# Application Note

extends your EnOcean by a new dimension

# myHomeControl®
# Schutz privater Daten

# Datendeklaration


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## Einleitung

**myHomeControl®** ist ein SmartHome-System. Es liegt in der Natur der Sache, dass das System mit persönlichen Daten der Bewohner operiert. Persönliche Daten sind z.B. Messwerte aber auch die Zustände der Installationsobjekte wie Lichter und Rollos.

Dieses Dokument beschreibt wie die persönlicher Daten in **myHomeControl®** geschützt werden. Es erklärt das Funktionsprinzip der Schutzfunktion und zeigt Gefahrenpotentiale auf, welche bei einer ungeeigneten Systemkonfiguration auftreten.

## Zusammenfassung

Generell kann das Smarthome-System **myHomeControl®** als sicher betrachtet werden.

Solange die in diesem Dokument gegebenen Ratschläge beachtet werden, ändert sich an der Sicherheit des Systems nichts auch, wenn das System erweitert wird.

## Gefahrenpotenzial

Was ist denn so gefährlich?

**myHomeControl®** speichert die aktuellen Zustände der Installationsobjekte sowie der Sensoren in einer Datenbank. Dies ist für die Steuerfunktion notwendig.

Diese Zustandsinformationen bilden persönliche Daten, da daraus Rückschlüsse auf das Verhalten der Anwender gezogen werden können.

Bei unsachgemässer Einrichtung des Systems besteht die Gefahr, dass Unberechtigte sich diese Daten aneignen.

Mit diesem Wissen lassen sich Schlüsse über das Verhalten der Bewohner ziehen wie:

- Zu welchen Zeiten steht das Gebäude leer?
- Wann pflegen die Bewohner zu Bett zu gehen?
- Vieles mehr …

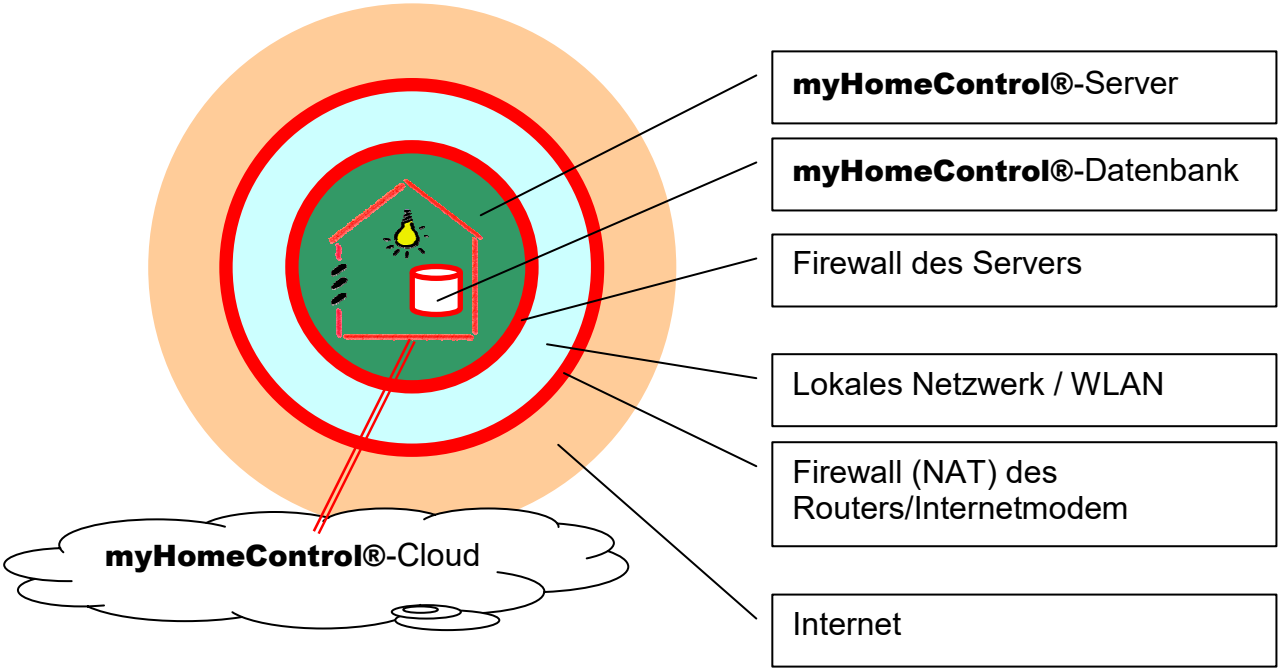

BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## Funktionsprinzip

Das Gebäude-Steuersystem **myHomeControl®** arbeitet auf einem lokalen Server. Dieser Server ist im Gebäude installiert und typischerweise mit dem lokalen Netzwerk verbunden.

## Hüllenmodel

Die datentechnische Situation des Servers kann man sich als Zwiebelschalen-Model vorstellen. Die verschienen Hüllen werden durch Schutzmechanismen (z.B. Firewalls) von einander abgeschirmt.




In jeder Hülle gelten andere Sicherheitsstandards:

### myHomeControl®-Server

Dieser Bereich wird durch die Firewall des Betriebssystems des Servers geschützt.

Die Systemzustände, welche auch persönliche Daten beinhalten, werden in einer verschlüsselten Datenbank gespeichert. Nur die **myHomeControl®**-Software ist authentifiziert die Daten zu lesen und zu schreiben.

Der Zugriff auf Dateien auf dem Server aus dem lokalen Netzwerk ist gesperrt.

Das Login in das Serverbetriebsystem ist passwortgeschützt.

### Lokales Netzwerk

Unter dem lokalen Netzwerk versteht man das gebäudeinterne Computer-Netzwerk. Hierzu gehört auch das Wireless-LAN. In diesem Netzwerk bewegen sich die privaten Geräte des Anwenders. Das lokale Netzwerk wird zur privaten Sphäre gezählt.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

Dieses Netzwerk wird einerseits durch die Firewall des Internet-Modems oder Routers geschützt (NAT). Der Router schützt den Datenzugriff aus dem Internet. Solange keine Ports (Portforwarding) geöffnet werden, ist das Eindringen aus dem Internet nicht möglich.

Wireless-LAN ist ebenfalls Teil des lokalen Netzwerks und muss mittels eines aktivierten Verschlüsselungsmechanismus gegen Eindringlinge geschützt werden.

### Internet

Das Internet ist ein öffentlicher Bereich in welchem sich jeder frei bewegen darf.

## Schutzkonzept

Die Schutzmechanismen zwischen den Hüllen verhindern unbefugtes Eindringen in die nächst tiefer gelegene Hülle. Die Schutzmechanismen erlauben jedoch den Datenzugriff in die umgebende Hülle.

Beispiele:

Die Firewall des Routers erlaubt den Teilnehmern des lokalen Netzers auf Webseiten im Internet zuzugreifen. Sie erlaubt jedoch keinen Zugriff auf die Teilnehmer vom Internet aus.

Die Firewall des Servers erlaubt dem Server z.B. Online-Wetterdaten im Internet zu lesen, jedoch keinen Zugriff auf Daten welche auf dem Server gespeichert sind. Weder aus dem lokalen Netzwerk noch aus dem Internet.

## Drittgeräte

Mit Drittgeräten sind in diesem Kontext Geräte gemeint, welche in das lokale Netzwerk des Anwenders eingebunden wurden. Beispiele hierfür sind: Kameras, Drucker, Audiosysteme, Lichtsteuersysteme, Haustechnik.

Einige diese Geräte ermöglichen den Zugang aus dem Internet. Typischerweise, wenn sie sich auch aus dem Internet bedienen oder auslesen lassen.

Problematik:

**Beeinträchtigung der Schutzmechanismen**

Es gibt Drittgeräte, welche die Konfiguration der Firewall im Router verändern z.B. indem sie ein Portforwarding einrichten. Dies schafft theoretisch die Möglichkeit, dass sich ein Eindringling auf betriesystemebene des Gerätes einwählt und sich somit im lokalen Netzwerk bewegen kann.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## myHomeControl®-Cloud

Die **myHomeControl®**-Cloud ist eine Dienstleistung von BootUp. Die **myHomeControl®**-Cloud dient als Vermittlungsstelle für verschiedene Dienste, welche **myHomeControl®**-Installationen optional benützen können. Die Verbindung zwischen **myHomeControl®**-Installation und **myHomeControl®**-Cloud ist nicht zwingend erforderlich. Sie wird nur in folgenden Fällen benötigt:

Beispiele hierfür sind:

- **Online-Wetterdaten**
  **myHomeControl®**-Installationen können Wetterdaten von der **myHomeControl®**-Cloud beziehen.
- **Alexa-Sprachsteuerung**
  Die **myHomeControl®**-Cloud vermittelt die Sprachbefehle zwischen Amazon und der **myHomeControl®**-Installation

Sinn der Vermittlung durch die **myHomeControl®**-Cloud ist es die **myHomeControl®**-Installationen datentechnisch abzuschirmen. Die Kommunikation zwischen den **myHomeControl®**-Installationen und der **myHomeControl®**-Cloud ist verschlüsselt und mit einer Authentifizierung ausgestattet. Die Kommunikation ist von der **myHomeControl®**-Installation getrieben und erfordert keine spezielle Konfiguration des Routers.

Die **myHomeControl®**-Cloud schirmt die **myHomeControl®**-Installationen gegenüber den benützten Internetdiensten ab.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## Kommunikationskanäle

Um den Datenaustausch zwischen dem **myHomeControl®**-Server und anderen Geräten zu ermöglichen müssen Kommunikationskanäle eingerichtet werden, z.B. für den Fernzugang von einem mobilen Gerät aus, muss ein entsprechender Kommunikationskanal geöffnet werden.

Es gibt Kommunikationskanäle unterschiedlicher Art. Sie unterscheiden sich:

- im Umfang der auszutauschenden Daten
- in der Art wie sie getrieben werden
- in der Art der Authentifizierung des Kommunikationspartners
- in der Art der Verschlüsselung der Daten

### Beurteilungskriterien

Im Folgenden werden für alle Kommunikationskanäle, welche **myHomeControl®** benutzt, die Gefahrensituation deklariert.

Folgende Kriterien gilt es zu beurteilen:

- Art der Kommunikation
  Wie erfolgt der Verbindungsaufbau? Welche Instanz initiiert den Verbindungsaufbau?
  Erfolgt eine Authentifizierung des Kommunikationspartners?
  Wie wird der Datenaustausch getrieben?
- Beeinträchtigung der Schutzvorrichtungen
  Werden die Einstellungen einer Firewall verändert?
  Wird eine Schutzfunktion beeinträchtigt?
- Art der kommunizierten Daten
  Werden private Daten ausgetauscht? Werden Daten ausgetauscht, welche Rückschlüsse über das Verhalten des Benutzers ermöglichen?

## Inselbetrieb (supersave)

**myHomeControl®** kann als Insel betrieben werden. In dieser Betriebsart benötigt **myHomeControl®** keinen Anschluss an das lokale Netzwerk. Es werden **keine** Kommunikationskanäle geöffnet.

Diese Betriebsart erfordert jedoch, dass der Server mit einem Touchscreen ausgestattet ist, da eine Bedienung von Fern nicht möglich ist. Diese Betriebsart verhindert jede Möglichkeit in den Server einzudringen.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

Typischerweise wird der **myHomeControl®**-Server mit dem lokalen Netzwerk verbunden um die Fernbedienung zu ermöglichen. Es werden folgende Kommunikationskanäle geöffnet:

## TeamViewer

Dieser Cloud basierte Dienst, ermöglicht es die Bedienoberfläche des **myHomeControl®** Servers auf Client-Geräten wie Computer, Tablets und Smartphones zu übertragen (Fernbedienung). Dabei spielt es keine Rolle ob sich der Client im lokalen Netzwerk oder im Internet befindet.

| | |
|---|---|
| Kommunikationsart: | Die Datenkommunikation ist vom TeamViewer-Client auf dem **myHomeControl®**-Server getrieben.<br>Die Datenkommunikation ist verschlüsselt und entspricht den aktuellen Sicherheitsstandards. Die Authentifizierung erfolgt über eine Kennung (ID) und ein Passwort. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | Private Daten: Systemzustände |

TeamViewer kann auf dem **myHomeControl®**-Server auch deaktiviert werden.

## VNC

Dieser Dienst, ermöglicht es die Bedienoberfläche des **myHomeControl®**-Servers auf Client-Geräten wie Computer, Tablets und Smartphones zu übertragen. Dieser Dienst arbeitet lokal. Der VNC-Server Dienst ist auf dem **myHomeControl®**-Server installiert und wartet auf Anfragen von einem VNC-Client. Der VNC-Server öffnet einen Port, über welchen er aus dem lokalen Netzwerk angesprochen werden kann.

Theoretisch besteht die Möglichkeit, dass über diesen Port der VNC-Server ausgehebelt wird um in den **myHomeControl®**-Server einzudringen.

Dieser Dienst ist nur für das lokale Netzwerk geeignet.

| | |
|---|---|
| Kommunikationsart: | Die Datenkommunikation ist verschlüsselt und entspricht den aktuellen Sicherheitsstandards. Die Authentifizierung erfolgt über ein Passwort. |
| Beeinträchtigung der Schutzvorrichtungen: | In der Firewall des **myHomeControl®**-Servers wird Port 5900 geöffnet |
| Dateninhalte: | Private Daten: Systemzustände |

Der VNC-Server kann auf dem **myHomeControl®**-Server auch deaktiviert werden.

## CompactWEB

Dieser Dienst ermöglicht es über einen Webbrowser Systemzustände abzufragen und zu ändern (schalten, dimmen, etc.). **myHomeControl®** betreibt lokal auf dem **myHomeControl®**-


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

Server einen Web-Server, welcher die entsprechenden Webseiten erstellt und zum Download anbietet.

Dieser Dienst ist nur für das lokale Netzwerk geeignet.

| | |
|---|---|
| Kommunikationsart: | Die Datenkommunikation basiert auf HTTP und ist nicht verschlüsselt. |
| Beeinträchtigung der Schutzvorrichtungen: | In der Firewall des **myHomeControl®**-Servers wird Port 80 geöffnet |
| Dateninhalte: | Private Daten: Systemzustände |

CompactWEB kann auf dem **myHomeControl®**-Server auch deaktiviert werden.

## Online Wetterdaten

Dieser Dienst, ermöglicht es **myHomeControl®** online-Wetterdaten zu lesen. Dies ist eine sinnvolle Ergänzung, wenn keine lokale Wetterstation vorhanden ist.

Für die Anforderung der Wetterdaten, wird der Gebäudestandort und die Kennung des **myHomeControl®**-Servers zur **myHomeControl®**-Cloud übertragen. Die Datenabfrage zwischen **myHomeControl®**-Cloud und Wetterdienst ist anonymisiert.

| | |
|---|---|
| Kommunikationsart: | Es wird eine gesicherte, verschlüsselte Verbindung zur **myHomeControl®**-Cloud benutzt. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | → Gebäudestandort und die Kennung des **myHomeControl®**-Servers<br>← Wetterdaten |

Ist eine lokale Wetterstation eingebunden, so entfällt die Abfrage der Online-Wetterdaten.

## Hue-Leuchten

Um Philips-Hue Leuchten mit myHomeControl zu steuern, erfolgt ein Datenaustauch zwischen dem **myHomeControl®**-Server und der Hue-Bridge.

Die Datenkommunikation ist vom Server getrieben. Es sind keine Konfigurations-massnahmen bei den Firewalls erforderlich, welche die Schutzfunktion einschränken.

| | |
|---|---|
| Kommunikationsart: | Die Kommunikation erfolgt im lokalen Netzwerk via HTTP und ist nicht verschlüsselt. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | Zustandsinformationen der Hue-Leuchten |


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

Die Hue-Bridge ist ein intelligentes Gerät mit Linux-Betriebsystem. Das Gerät wird über die Hue-App regelmässig mit Updates versorgt. Der Anwender hat keine Möglichkeit das Betriebssystem-Passwort zu verändern.
Daher besteht bei diesem Gerät die Gefahr, dass eine Einwahl von Fern erfolgen kann. Der Eindringling befindet sich dann auf Betriebssystemebene und hat Zugang zum lokalen Netzwerk!

## Alexa Sprachsteuerung

Dieser Dienst, ermöglicht es **myHomeControl®** mit dem Alexa-Sprachdienst von Amazon zu verknüpfen. Der Datenaustausch erfolgt über die **myHomeControl®**-Cloud.

Für die Anforderung des nächsten Schaltkommandos, wird die Kennung des **myHomeControl®**-Servers und die Email-Adresse des Amazon-Kontos zur **myHomeControl®**-Cloud übertragen. Der Datenaustausch zwischen **myHomeControl®**-Cloud und Alexa-Sparchdienst ist anonymisiert.

Bei der Paarung bzw. wenn Alexa die verfügbaren Geräte einliest, übermittelt der **myHomeControl®**-Server eine Liste der Steuerungsobjekte mit ihren Namen an den Sprachdienst. Während des normalen Betriebs werden Zustandsinformationen an den Sprachdienst nur übermittelt, wenn dies im myHomeControl-Projekt aktiviert wurde.

| | |
|---|---|
| Kommunikationsart: | Es wird eine gesicherte, verschlüsselte Verbindung zur **myHomeControl®**-Cloud benutzt. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | →Kennung des **myHomeControl®**-Servers und die Email-Adresse des Amazon-Kontos<br>←Steuerkommando |

Die eigentliche Spracherkennung erfolgt jedoch auf einem Server in Amerika oder Irland. Wird eines der Kennworte „Alexa, Amazon, Computer, ..“ genannt, so schaltet sich die Spracherkennung aktiv und das Gespräch wird zu genanntem Server übertragen.

## Apple-HomeKit

Dieser Dienst, ermöglicht es **myHomeControl®** mit dem HomeKit von Apple zu verknüpfen.

Der Datenaustausch erfolgt zwischen dem **myHomeControl®**-Server und den Apple-Geräten, welche unter der Apple-ID angemeldet sind mit welcher der **myHomeControl®**-Server gepaart wurde.

| | |
|---|---|
| Kommunikationsart: | Die Sicherung der Datenkommunikation wird durch Apple vorgegeben und kann als sicher betrachtet werden. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | Private Daten: Systemzustände |


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

Die eigentliche Spracherkennung erfolgt jedoch auf einem Server in Amerika. Wird das Kennwort „Hi Siri“ genannt, so schaltet sich die Spracherkennung aktiv und das Gespräch wird zu genanntem Server übertragen.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## Kameras

Via JPEG-, MJPEG oder RTSP-Stream können Kameras in **myHomeControl®** eingebunden werden. Der Kommunikationskanal für die Bildübertragung wird vom **myHomeControl®**-Server geöffnet.

Dieser Dienst ist nur für das lokale Netzwerk geeignet.

| | |
|---|---|
| Kommunikationsart: | nicht verschlüsselt. |
| Beeinträchtigung der Schutzvorrichtungen: | Keine |
| Dateninhalte: | Private Daten: Kamerabilder |

## Modbus-TCP

Dieser Dienst wird für den Datenaustausch mit der Haustechnik (Heizung, Lüftung, PV) benutzt. Die Kommunikation wird von **myHomeControl®** getrieben.

Dieser Dienst ist nur für das lokale Netzwerk geeignet.

| | |
|---|---|
| Kommunikationsart: | Das ModbusTCP-Protokoll ist weder authentifiziert noch verschlüsselt. |
| Beeinträchtigung der Schutzvorrichtungen: | keine |
| Dateninhalte: | Private Daten: Systemzustände der Haustechnik |


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch

## Quintessenz

Die SmartHome Software **myHomeControl®** verwendet eine sichere Architektur. Die Wahrscheinlichkeit, dass Kriminelle über die Funk-Schnittstelle oder das lokale Netzwerk eindringen ist praktisch nicht vorhanden. Die Wirksamkeit der Sicherheitsmaßnahmen und Verfahren setzt voraus, dass sichere Passwörter Verwendung finden. Die Anwendung **myHomeControl®** kann Status- und Gefahrenmeldungen an Geräte im Internet senden, ohne selbst offen für das Internet zu sein.

Bei der Einbindung von Drittgeräten ins lokale Netzwerk ist steht's Vorsicht geboten. Diese Geräte öffnen oft Verbindungen in Cloud-Anwendungen, welche ev. das Eindringen ins lokale Netzwerk ermöglichen.


BootUp GmbH | Sonnenbergstrasse 23 | CH-5236 Remigen | Schweiz | Tel: +41 56 284 09 21 | Fax: +41 56 284 09 22
© 2017 | Irrtümer und technische Änderung vorbehalten. | www.BootUp.ch | www.myHomeControl.ch |info@bootup.ch