beheerssysteem

Het beheerssysteem is het netwerk van regelaars dat de klimaatinstallatie aanstuurt. Over het algemeen hebben controllers en andere gerelateerde apparaten een beperkte beveiliging. Het netwerkverkeer tussen onderdelen van het beheerssysteem is vaak ook onversleuteld vanwege het gebruik van niet-versleutelde protocollen en de noodzaak van onderlinge verbondenheid. Deze apparaten zullen naar verwachting langer dan tien jaar 24 uur per dag functioneren. Daarom is het erg moeilijk om ze tijdens hun gehele levensduur up-to-date en veilig te houden.

Beheerssystemen moeten altijd gebruikmaken van een apart daartoe ingericht technisch netwerk dat beveiliging biedt door het beheerssysteem te scheiden van alle mogelijke manieren om van buitenaf toegang te krijgen. Daarom mogen beheerssystemen nooit draaien op netwerken met internettoegang.

3.2 De Edge Gateway

Om gebruik te kunnen maken van Clouddiensten moet het beheerssysteem verbinding maken met internet. We gebruiken de Priva Edge Gateway om een veilige verbinding te bieden tussen het beheerssysteem en het internet. De Priva Edge Gateway is een gesloten systeem dat alleen voor Priva-diensten kan worden geconfigureerd en gebruikt. Niet-Priva-software kan er niet op draaien.

Om het internet fysiek te scheiden van het technische netwerk dat onze controllers gebruiken, worden drie afzonderlijke netwerkkaarten gebruikt die niet onderling gegevens kunnen uitwisselen. Hierdoor blijven de controllers op logische wijze gescheiden van het internet.

De eerste netwerkkaart, LAN1, maakt de verbinding met de buitenwereld. Ter bescherming tegen mogelijke indringers gebruikt LAN1 uitgaande verbindingen en alleen de minimaal noodzakelijke inkomende verbindingen. Elke communicatie tussen het beheerssysteem en de cloud wordt altijd geïnitieerd door de Edge Gateway.

LAN2 sluit de Edge Gateway aan op het technische netwerk. Om verbinding te maken met de andere apparaten, heeft LAN2 poorten open staan voor inkomend verkeer.

LAN3 is voor service op locatie. Via LAN3 is de lokale web-UI toegankelijk voor het openen en wijzigen van apparaat- en netwerkinstellingen.

We gebruiken standaard Microsoft-componenten om te communiceren tussen het beheerssysteem en de cloud. Onze diensten maken met name gebruik van IoT Hub en Service Bus van Microsoft Azure. Het netwerkverkeer tussen de Priva Edge Gateway en de cloud is versleuteld. In tegenstelling tot sommige andere toegangsmethoden, zoals VPN, gebruikt onze architectuur een systeem dat is gebaseerd op berichten. Er is dus geen volledige datalink tussen het beheerssysteem en de buitenwereld. Er worden slechts zeer beperkt relevante gegevens uitgewisseld.

3.3 Beveiliging van de cloud: toegangscontrole

De belangrijkste verdediging tegen ongeoorloofde gebruikerstoegang tot onze Clouddiensten is een authenticatielaag op basis van het OAuth2-protocol. We gebruiken Azure Active Directory B2C (AAD B2C) als onze identiteitsprovider en een Identity Server-implementatie biedt de autorisatieregels voor deze identiteiten. Het is zo ingesteld dat de communicatie met al onze diensten altijd via HTTPS (TLS v1.2 of hoger) verloopt.

Na authenticatie van een gebruiker via AAD B2C worden zijn of haar rechten gecodeerd in een JSON Web Token, en ondertekend met een persoonlijke sleutel. Op het moment dat een van onze applicaties toegang tot uw gegevens vraagt, moet die applicatie de token aanbieden aan de dienst die deze bewaart. Deze dienst controleert met de openbare sleutel vervolgens of de token niet is aangepast en of de gebruiker recht heeft op toegang tot de gevraagde informatie.

Gebruikers van Priva-diensten gebruiken Access Control. Dit maakt het voor gebruikers met beheerrechten binnen een organisatie mogelijk om na te gaan welke accounts toegang mogen hebben tot welke functies en locaties. Bij aankoop van een dienst verschaffen we de koper toegangsrechten, waarna de koper anderen kan uitnodigen en hun rechten kan beheren.

Standaard is MFA (MultiFactorAuthenticatie) ingeschakeld voor nieuwe gebruikers. Dit biedt een hogere mate van beveiliging tijdens de loginprocedure. Aanvullend op het gebruikerswachtwoord gebruikt MFA een tweede authenticatiefactor, zoals een tekstbericht met een eenmalige code, om toegang te krijgen tot de Clouddiensten.

Aanvullend ondersteunen onze diensten ook het gebruik van het AAD van de klant, waarmee de klant uitgebreidere mogelijkheden heeft om het beveiligingsbeleid te beheren.

3.4 Welke endpoints gebruiken Priva-diensten?

Om te verbinden met de diensten in de cloud gebruikt onze Edge Gateway Fully Qualified Domain Names (FQDN's). Een volledig overzicht van specifieke FQDN's is beschikbaar in de documentatie van de Edge Gateway.

3.5 Wie is eigenaar van de gegevens?

Het is ons beleid dat de gegevens toebehoren aan de eigenaar van het systeem dat de gegevens genereert. We behouden ons echter wel het recht voor om gegevens, nadat deze geanonimiseerd zijn, te gebruiken voor ontwikkeldoeleinden. Priva's volledige beleid ten aanzien van het gebruik van gegevens is beschreven in onze algemene en dienstspecifieke voorwaarden, en in ons privacybeleid.

3.6 Waar staan uw gegevens opgeslagen?

Al onze Clouddiensten worden gehost in de regio West-Europa van Microsoft Azure. De datacenters in deze regio zijn momenteel fysiek gesitueerd in/bij Amsterdam. Ten behoeve van disaster recovery zijn deze Microsoft-datacenters gekoppeld aan de datacenters van Azure in de regio Noord-Europa. Deze zijn fysiek gesitueerd in/bij Dublin in Ierland. In noodgevallen kunnen uw gegevens tussen deze twee locaties worden overgezet. Voor deze gegevensoverdracht wordt altijd gebruik gemaakt van de eigen bedrijfscommunicatie-infrastructuur van Microsoft.