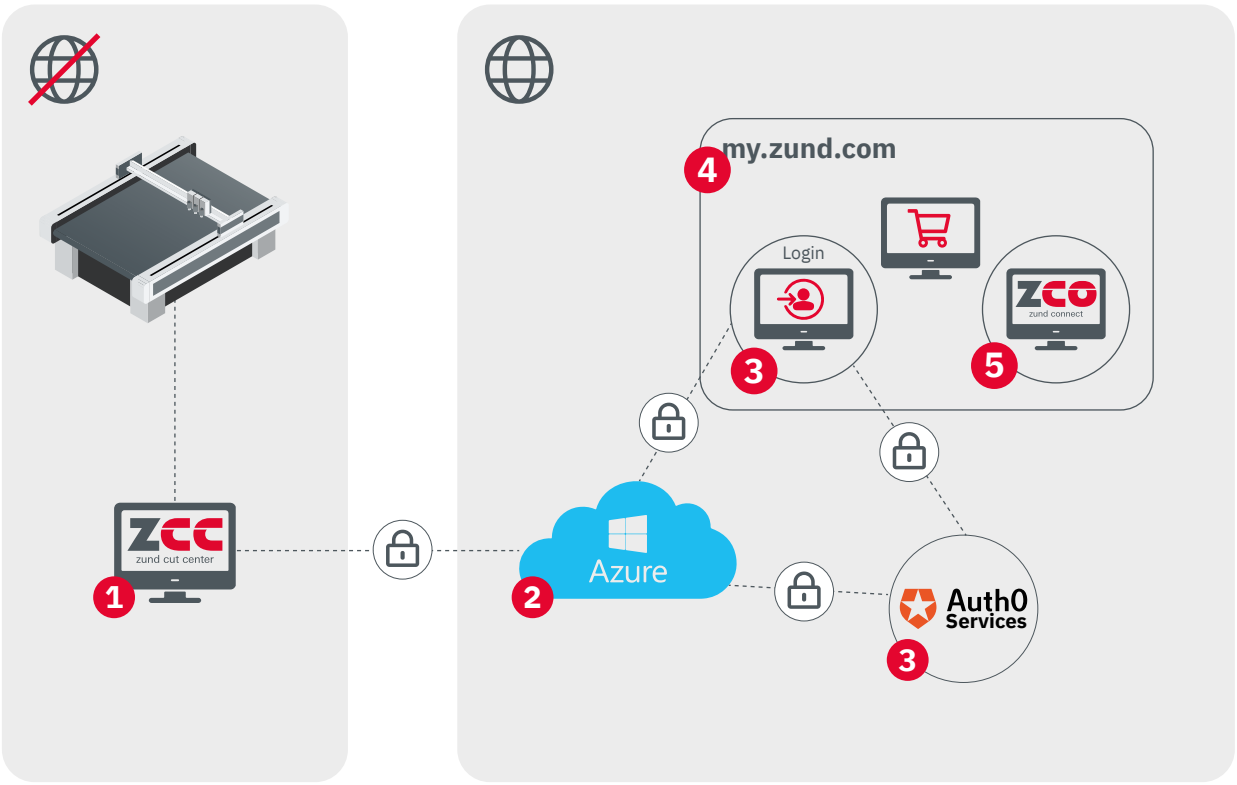
Gegevensveiligheid - Zünd Connect

Het gebruik van beproefde beveiligingsstandaarden en -componenten zorgt ervoor dat er voor gegevens en toegang een hoog niveau van bescherming wordt toegepast. Op deze manier worden de gegevens beschermd tegen kwaadwillig gebruik dat buiten het privacybeleid valt. Tevens worden de gegevens zo goed mogelijk beschermd tegen opzettelijke vernietiging door derden. Ze worden uitsluitend door de cutter naar de cloud gestuurd. Er is geen toegang vanuit de cloud tot de cutter.



Elke verbinding is met TLS 1.2 (Transport Layer Security) volgens RFC 5246 beveiligd.

Sub-systeem 1: Cutter Operation
Met de installatie van Zünd Cut Center (ZCC) wordt er een IoT-proxy voor Zünd Connect geïnstalleerd. De gebruiker moet uitdrukkelijk akkoord gaan met de installatie van de proxy. Deze proxy draait als een Windows-service op de achtergrond en bevat een lokale gegevensbuffer. In deze buffer worden gegevens die niet direct kunnen worden verzonden veilig op de harde schijf opgeslagen. Dit kan bijvoorbeeld het geval zijn wanneer de verbinding met de IoT-hub tijdelijk wordt onderbroken.
De proxy communiceert via AMQP: 5671 en https: 443 via een met TLS1.2 versleutelde verbinding met de IoT-hub. De authenticatie vindt plaats via een unieke sleutel die tijdens de installatie wordt gegenereerd.

Sub-systeem 2: Azure-cloud
De gegevens worden in een speciale instantie van de Microsoft Azure-cloud opgeslagen en verwerkt. Dit zorgt ervoor dat de nieuwste beveiligingsupdates van Microsoft te allen tijde worden uitgevoerd en het garandeert een hoog niveau van stabiliteit en beveiliging. Alle toegang tot de backend-database is met een wachtwoord beveiligd. De wachtwoorden die hiervoor worden gebruikt, zijn beveiligd in een speciaal ontworpen Key Vault in de Azure-cloud. Gegevenstoegang van het dashboard naar de backend is alleen mogelijk met de tijdelijke toegangstokens die worden gegenereerd wanneer de gebruiker zich aanmeldt.

Sub-systeem 3: Gebruikersauthenticatie
Om Zünd Connect te kunnen gebruiken, moet de gebruiker zich met een gebruikersnaam en wachtwoord op Mijn Zünd aanmelden. Voor registratie, login en wachtwoordherstel kiest Zünd voor de bewezen en veilige third-party oplossing van Auth0 om de hoogste veiligheidsnormen te garanderen.

Sub-systeem 4: my.zund.com
Zünd Connect is ingebed in het Zünd klantenportaal Mijn Zünd. Dit betekent dat de aanmelding van de gebruiker voor het gehele portaal geldig is.

Sub-systeem 5: Zünd Connect
De productie-efficiëntie, productieverliezen en hun oorsprong, evenals het snijmachine-overzicht kunnen worden bekeken vanaf elke desktopcomputer met een up-to-date webbrowser.

Hostnames ZundConnectProxy

Log data, via HTTPS (port 443)
dc.services.visualstudio.com

File upload (e.g. support report, .zcc-Files), via HTTPS (port 443)
zuend-iot-prod-hub.azure-devices.net
fileprodstore.blob.core.windows.net

Device provisioning (during the installation), via HTTPS (port 443)
zuend-iot-prod-cert-fn.azurewebsites.net

Events, via AMQP (port 5671)
zuend-iot-prod-hub.azure.devices.net

06/2024

Zünd Systemtechnik AG
Industriestrasse 8 | CH-9450 Altstätten | T +41 71 554 81 00 | info@zund.com | www.zund.com

ZÜND
swiss cutting systems