



Living Space® | Smart Home

# Smart Home. Ja sicher!

## Ratgeber für Netzwerksicherheit bei der Gebäudesystemsteuerung

# Smart Home. Das ganze Haus im Griff.

Absolut alltagstauglich. Ein Smart Home bietet maximalen Komfort. Es lässt sich gewohnt über Bedienelemente an der Wand und darüber hinaus sogar über Smartphone und Tablet bedienen. Dabei eröffnet es uns ganz neue Möglichkeiten der Haussteuerung, die mit herkömmlichen Schaltern nicht realisierbar sind. Zudem ist das System immer an geänderte Bedürfnisse anpassbar. So ist Zukunftssicherheit gewährleistet.



## Jalousie-Management

Für jeden Anlass. Sonniges Tageslicht zum Lesen oder angenehmer Sichtschutz am Abend. Und das auf Wunsch auch automatisch.

## Sicherheit

Sicherheitsanwendungen wie z. B. Brandschutz, Anwesenheitssimulation, Bewegungsmelder und Alarmtechnik sind in einem Smart Home bestens integriert.



### Beleuchtung

In einem Smart Home lassen sich mit dem Licht ganz leicht verschiedene Atmosphären erzeugen – von romantisch bis gemütlich. Verschiedene Leuchten und Leuchtmittel verändern auf Knopfdruck nicht nur ihre Leuchtkraft, sondern auf Wunsch auch ihre Farbe.

### Szenen

Essen, sich einen Film ansehen oder einfach entspannen – bei verschiedenen (Un-)Tätigkeiten haben wir verschiedene Vorstellungen vom perfekten Licht, Temperatur und Sichtschutz. Mit der Szenenfunktion sind die gewünschten Verhältnisse nur einen Tastendruck entfernt.

### Multimedia

Einfach alles bequem nutzen und sogar vernetzen. Ob Smart-TV, Hi-Fi-Anlage, Computer oder Tablet.

### Raumtemperatur

Egal wie warm Sie es mögen, wenn Sie nicht zu Hause sind, kann die Heizung ruhig ausbleiben. In einem Smart Home tut sie das auch.

# Smart Home braucht Sicherheit. Risiken rechtzeitig erkennen.



Intelligente Gebäudetechnik ist heute ein fester Bestandteil moderner Elektroinstallation. Das Haus wird als Lebensraum verstanden und soll an die individuellen Bedürfnisse angepasst werden. Dabei liegen die Vorzüge des vernetzten Zuhauses auf der Hand: Per Smartphone oder Tablet lassen sich IP-Kamera, Beleuchtung oder Heizung bedienen – sogar von unterwegs. Dabei ist es wichtig, seine Daten richtig zu schützen, um Risiken zu minimieren.



ABB und Busch-Jaeger ist die Sicherheit unserer Kunden extrem wichtig. Daher überprüfen wir immer die IP-Sicherheit von Komponenten für die Gebäudesystemtechnik in unterschiedlichen Test-Konfigurationen. Um die Risiken

### Einblicke ins Privatleben

Sobald man elementare Dinge der Privatsphäre – wie Türen, Fenster oder Kameras – über das Internet miteinander verknüpft, wird es höchste Zeit für einen umfassenden Schutz. Denn gerade wenn der Nutzer von unterwegs auf die Überwachungskameras zugreifen kann, besteht das Risiko, dass diese Daten von Dritten mitgelesen werden könnten. Auch das Abfangen von einfachen Steuersignalen wie Lichtanschlüssen oder Lichtauschaltern birgt Gefahren, da es Rückschlüsse auf Ihre Gewohnheiten zulässt, die sich Einbrecher zunutze machen könnten.

### Fremdsteuerung Ihres Hauses

Gelingt es einem Dritten, sich in eine Smart-Home-Anlage zu hacken, so besteht auch das Risiko einer Fremdsteuerung und Umprogrammierung. Dadurch geht ein Großteil des vom Installateur geschaffenen Mehrwerts verloren und die Anlage muss gegebenenfalls erneut programmiert werden.

eines Smart Home jedoch auf ein Minimum zu bringen, bedarf es auch der Mitwirkung des Installateurs und des Endkunden, da die richtige Installation und die Wahl der Passwörter ein integraler Bestandteil der Sicherheit sind.

# Smart Home Realisierung. Risiken minimieren.

Erhöhung der Sicherheit. Smart Home Systeme machen eine Planung, Installation und Programmierung durch Fachhandwerker erforderlich. Generell empfiehlt es sich, einen Installateur beziehungsweise Systemintegrator für Gebäudeautomation hinzuzuziehen. Bei der Realisierung sind einige Sicherheitstipps zu beachten.

## Montage von Leitungen und Geräten

- » Anwendungen und Geräte sollten fest installiert werden, um zu verhindern, dass diese leicht entfernt werden und dadurch unbefugte Personen Zugang zur Anlage erhalten.
- » Die Leitungsenden der Kabel sollten nicht sichtbar sein oder aus der Wand herausstehen, weder innerhalb noch außerhalb des Gebäudes.

## Diebstahlschutzeinrichtung

- » Diebstahlschutzeinrichtung sollte verwendet werden (Sicherung durch Schrauben, nur mit Werkzeug entfernbar, hohe Abzugskräfte).





### Gerätepasswort

- » Verwenden Sie, falls verfügbar, ein Gerätepasswort. Das Gerätepasswort schützt vor unerlaubtem Zugriff durch Dritte.

### Begrenzt geschützte Bereiche

- » Busleitungen im Außenbereich stellen ein erhöhtes Risiko dar. Der physische Zugang zum KNX-Twisted-Pair-Kabel sollte hier besonders erschwert werden.
- » Möglichst keine Verlegung von Netzwerkleitungen im Außenbereich
- » Außengeräte müssen gegen unerlaubte Demontage abgesichert sein.
- » Geräte, die in begrenzt geschützten Bereichen verbaut sind (Außenbereich, Tiefgarage, WC etc.), können als zusätzlicher Schutz als eigene Linie ausgeführt werden. Durch Aktivierung der Filtertabelle im Linienkoppler wird verhindert, dass ein Angreifer Zugriff auf die gesamte Anlage erlangen kann.

# Smart Home Netzwerk. Risiken minimieren.

## Getrenntes LAN-/WLAN-Netzwerk

- » Für die Gebäudeautomation sollte ein getrenntes LAN- oder WLAN-Netzwerk mit eigener Hardware (Router, Switches etc.) verwendet werden.
- » Für ausreichende WLAN-Abdeckung sorgen. Hierfür sind zusätzlich installierte WLAN-Access-Points hilfreich.

## Sicherheits-Mechanismen für IP-Netzwerke verwenden

- » Verwenden von Antivirus-Software und Firewall
- » Verschlüsselung von Drahtlosnetzwerken (WPA2 oder höher)
- » Verwenden von sicheren Passwörtern
- » MAC-Filter verwenden

## Sicheres Passwort

Passwörter schützen zahlreiche sensible Daten von uns, ein Missbrauch ist oft nur schwer oder gar nicht mehr rückgängig zu machen. Im Folgenden werden die Kennzeichen eines sicheren Passworts beschrieben.

Regeln für ein sicheres Passwort:

- » Das Passwort muss mindestens 8 Zeichen umfassen.
- » Es sollte mindestens 2 Sonderzeichen, eine Zahl, einen Kleinbuchstaben und einen Großbuchstaben enthalten.

## Passwort-Manager

Wenn es für Sie immer schwieriger wird, sich die unzähligen Passwörter zu merken, helfen Passwort-Manager dem Gedächtnis auf die Sprünge.

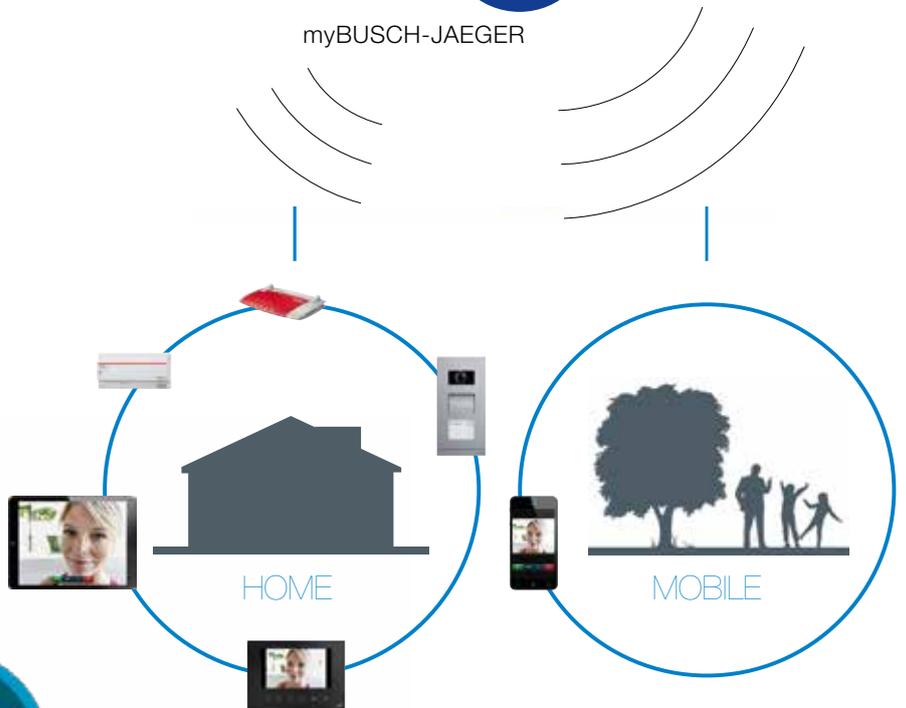
Passwort-Manager speichern auf sichere Art und Weise die Benutzernamen und Passwörter, die Sie beim Zugriff auf Webseiten verwenden, und fügen sie beim nächsten Besuch automatisch für Sie ein.

Ergänzend zum sicheren Passwort sollte man die Mehrfaktor-Authentifizierung nutzen. Hierbei wird meist ein zweiter – temporärer – Code verwendet. Apple, Facebook, PayPal und andere große Internetdienstleister bieten diese Möglichkeit an.





myBUSCH-JAEGER

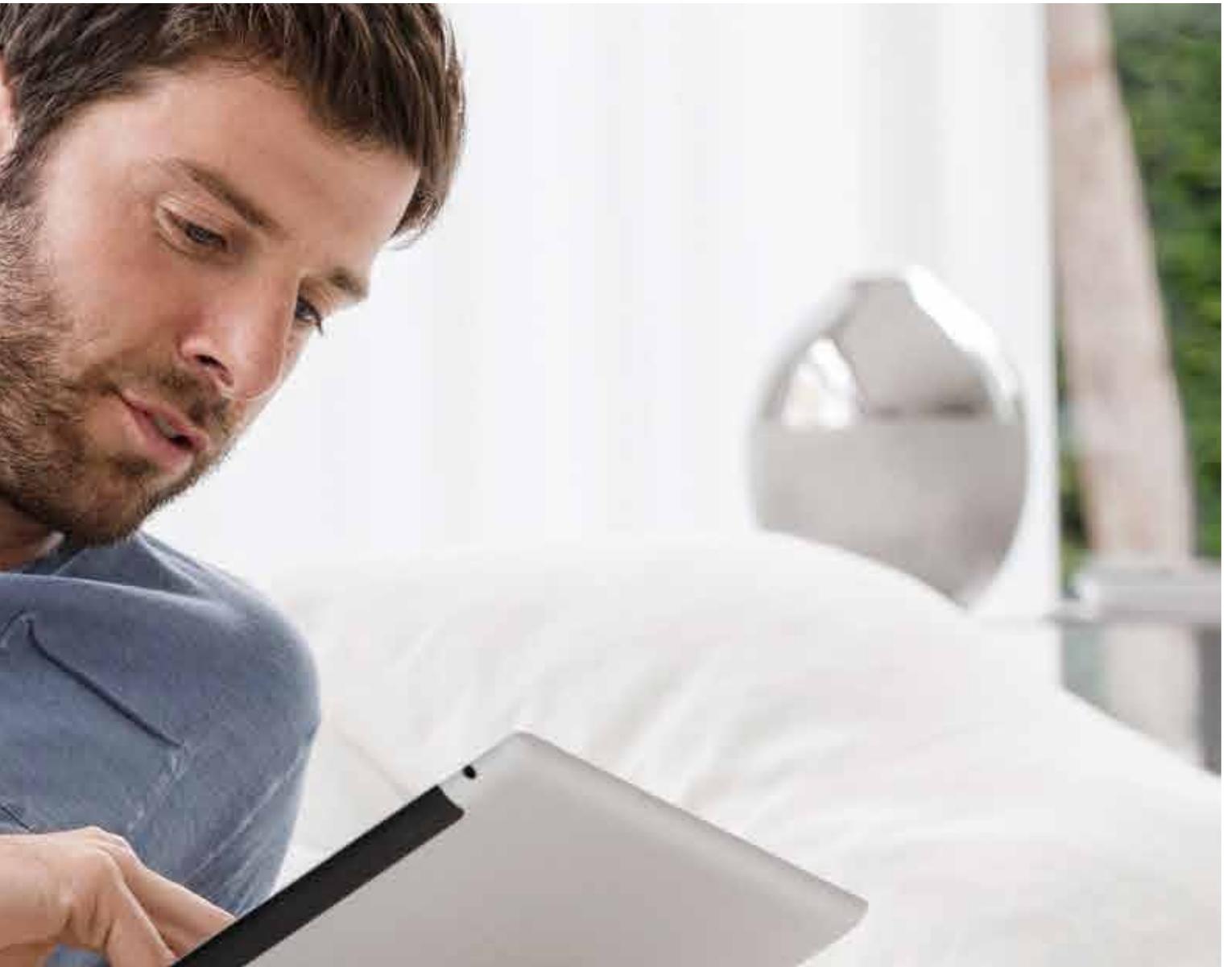


### Fernzugriff

- » KNXnet/IP Routing und KNXnet/IP Tunneling sind bei der Verwendung im Internet nicht sicher, da sie ein unverschlüsseltes Protokoll verwenden.
- » Es sollten keine Ports von Routern Richtung Internet geöffnet werden: Dies verhindert, dass die KNX-Kommunikation im Internet sichtbar wird.
- » Um Fernzugriff zu erlangen, empfiehlt sich ein VPN-Tunnel oder myBUSCH-JAEGER. Das myBUSCH-JAEGER-Portal ist ein Service der ABB, der höchsten Bedienkomfort für den Fernzugriff mit Smartphone und Tablet garantiert. Der Endkunde braucht keinen DynDNS Account. Eine Verbindung baut sich über eine Cloud auf, indem man sich auf myBUSCH-JAEGER registriert und einloggt.

Smart Home. Ja sicher!  
Ein gutes Gefühl.





Ein Smart Home ist intelligent und komfortabel. Wird es zudem fachgerecht vor dem Zugriff Dritter geschützt, lässt es sich bedenkenlos genießen – und das von überall. Je komplexer die technischen Systeme werden und je weiter die digitale Vernetzung in Gebäuden voranschreitet, desto kritischer müssen die damit verbundenen Sicherheitsaspekte betrachtet werden.

**ABB AG**  
**Electrification Products**

**Zentrale**

Clemens-Holzmeister-Straße 4  
1109 Wien, Österreich  
Telefon: +43 (0)1 60109 6203  
Telefax: +43 (0)1 60109 8600

**Kundencenter**

Telefon: +43 (0)1 60109 6530  
E-Mail: [at-lpkc@abb.com](mailto:at-lpkc@abb.com)

**[www.abb.at/lowvoltage](http://www.abb.at/lowvoltage)**

**Hinweis:**

Nachdruck und fotomechanische Wiedergabe sind nur mit unserer ausdrücklichen Genehmigung gestattet.

Die Druckerzeugnisse von ABB / Busch-Jaeger informieren nach bestem Wissen, die Aussagen sind jedoch nicht rechtsverbindlich. Alle Abbildungen und Fotografien der dargestellten Produkte sind in Bezug auf Farbigkeit, Abmessungen und Ausstattung nicht verbindlich.

Die meisten ABB / Busch-Jaeger Produkte sind eingetragene Warenzeichen.

Die Angaben in diesem Katalog sind ohne Gewähr. Änderungen und Aktualisierungen, die dem Fortschritt dienen, bleiben vorbehalten.

Alle Produkte in diesem Druckerzeugnis, die den CE-Richtlinien entsprechen, tragen auf der Verpackung und dem Produkt die entsprechende Kennzeichnung.

Copyright© 2016 ABB  
Alle Rechte vorbehalten