HomeMatic Know-how

Teil 21: Homematic Sicherheit

In unserer Reihe „Homematic Know-how“ zeigen wir anhand von kleinen Detaillösungen, wie man bestimmte Aufgaben im Homematic System konkret lösen kann. Dies soll insbesondere Homematic Einsteigern helfen, die Einsatz- und Programmiermöglichkeiten besser zu nutzen. In dieser Ausgabe zeigen wir, welche Möglichkeiten es gibt, ein Homematic System möglichst sicher zu betreiben.

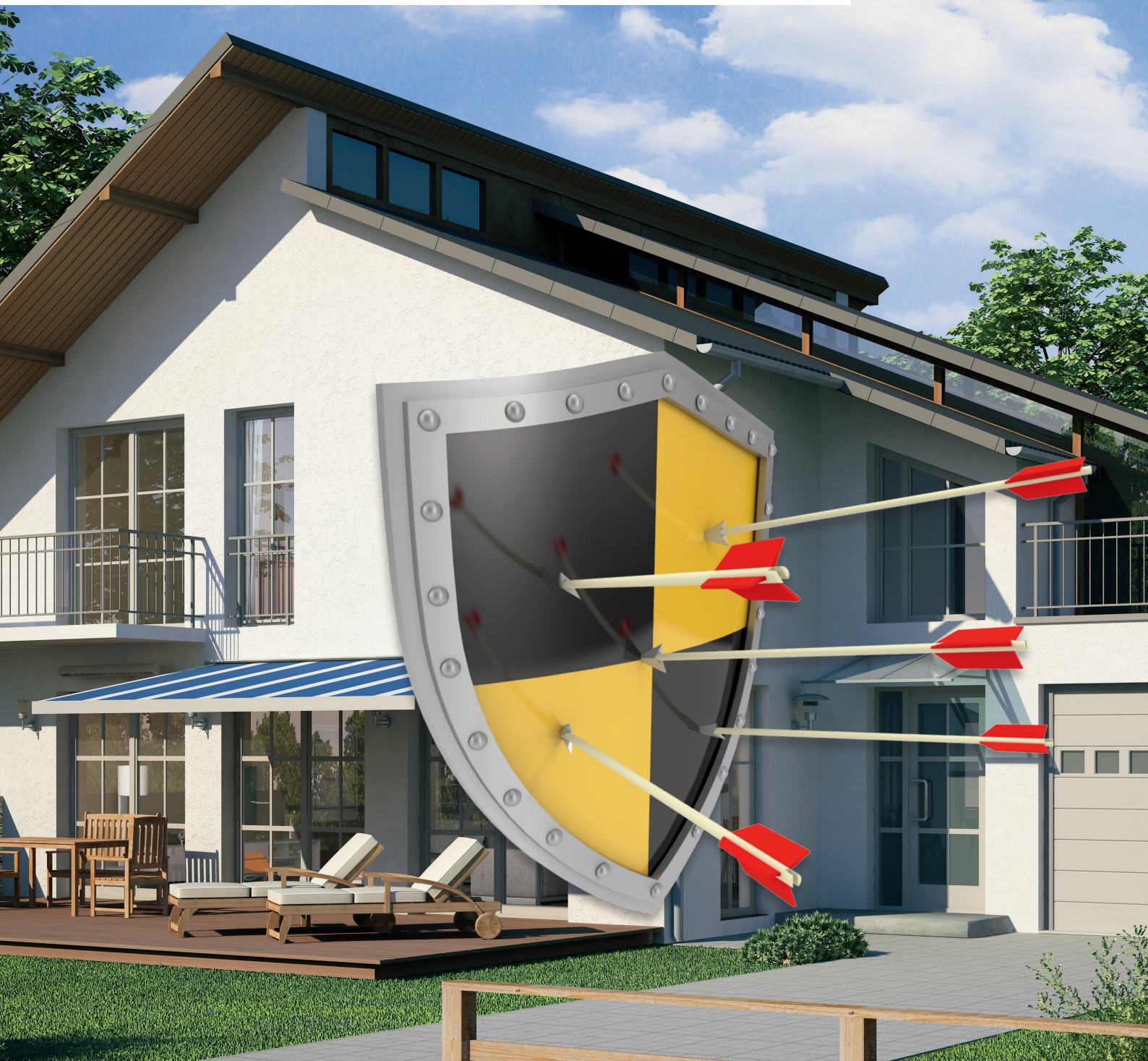

Bild 1: WebUI-Startseite mit dem rechts angezeigten Kennwort-Hinweis

Fragen zur Sicherheit eines Smart Home Systems kommen gerade in der heutigen „Immer-und-alles-online-Zeit" sehr häufig auf. Nicht zuletzt auch, weil die Medien dieses immer wieder thematisieren, wobei allerdings die entsprechenden Lösungsansätze zur Optimierung der Sicherheit auf der Strecke bleiben.

Im Folgenden werden die wichtigsten Punkte in Bezug auf das Homematic System und der Verwendung der Homematic Zentrale CCU2 im lokalen Netzwerk sowie beim Fernzugriff und auch die gesicherte Funkkommunikation näher erläutert.

Lokaler Netzwerkzugriff auf die Homematic Zentrale

Bereits bei der Ersteinrichtung der CCU2 ist eine Verbindung mit dem heimischen Netzwerk erforderlich, um die aktuelle Firmware-Version einzuspielen sowie das System bequem per PC-Browser einrichten und programmieren zu können. Die folgenden Punkte sollten direkt bei der Einrichtung des Systems beachtet und entsprechend konfiguriert werden, um Unbefugten den Zugriff auf das System zu verwehren.

Gerade in Bezug auf das lokale Netzwerk ist allerdings auch anzumerken, dass in erster Linie der Betreiber des Netzwerks die Fäden selbst in der Hand hält. Man sollte sich daher zunächst einmal Gedanken machen, wer ggf. auch aus dem privaten Umfeld Zugang zum lokalen Netzwerk hat. Nahezu jeder besitzt heutzutage ein Smartphone und möchte gerne immer und überall surfen. Daher wird das WLAN-Passwort zum privaten Netzwerk schnell mal weitergereicht, wodurch dann bereits ein Zugriff auf alle Netzwerkgeräte möglich ist. Es empfiehlt sich, sofern der WLAN-Router es zulässt, für solche Zwecke ein WLAN-Gast-Netzwerk einzurichten, welches lediglich den Zugriff auf das Internet bietet, aber den Zugriff auf lokale Netzwerkgeräte verwehrt.

1. Benutzerpasswort einrichten

Nach dem Einspielen der aktuellen Firmware-Version der CCU2 wird man auf der Startseite der Homematic WebUI freundlich mit einem roten Hinweis „Kein Kennwort gesetzt" begrüßt (siehe Bild 1).

Zur Einrichtung des persönlichen Benutzerkennworts fährt man mit dem Mauszeiger über den Button „Einstellungen" und klickt anschlie-

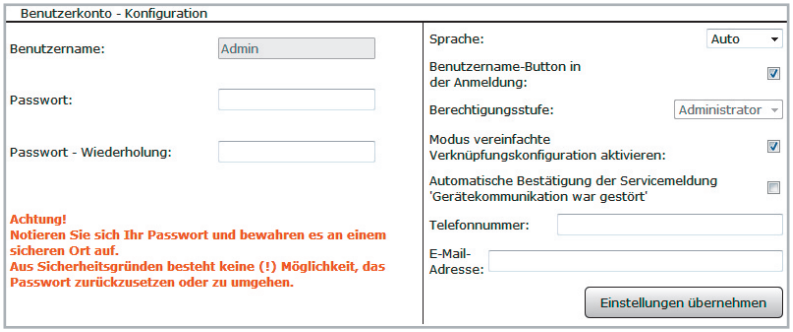

Bild 2: Eingabemaske für das Benutzerpasswort

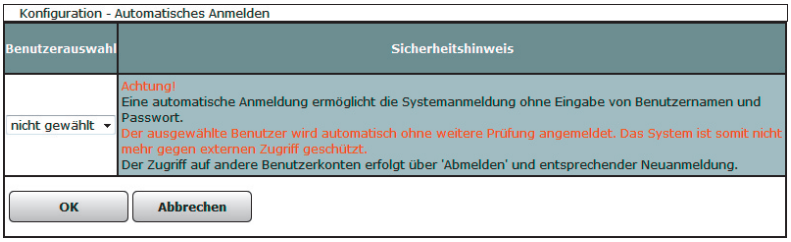

Bild 3: Einstellung für das automatische Anmelden an der WebUI

Bild 4: Nach abgeschlossener Programmierung sollte die WebUI immer per Klick auf „Abmelden" verlassen werden.

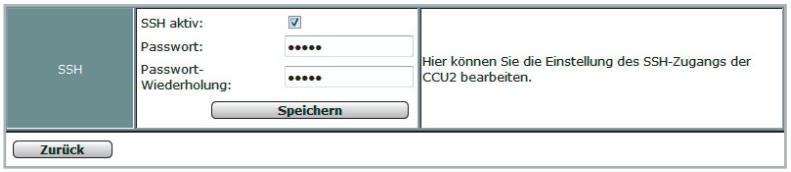

Bild 5: Eingabefelder für das persönliche SSH-Passwort

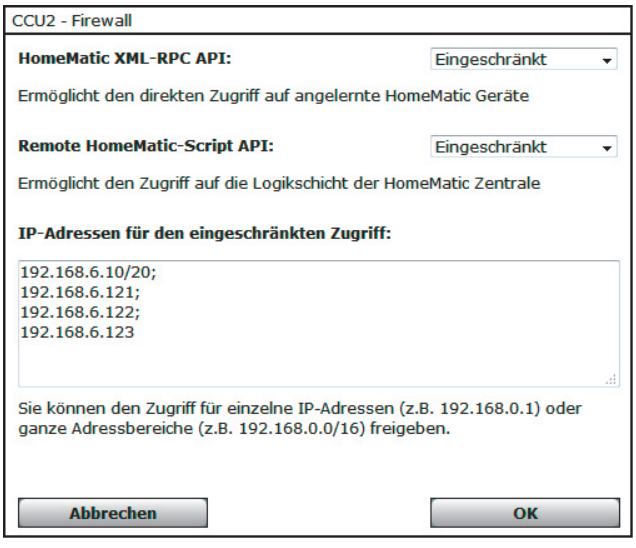

Bild 6: Zeigt beispielhaft eine Firewall-Konfiguration. Die erste Zeile (192.168.6.10/20;) stellt einen Adressbereich da. Darunter drei Einzeladressen. Wichtig: In der letzten Zeile darf am Ende kein Semikolon stehen.

ßend auf „Benutzerverwaltung". Im folgenden Fenster erscheinen alle angelegten Benutzer, für welche man jeweils durch einen Klick auf „Bearbeiten" ein persönliches Benutzerkennwort festlegen kann (siehe Bild 2).

Möchte man zudem auch den auf der Anmeldeseite angezeigten Button mit dem Benutzernamen entfernen, kann der Haken für „Benutzername-Button in der Anmeldung" entfernt werden.

Das gesetzte Passwort wird nach einem Klick auf „Einstellungen übernehmen" gespeichert und bei jedem Einloggen auf der WebUI abgefragt.

Sofern weitere Nutzer das System über die WebUI lediglich bedienen sollen, lassen sich über die Benutzerverwaltung auch reine Benutzer- oder auch Gastkonten einrichten.

2. Automatisches Anmelden deaktivieren

Das automatische Anmelden auf der WebUI ist zwar sehr bequem, da einem die vielleicht lästige Eingabe der Zugangsdaten erspart bleibt. Man sollte dabei jedoch bedenken, dass jede Person, die Zugriff auf das lokale Netzwerk hat, einfach durch die Eingabe der Zentralen-IP-Adresse direkt und ohne Eingabe von Zugangsdaten auf die WebUI gelangt und sich hier frei bewegen kann.

Um das automatische Anmelden zu deaktivieren, klickt man in der Übersicht der Benutzerverwaltung unten auf den Button „Automatisches Anmelden", wählt links in der Auswahl „nicht gewählt" und speichert mit einem Klick auf „OK" ab (siehe Bild 3).

3. Von der WebUI abmelden

Sofern man seine zu erledigenden Arbeiten auf der WebUI abgeschlossen hat, sollte immer eine saubere Abmeldung erfolgen. Hierdurch wird nicht nur die aktuelle Konfigurationssitzung abgespeichert, sondern auch die geöffnete Sitzungs-ID geschlossen (siehe Bild 4).

4. SSH-/SFTP-Zugriff

Ein „normaler" Heimanwender wird den Konsolen- oder Dateisystem-Zugriff der Zentrale vermutlich weniger nutzen. Für fortgeschrittene Anwender oder gar Entwickler von Homematic Zusatzsoftware ist diese Zugriffsmöglichkeit unerlässlich.

Der SSH-Zugriff (Secure Shell) erfolgt über den Netzwerk-Port 22 und ermöglicht es dem Nutzer, über ein Konsolenprogramm wie z. B. Putty Shell-Befehle auf bzw. über die CCU auszuführen.

Des Weiteren kann mit SFTP-Programmen wie z. B. WinSCP auf die Dateisystemebene zugegriffen werden, wodurch das Kopieren/Erstellen/Ändern oder auch das Löschen von Dateien/Ordnern möglich ist.

Ab der Firmware Version 2.7.8 ist der SSH-Zugriff nicht mehr werkseitig aktiv, dieser muss vom Nutzer durch das Setzen eines Passworts zunächst aktiviert werden, das ursprüngliche Standard-Passwort ist nicht mehr gültig.

Um SSH zu aktivieren, ist unter „Einstellungen → Systemsteuerung → Sicherheit" ein Haken für „SSH aktiv" zu setzen, ebenso ist die Eingabe eines Passworts erforderlich (siehe Bild 5).

5. Firewall konfigurieren

In der Zentralen-Firmware-Version 2.27.x und neuer ist die CCU-Firewall optimiert und automatisch aktiviert. Die Firewall ermöglicht den Netzwerkzugriff auf die XML-RPC-API-Schnittstelle sowie die Einschränkung der Remote-Script-API-Schnittstelle.
Über die XML-RPC-API-Schnittstelle kann auf einzelne Geräte zugegriffen werden, die Remote-Script-API-Schnittstelle ermöglicht den Zugriff auf Räume, Gewerke und Programme. Die Firewall schränkt allerdings nicht den Zugriff auf den Webserver (die WebUI) der Zentrale ein.

In der WebUI werden hierzu unter „Einstellungen → Systemsteuerung → Firewall konfigurieren" nur die Netzwerkgeräte eingetragen, welche tatsächlich mit der Zentrale kommunizieren sollen bzw. müssen.

Um den Netzwerkgeräten den Zugriff auf diese Schnittstellen zu gewähren, ist die Eingabe der Geräte-IP-Adressen bzw. Adressbereiche erforderlich. Damit der IP-Adressen-Filter vollständig wirksam wird, sollten die beiden Schnittstellen „HomeMatic XML-RPC API" sowie „Remote HomeMatic-Script API" auf „Eingeschränkt" eingestellt werden (siehe Bild 6).

ACHTUNG: Sofern man diese Einstellung getätigt hat, muss einem bewusst sein, dass der Zugriff ggf. durch fehlerhafte Konfiguration oder bei Änderungen der Netzwerkstruktur (z. B. Router-Wechsel) nicht mehr von allen Netzwerkgeräten bzw. den verwendeten Software- oder App-Lösungen möglich ist.

In die Filterliste sollten für den bestmöglichen Schutz alle Geräte-IP-Adressen eingetragen werden, welche auf die Homematic Zentrale zugreifen müssen.

Dies sind in der Regel folgende Geräte:

- Computer (sofern Programme Zugriff benötigen: z. B. mediola NEO, contronics Homeputer)
- Smartphones/Tablets (welche per App Zugriff erhalten sollen)
- Fernzugriff per meine-homematic/CloudMatic, folgender Eintrag erforderlich: 10.192.0.0/12;
- Drittanbieter-Systeme bzw. Software (z. B. Openhab, FHEM, ioBroker, IP-Symcon)

Fernzugriff auf die Homematic Zentrale

Im Folgenden wird erläutert, welche Zugriffsmöglichkeiten zur Steuerung des Homematic Systems aus der Ferne bestehen, was zu beachten ist und welche Vor- bzw. Nachteile diese Möglichkeiten haben.

Sofern man keinen Fernzugriff benötigt oder Bedenken hat, das System im Netzwerk zu betreiben, ist es nicht erforderlich, eine der folgenden Zugriffsmöglichkeiten einzurichten.

Nur bei einem eingerichteten Fernzugriff ist auch der Zugriff aus dem Internet auf die CCU2 möglich.

Allerdings kann die Zentrale, sofern sie per Netzwerkkabel mit einem Internet-Router verbunden ist, Informationen abrufen bzw. senden. Dies sind z. B. Informationen über neue Firmware-Updates sowie der Zeitabgleich mit dem NPT-Zeitserver. Zudem können so z. B. mittels Zusatzsoftware oder per Skript auch Nachrichten (Mail/Push) versendet werden.

1. Port-Weiterleitung (Port Forwarding)

Von der Einrichtung einer Port-Weiterleitung ist strickt abzuraten!

Um per Port-Weiterleitung auf das System Zugriff zu erhalten, ist es erforderlich, die Ports der Homematic Zentrale, welche zunächst nur im internen Netzwerk zugänglich sind, über die Konfiguration im Internet-Router auch für den externen Zugriff, also aus dem Internet, zugänglich zu machen. Dies birgt ein extrem hohes Risiko, dass ggf. existierende oder auch aktuell noch unbekannte Sicherheitslücken der Zentrale für einen unbefugten Zugriff missbraucht werden könnten.

Aus diesem Grund wird hier nicht näher auf die dafür notwendige Einrichtung eingegangen.

2. VPN-Tunnel

VPN (Virtual Private Network) bzw. der VPN-Tunnel gilt als eine der sichersten Fernzugriffsmöglichkeiten. Bei einer VPN-Verbindung wird ein gesicherter, AES-verschlüsselter Tunnel zwischen einem mobilen Endgerät (z. B. Smartphone, Tablet, PC) und dem lokalen Heimnetzwerk hergestellt. Hierzu wird ein DDNS-Dienst benötigt, damit der Fernzugriff, auch bei den in Deutschland üblichen privaten DSL-Anschlüssen, mit wechselnder öffentlicher IP-Adresse jederzeit möglich ist. Diese Verbindung bietet zudem den Vorteil, dass nicht nur auf die Homematic Zentrale, sondern auch auf alle anderen im heimischen Netzwerk befindlichen Geräte zugegriffen werden kann.

Als eventuelle Nachteile kann man die für technische Laien ggf. komplex erscheinende Einrichtung sowie die bei gewünschtem Zugriff zunächst aufzubauende Verbindung aufführen.

Aufgrund der vielen verschiedenen DDNS-Anbieter und Internet-Router kann innerhalb der kostenlosen Technischen Kundenberatung von ELV kein Support zu dieser Einrichtung erfolgen. Allerdings findet man im ELV Shop unter dem Webcode #60063 hierzu eine Musteranleitung, welche eine solche Einrichtung erläutert.

3. Reverse Proxy

Die Verbindung über einen Reverse Proxy bietet sich als durchaus interessante Alternative zum VPN-Tunnel an. Allerdings ist die Einrichtung im Vergleich zum VPN-Tunnel noch komplexer und erfordert eine zusätzliche Hardware, auf welcher der Reverse-Proxy-Server aufgesetzt wird.

Warum sollte man überhaupt diesen Aufwand betreiben?

- Das vor dem Zugriff eines VPN-Tunnels erforderliche Aufbauen der Verbindung entfällt.
- Ermöglicht wie beim VPN-Tunnel nicht nur den Zugriff auf die Homematic Zentrale.
- Man vermeidet Cloud-Dienste und somit Netzwerk-Verbindungen, welche zum eigenen Netzwerk geöffnet werden.
- Apps können sich einfach wie beim VPN-Tunnel über eine IP-Adresse intern wie extern verbinden.
- Der Reverse-Proxy-Server lässt sich auf unterschiedlicher Hardware sowie vielen Betriebssystemen installieren.

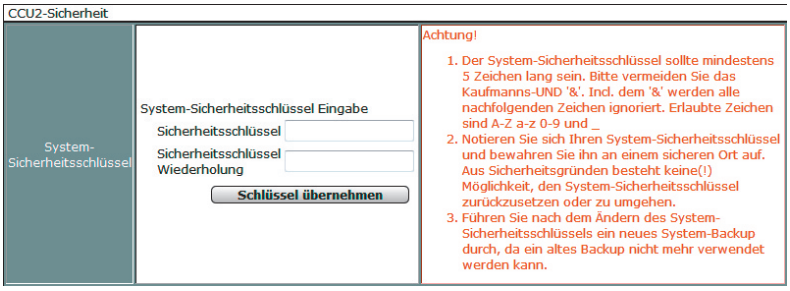

Bild 7: Eingabefelder für den persönlichen Systemsicherheitsschlüssel

Allerdings sind bei dieser Zugriffsmöglichkeit auch folgende Punkte zu berücksichtigen:

- Der Reverse Proxy sollte zwingend eine sichere Authentifizierung (Benutzername/Passwort) vornehmen, sowie eine per HTTPS gesichert Verbindung aufbauen.
- Da für einen Reverse Proxy meist OpenSource Software verwendet wird, muss diese ständig vom Nutzer aktualisiert werden. In OpenSource Software werden regelmäßig Sicherheitslücken entdeckt und meist auch zügig geschlossen.

Die Einrichtung eines Reverse-Proxy-Servers für einen sicheren Fernzugriff auf die Homematic Zentrale wird z. B. unter [1] erläutert.

4. Fernzugriff über eine Cloud-Lösung

Für Nutzer, die sich nicht mit der Einrichtung eines VPN-Tunnels oder Reverse-Proxy-Servers beschäftigen wollen, sind die Partnerlösungen von CloudMatic (meine-homematic.de) oder Orbylon empfehlenswert und einfach einzurichten.

Diese Partner bieten ähnlich wie beim VPN-Tunnel eine gesicherte Verbindung, welche auch ohne Netzwerktechnik-Kenntnisse einzurichten ist. Der Unterschied zum eigens eingerichteten VPN-Tunnel ist allerdings, dass diese getunnelte Verbindung nicht direkt zwischen dem Endgerät (Smartphone, Tablet, PC) und dem Heimnetzwerk, sondern zwischen der Zentrale und dem Cloud-Server des Partners aufgebaut wird. Das Endgerät muss sich somit zunächst mit dem Cloud-Server des Partners verbinden und erhält erst nach entsprechender Authentifizierung den Zugriff über die getunnelte Verbindung auf die Zentrale.

Vorteil ist, wie bereits erwähnt, die einfache Einrichtung, zudem sind nahezu alle Homematic Apps bereits für die Verwendung mit dem Dienst von CloudMatic (meine-homematic.de) vorbereitet. Ausnahme ist hier Orbylon, dieser Partner bringt neben dem Fernzugriff auch seine eigene App mit. Des Weiteren umfassen diese Lösungen weitere Funktionen. Welche dies im Einzelnen sind, kann unter [2] bzw. [3] nachgelesen werden.

Als eventuelle Nachteile kann man ggf. die folgenden Punkte auslegen: Trotz der mehrjährigen Partnerschaft zwischen diesen Anbietern und dem Hersteller eQ-3 sowie der ständigen Wartung und Pflege der für den Dienst erforderlichen Infrastruktur läuft die Verbindung, auch wenn diese verschlüsselt ist, über einen Dritten. Des Weiteren sind beide Lösungen nicht kostenfrei nutzbar, allerdings sind die anfallenden Kosten mit ca. 24 Euro im Jahr unter Berücksichtigung der vom Anbieter notwendigen Pflege sowie der enthaltenen Mehrwertdienste durchaus überschaubar und auch berechtigt.

Gesicherte Funkkommunikation

Neben den bereits behandelten netzwerkseitigen Sicherheitsthemen besteht im Homematic System auch die Möglichkeit, die Funkkommunikation zwischen der Homematic Zentrale und den Geräten zusätzlich zu verschlüsseln. Hierfür wird das symmetrische Kryptoverfahren AES 128 bit (Advanced Encryption Standard) verwendet.

Werkseitig sind alle Homematic Geräte bereits mit einem systemweiten Standard-Sicherheitsschlüssel versehen, sodass zumindest ab Werk alle sicherheitsrelevanten Geräte wie z. B. KeyMatic, WinMatic, Alarmsensoren und weitere Sender die gesicherte Verbindung nutzen.

Wie bei anderen Netzgeräten mit werksseitigen Passwörtern bzw. Schlüsseln auch (z. B. WLAN-Router) sollte der Schlüssel für die Funkkommunikation individuell gesetzt werden.

Folgend wird erläutert, wie dieser persönliche Schlüssel gesetzt wird, was generell bei der Verwendung zu beachten ist und welche Vor- bzw. Nachteile dieser ggf. haben kann.

1. Persönlicher Systemsicherheitsschlüssel

Bevor ein persönlicher Systemsicherheitsschlüssel eingetragen bzw. eine weitere Änderung des bereits gesetzten Schlüssels vorgenommen wird, sollte immer ein System-Backup erstellt werden. Es empfiehlt sich, diese Backup-Datei entsprechend umzubenennen, damit man bei ggf. auftretenden Problemen noch weiß, welche Sicherung der Systemkonfiguration ohne Schlüssel bzw. mit einem alten Schlüssel verwendet wurde. Die Vergabe eines persönlichen Systemsicherheitsschlüssels und damit das Überschreiben des Standardschlüssels wird in der WebUI unter „Einstellungen → Systemsteuerung → Sicherheit → System-Sicherheitsschlüssel" durchgeführt (siehe Bild 7).

ACHTUNG: Den in der WebUI nebenstehenden und rot markierten Hinweisen sowie den hier beschriebenen sollte der Nutzer in jedem Fall Beachtung schenken, um nachfolgende Probleme zu vermeiden.

Nachdem der persönliche Systemsicherheitsschlüssel eingetragen wurde, sind die folgenden Punkte zwingend zu beachten:

- Der neu gesetzte Systemsicherheitsschlüssel muss von der Zentrale an alle bereits angelernten Geräte übertragen werden. Daher muss nach einer Schlüsseländerung zwingend in der WebUI unter Servicemeldungen kontrolliert werden, für welche Geräte noch „Konfigurationsdaten stehen zur Übertragung an" gemeldet wird (siehe Bild 8). Werden diese Daten und somit der Schlüssel nicht an die Geräte übertragen, kann dies zur Folge

Erste Meldung Datum/Zeit	Letzte Meldung Datum/Zeit	Name	Bild	Seriennummer	Gewerk	Raum	Letzte Änderung	Servicemeldung	Aktion
		Filter		Filter	Filter	Filter		Filter	
18.04.2017 18:33:11	18.04.2017 18:33:11	Handsender KeyMatic:0		NEQ0683293:0			18.04.2017 18:33:11	Konfigurationsdaten stehen zur Übertragung an	Bestätigen

Bild 8: Noch zur Übertragung anstehende Konfigurationsdaten, welche durch kurze Betätigung der Config-Taste am Gerät übernommen werden müssen

Name	Typenbezeichnung	Bild	Bezeichnung	Seriennummer	Interface/ Kategorie	Übertragungsmodus	Gewerke	Räume				Aktionen
Filter	Filter		Filter	Filter	Filter	Filter	Filter	Filter				
Handsender KeyMatic	HM-RC-Key4-2		HM-RC-Key4-2	NEQ0683293	BidCos-RF	Gesichert	Taster		☑	☑	☐	Einstellen Löschen Direkte Programme
− Handsender KeyMatic:1 Handsender KeyMatic:2	HM-RC-Key4-2		HM-RC-Key4-2	NEQ0683293:1 NEQ0683293:2	Sender	Gesichert	Taster		☑	☑	☐	Einstellen Direkte Programme
Handsender KeyMatic:1 Tasterkanal	HM-RC-Key4-2		HM-RC-Key4-2	NEQ0683293:1	Sender	Gesichert	Taster		☑	☑	☐	Einstellen Direkte Programme
Handsender KeyMatic:2 Tasterkanal	HM-RC-Key4-2		HM-RC-Key4-2	NEQ0683293:2	Sender	Gesichert	Taster		☑	☑	☐	Einstellen Direkte Programme

Bild 9: Beispiel für ein Gerät mit seinen einzelnen Kanälen

haben, dass diese nicht mehr mit der Zentrale kommunizieren bzw. nach mehrfachem Schlüsselwechsel oder gar dem Verlust des Schlüssels sich nicht mehr in den Werkszustand versetzen lassen bzw. nicht mehr angelernt werden können.

- Für alle netzspannungsversorgten Geräte wird die Übertragung des Schlüssels, sofern die Geräte erreichbar sind, automatisch und sofort durchgeführt.
- Für batteriebetriebene Geräte gilt dies nur teilweise. Geräte wie z. B. KeyMatic, Heizkörper- sowie Wandthermostaten, welche nach dem Burst-Empfängerverfahren arbeiten, bekommen den neuen Schlüssel in der Regel auch direkt mitgeteilt.
- Für alle anderen batteriebetriebenen Sensoren wie z. B. Bewegungsmelder, Fensterkontakte sowie Wand- und Handsender, welche aus Energiespargründen nur bei einer Betätigung der Config-Taste bzw. ihrer zyklischen Statusmeldung oder bei Auslösung mit der Zentrale kommunizieren, ist es besonders wichtig, die Servicemeldungen in der WebUI zu beachten. Die ausstehenden Konfigurationsdaten und somit der neue Schlüssel werden wie in der Geräte-Bedienungsanleitung beschrieben nach einer kurzen Betätigung der Config-Taste übertragen (siehe Bild 8).
- Die Übertragung der noch ausstehenden Konfigurationsdaten sollte Gerät für Gerät erfolgen.

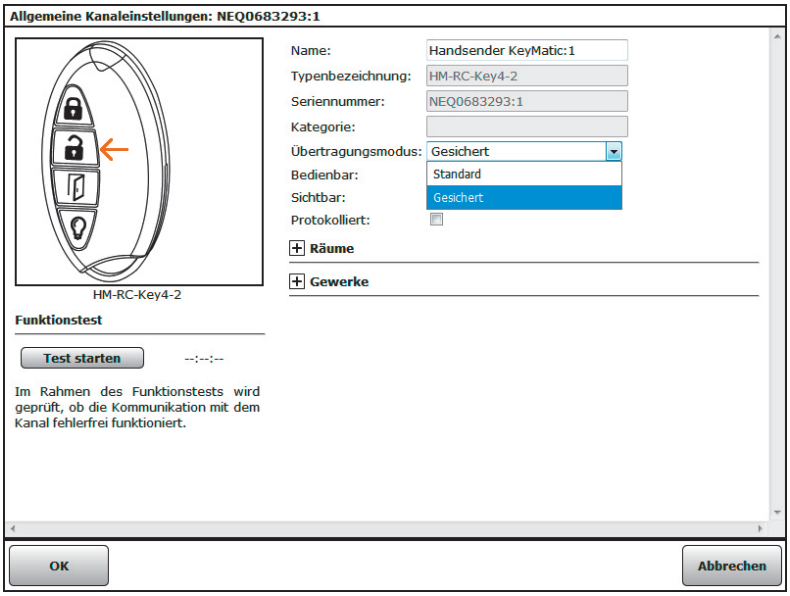

Bild 10: Beispiel für die Kanaleinstellungen eines Handsenders

Nach der Betätigung der Config-Taste eines Geräts muss also kurz gewartet werden, bis die Daten übertragen wurden. Dass eine Übertragung stattfindet, ist an der schnell blinkenden Geräte-LED erkennbar. Ist die Übertragung abgeschlossen, erlischt die LED. War die Übertragung erfolgreich, verschwindet die Servicemeldung in der WebUI automatisch.

Name	Typenbezeichnung	Bild	Bezeichnung	Seriennummer	Interface	Firmware
Handsender KeyMatic	HM-RC-Key4-2		HM-RC-Key4-2	NEQ0683293	BidCos-RF	Version: 1.2

Geräteparameter

Parameter
Reset per Gerätetaste sperren ☐

Bild 11: Parameter „Reset per Gerätetaste sperren“

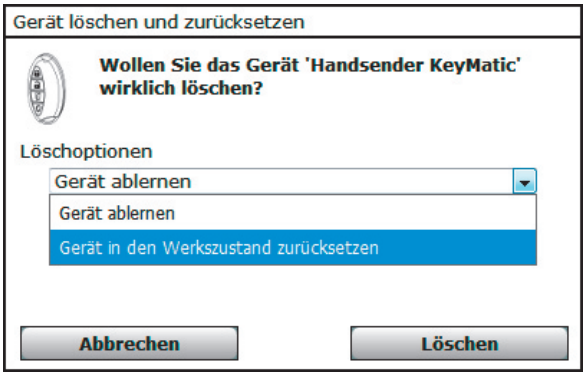

Bild 12: Korrekte Löschoption zum Entfernen des persönlichen Systemsicherheitsschlüssels

- Sofern ein umfangreiches System mit vielen Funkkomponenten betrieben wird, ist es zudem nicht ausgeschlossen, dass aufgrund der Anzahl zu übertragender Konfigurationsdaten das Sendelimit (Duty-Cycle) der Zentrale erreicht wird. Da in der aktuellen Version der Zentralen-Software eine entsprechende Hinweismeldung beim Erreichen des Duty-Cycles fehlt, ist dies für den Nutzer lediglich daran erkennbar, dass trotz der Betätigung der Geräte-Config-Taste die Daten nicht erfolgreich zu übertragen sind. In diesem Fall kann der Nutzer lediglich eine Stunde warten bzw. die Zentrale neu starten.

2. Übertragungsmodus

Damit die gesicherte Funkkommunikation mit dem persönlichen Systemsicherheitsschlüssel greift, muss je nach Gerätetyp der Übertragungsmodus in der Geräte-Konfiguration angepasst werden. Wie bereits erwähnt, ist dieser für sicherheitsrelevante Geräte bereits werkseitig konfiguriert. Möchte man diesen auch für weitere Geräte konfigurieren, ist hierzu die Geräteliste über „Einstellungen –> Geräte" zu öffnen. Anschließend öffnet man links durch einen Klick auf das Plus-Symbol die Unterkanäle des Geräts (siehe Bild 9). Klickt man nun in der Namensspalte auf den Kanalnamen, öffnet sich das Fenster für die allgemeinen Kanaleinstellungen (siehe Bild 10).

Hier kann unter Übertragungsmodus nun von „Standard" auf „Gesichert" umgestellt werden, anschließend sind je nach Gerätetyp erneut die Servicemeldungen zu beachten. Zu überlegen ist allerdings, ob es notwendig ist, jegliche auch nicht sicherheitsrelevante Gerätekommunikation auf „Gesichert" umzustellen. Ein Handsender, welcher beispielsweise direkt mit einem Dimmer verknüpft wurde, benötigt die gesicherte Kommunikation ggf. nicht zwingend.

3. Geräte-Werksreset bei gesetzten Systemsicherheitsschlüsseln

Sofern ein persönlicher Systemsicherheitsschlüssel gesetzt wurde, ist der Geräte-Werksreset nicht mehr möglich, allerdings gilt dies nicht für alle Geräte des Homematic Systems. Primär „ältere" Geräte-Generationen sind gegen den Reset bei gesetztem Schlüssel gesperrt. Bei neueren Geräten ist der Reset möglich, sofern der Nutzer nicht den in der Gerätekonfiguration ersichtlichen Parameter „Reset per Gerätetaste sperren" aktiviert hat (siehe Bild 11).

4. Folgen bei Schlüsselverlust

Es ist wichtig, dass, wie im Hinweistext der WebUI sowie dem WebUI-Handbuch [4] beschrieben, eine Dokumentation über die vom Nutzer gesetzten Systemsicherheitsschlüssel geführt wird. Hierzu gehören wie eingangs beschrieben das Erstellen und entsprechende Bezeichnen der Backups sowie das Notieren des zugehörigen Sicherheitsschlüssels. Des Weiteren sollte nicht nur der aktuell vergebene Schlüssel, sondern auch die vorhergehenden Schlüssel notiert sowie die zugehörigen Backups gespeichert bleiben. Somit ist es jederzeit möglich, sofern z. B. einmal der Schlüssel nicht an ein Gerät übertragen wurde, auf einen älteren Stand zurückzuspringen. Anschließend kann das Gerät über die Geräteliste mit der Option „Aus Homematic Zentrale löschen" sauber abgelernt/gelöscht werden, wodurch dann nach erfolgreicher Übertragung der Konfigurationsdaten der Schlüssel aus dem Gerät entfernt wird (siehe Bild 12).

Sollte der Systemsicherheitsschlüssel trotz Beachtung der genannten Punkte nicht bekannt und auch der Reset der Geräte nicht möglich sein, bleibt lediglich das Einsenden der Geräte zum kostenpflichtigen Firmware-Flash. Die Abwicklung sowie anfallenden Kosten sind in einem Hinweisblatt, zu finden unter Webcode #60064 im ELV Shop, aufgeführt.

5. Vor-/Nachteile

Der Hauptvorteil einer verschlüsselten Kommunikation liegt klar auf der Hand. Einem unbefugten Dritten wird die Möglichkeit genommen, die Funkkommunikation von außen zu beeinflussen bzw. letztlich die Geräte zu steuern. Zudem sind Geräte, die ggf. durch Dritte entwendet wurden, aufgrund des eigenen Sicherheitsschlüssels gegen das Zurücksetzen in den Auslieferungszustand sowie das Anlernen an eine andere Zentrale gesperrt (siehe Punkt 3).

Als eventuelle Nachteile lassen sich hier ggf. die folgenden Punkte aufführen:

- Je nach Programmierung kann es zur Erhöhung des Zentralen-Duty-Cycles führen.
- Die Batterielaufzeiten werden geringfügig verkürzt.
- Schaltbefehle werden minimal verzögert ausgeführt.
- Zur Vermeidung von Kommunikationsstörungen müssen in Zentralenprogrammen Verzögerungszeiten zwischen den Aktivitäten eingefügt werden. Dieser Hinweis gilt allerdings auch bei Verwendung des Standard-Übertragungsmodus (siehe Webcode #60062 im ELV Shop).

Die aufgeführten Punkte sind durch die für die Verschlüsselung notwendige, mehrfache Kommunikation zwischen Sender und Empfänger zu begründen.

Abschließend bleibt zu sagen, dass mit diesem Artikel lediglich die wichtigsten Punkte bezüglich der Netzwerk Sicherheit der Zentrale sowie der Funk-Kommunikation zwischen der Zentrale und den Homematic Komponenten behandelt wurden. Viele weiterführende Informationen zum Thema findet man z. B. im Homematic Forum [5].

Die Sicherheit des Homematic IP Systems werden wir in einem separaten Artikel beleuchten. ELV

Weitere Infos:

[1] www.elv.de: Webcode #60065
[2] www.meine-homematic.de
[3] www.myorbylon.de
[4] www.elv.de: Webcode #60066
[5] www.elv.de: Webcode #60067