Wie aus einem Brennstoffzellenheizsystem ein IoT-Device wurde

(Internet-of-Things)

Kunde	HEXIS AG
Hardware	ARM-Cortex-M4 (STM32F439), Linux-Server-Appliance
Programmier-Sprachen	ANSI-C / PHP / SQL / JavaScript
Speziell	Aufbau eines "LowCost"-Fernwirksystems und Erweiterung der bestehenden Firmware um eine gesicherte Internet-Kommunikation

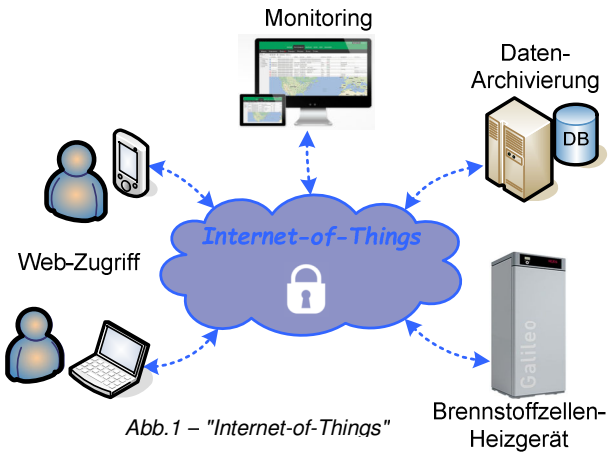

Abb.1 – "Internet-of-Things"

In das Internet "hinein" kommt man von überall, aus dem Internet "heraus" – auf lokale Netzwerke – kommt man nicht ohne weiteres (…Firewalls blockieren Internetzugriff auf Geräte in lokalen Netzwerken).

Möchte man über das Internet auf ein Gerät in einem lokalen Netzwerk zugreifen (Fernzugriff), muss man die Konfiguration der Firewall Vorort manipulieren, sodass diese die Verbindungen von "aussen" (Internet) nach "innen" (lokales Netzwerk) zulässt. Diese Manipulation birgt Sicherheitsrisiken für das lokale Netzwerk und ist daher für viele Anwendungen nicht zulässig.
Alternativ hierzu werden oft "Virtuelle-Private-Netzwerke (VPN)" mit sogenannten VPN-Gateways eingesetzt. Bei einer kleineren Anzahl von Endgeräten ist dies eine praktikable Lösung - sollen aber eine wachsende Zahl von örtlich verteilten Systemen permanent erreichbar sein, kann der Aufwand für ein solches VPN-Netzwerk sehr schnell sehr gross werden → Gründe:

- VPN-Gateways erzeugen Kosten bezüglich Gateway-Hardware und Installationsaufwand Vorort.
- VPN-Netzwerkserver müssen mit steigender Anzahl von VPN-Clients performanter ausgelegt werden (steigende Unterhaltskosten über die Zeit)
- Der Datendurchsatz eines "Virtuell-Privaten-Netzwerk" wird mit steigender Anzahl VPN-Clients geringer
- Das permanente Aufrechterhalten eines VPN-Kanals erfordert eine stetige Datenverbindung ("Daten-Grundlast"), auch wenn keine Nutzdaten transportiert werden (→ ineffizient).

Das Projekt

Unser Kunde – die Hexis AG – entwickelt und produziert innovative Brennstoffzellenheizgeräte für Ein- und Mehrfamilienhäuser. Nebst einem innovativen Produkt, möchte sie ihren Kunden zusätzlich Dienstleistungen rund um den Betrieb ihrer Geräte anbieten und benötigt hierzu einen zuverlässigen Fernzugriff.
Ursprünglich verwendete die Hexis AG ein Fernwirksystem basierend auf VPN-Gateways – mit dem Einstieg in die Serienproduktion hatte dieses System aber keine Zukunft mehr und Sotronik erhielt den Auftrag ein neues Fernwirksystem aufzubauen.
Die wesentlichsten Anforderungen an dieses neue Fernwirksystem waren:

- Es muss an jedem Internetanschluss ohne manuelles Zutun zuverlässig funktionieren (auch bei sehr langsamen Internetanschlüssen, 24/7-Betrieb, plug&play)
- Es muss den aktuellen Security-Standards genügen
- Zusätzliche Installations- oder Hardwarekosten pro Brennstoffzellenheizgerät dürfen nicht entstehen
- Es muss mit einer sehr geringen "Daten-Grundlast" auskommen – somit also ein gutes Nutzdaten-verhältnis aufweisen

Die Technologie

Sotronik erstellte ein Konzept, das auf dem "SSL"-Kommunikationsstandard aufsetzt (HTTPS-Protokoll) und u.a. auch im "Homebanking"-Bereich Anwendung findet. Hierbei initiiert ein SSL-Client eine verschlüsselte Verbindung zu einem SSL-Server im Internet. Die Verbindung verwendet den Port 443, der bei Firewalls für ausgehende Verbindungen standardmässig offen ist (→ kein Eingriff in die Firewall-Konfiguration notwendig).
Konzeptidee: Hat man nun zwei solcher SSL-Clients (z.B. irgendein "Endgerät" und ein Web-Browser), kann man diese über eine zentrale "Datendrehscheibe" (Server) virtuell miteinander verbinden und erhält so eine gesicherte Kommunikation zwischen beiden Clients. Über die "Datendrehscheibe" können zudem Zugriffsregeln und Authentifizierungsmechanismen definiert werden.

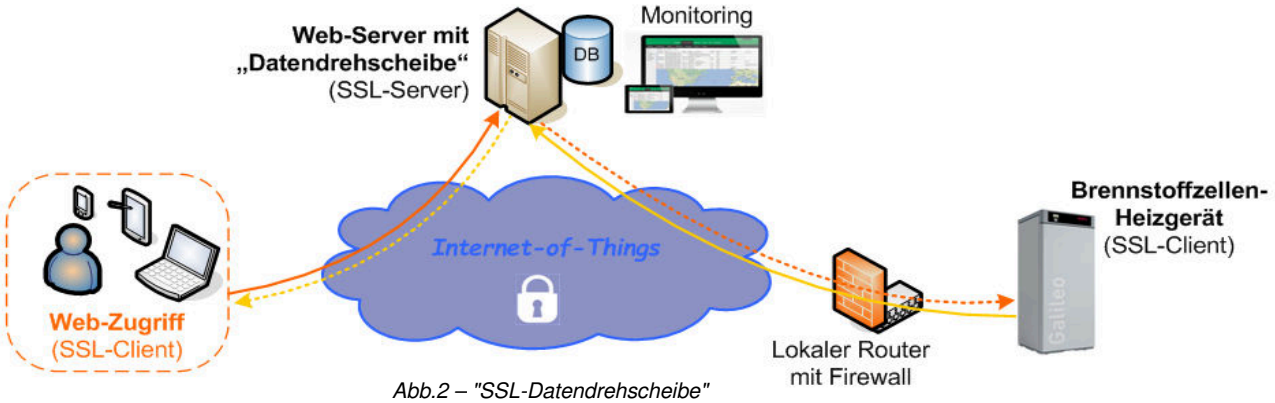

Abb.2 – "SSL-Datendrehscheibe"

Die Umsetzung

Das Brennstoffzellenheizgerät verfügt über eine Ethernet-Schnittstelle, die von einem Cortex-M4-Mikrocontroller betrieben wird. Sotronik erweiterte die in ANSI-C entwickelte Firmware um einen SSL-Client (C-Library-Implementation) und entwickelte einen Mechanismus, der zyklisch eine verschlüsselte HTTPS-Verbindung zu einem zentralen Web-Server von Hexis aufbaut.
Beim Verbindungsaufbau wird der Gerätestatus mit übermittelt und die Verbindung wieder getrennt, falls keine Fernzugriffsanforderung besteht. Besteht eine Anforderung, wird die Request-Zykluszeit für die Dauer des Fernzugriffs herabgesetzt und aktuelle Prozessdaten mit maximaler Transferrate an den Server übertragen. Der Server wiederum stellt diese empfangenen Daten dem anfragenden SSL-Client (z.B. Web-Browser) zur Verfügung. Es entsteht so ein "virtueller-Direkt-Fernzugriff", der performant ist und ein sehr gutes Übertragungs-/Nutzdatenverhältnis aufweist.
Als "Datendrehscheibe" dient eine MySQL-Datenbank, die nebst der Prozessdatenarchivierung auch das Zugriffsmanagement steuert. Über eine schlanke PHP-API auf dem "SSL-Server" werden alle Client-Anfragen, Authentifizierungsabläufe und die Erst-Registrierung der Clients automatisch geregelt. Fehlerzustände und auftretende Ereignisse werden erfasst und gemäss einer vordefinierten Alarmierungskette automatisch kommuniziert (per SMS und Email).

Das Fazit

Die Hexis AG betreibt nun ein zuverlässiges und kostenoptimiertes Fernwirksystem, über das sie in der Lage ist, ihren Kunden zusätzliche Dienstleistungen rund um den Komfort und den Betrieb ihrer Brennstoffzellen-heizgeräte anzubieten. Das Einverständnis der Endkunden vorausgesetzt, hat die Hexis AG auch zusätzlich die Möglichkeit, Langzeitdaten zum Betrieb der Systeme in realer Umgebung zentral zu erfassen und für zukünftige Entwicklungen auszuwerten.
Durch vorauseilende Ereignismeldungen, kann frühzeitig auf Betriebsstörungen reagiert und der Komfortbetrieb der Heizsysteme sichergestellt werden.
Ganz im Sinne von "Internet-of-Things" befriedigt die Hexis AG mit dieser Lösung auch Kundenansprüche bezüglich Smartphone-APP- und Web-Browser-Bedienung und ist durch den zentralen Web-Server auch für zukünftige Anforderungen an die Kommunikation und Vernetzung von Geräten im SmartHome-Bereich gerüstet.