24

ElektroSPICKER

Fakten und Tipps auf einen Blick

DATENSICHERHEIT IM SMART HOME

Wie lassen sich die Themen Datensicherheit und Smart Home vereinen? Was ist bei der Umsetzung zu beachten? Wieso kann Transparenz zu Datensicherheitsmaßnahmen gefährlich sein?

Hier geht es zur Online-Version.

Die Nachfrage nach Smart Home steigt stetig. Das vernetzte Wohnen erleichtert nicht nur den Alltag, sondern birgt auch weitere Vorteile, wie Zeitersparnis und Energieeffizienz.

Gleichzeitig bestehen gerade bei der Vernetzung des Zuhauses Unsicherheit und Bedenken hinsichtlich Datensicherheit, denn nirgendwo ist die Bedeutung von Privatsphäre so groß wie in den eigenen vier Wänden.

Gut zu wissen
Knapp 61% aller Endverbraucher legen laut einer durch den TÜV Rheinland beauftragten Umfrage bei der Smart Home-Anschaffung Wert auf die Datensicherheit und den Datenschutz des Systems.

Während die Anzahl der Smart Home Systeme stetig zunimmt, bremsen Bedenken hinsichtlich Datenschutz und Datensicherheit die Verbreitung laut dem Smart Home Consumer Survey (2018) von Deloitte jedoch stark. Diese Skepsis scheint auch nicht abzunehmen, sondern weiterhin zu steigen. Gerade im Bereich der Weitergabe von System-Nutzungsdaten herrscht nach wie vor Zurückhaltung.

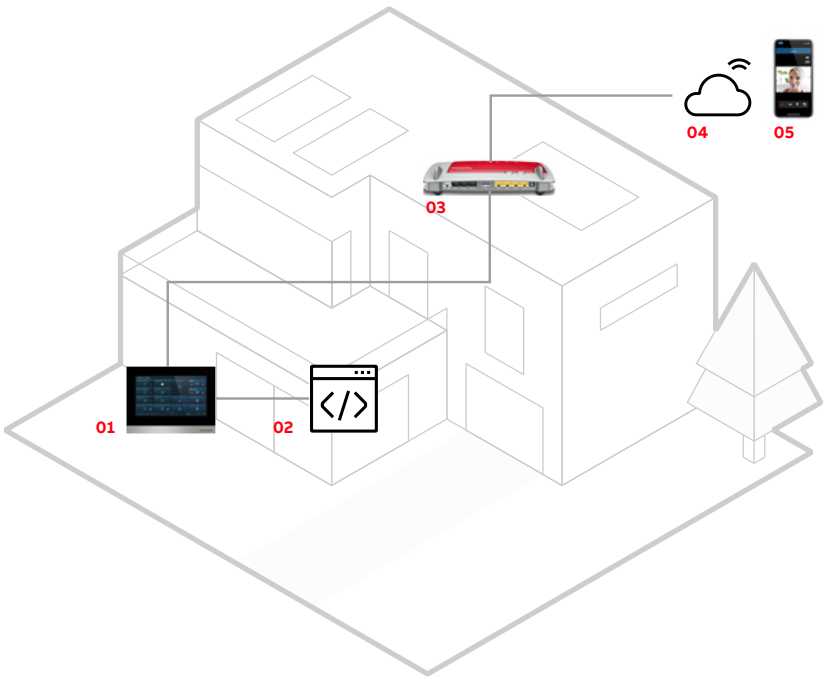
Sicher im Smart Home

Datenschutz und Datensicherheit – was heißt das?

Datenschutz
Der Begriff Datenschutz beschreibt den Verbraucherschutz bzgl. des Umgangs mit persönlichen Daten. Hier liegt der Fokus besonders darauf, dass die Nutzer genau wissen, wofür ihre persönlichen Daten verarbeitet werden und kein Datenmissbrauch stattfindet. Da im Smart Home besonders viele sensible Informationen, wie das Nutzungsverhalten oder auch die Kameraaufnahmen der Türsprechanlage, digital verarbeitet werden, ist es sinnvoll, dass der Elektrofachmann im Vorfeld einer Installation und Inbetriebnahme eine vertragliche Zustimmung vom Kunden einholt.

Datensicherheit
Bei der Datensicherheit geht es, vereinfacht formuliert, um die Sicherheit der auf den Geräten gespeicherten Daten, unabhängig davon, ob diese personenbezogen sind oder nicht. Da sich hierunter aber auch häufig persönliche Daten befinden, ist der Datenschutz ein Teilbereich der Datensicherheit.
Im Smart Home sind das z.B. festgelegte Szenen, wann die Rollläden rauf- oder runtergefahren oder wann alle Lichter ausgemacht werden.

Es gibt verschiedene Punkte, an dem das Risiko besteht unbefugten Zugriff auf ein Smart Home zu erlangen. Diese lassen sich jedoch einfach sichern.



01 Smart Home System – Verschlüsselung mit einem sicheren Passwort (regelmäßig wechseln)

02 Firmware – Regelmäßige Installation von Updates und Sicherheits-Patches

03 Router – schwer entschlüsselbares WLAN-Passwort (regelmäßig wechseln), nicht dem Nutzer zuordenbare Netzwerkbezeichnung

04 Cloud – Auswahl eines Systems, das u.a. im Kontext Informationssicherheit VDE-geprüft ist

05 Smartphone – Keine leicht zu entschlüsselnde PIN wählen

4 Schritte zur Erhöhung der Datensicherheit

1

Regelmäßige Updates
Das Updaten der Smart Home Geräte sorgt nicht nur dafür, dass neue Funktionen auf den Geräten installiert, sondern auch potenzielle Sicherheitslücken geschlossen werden. Um eine stets aktuelle Software zu haben, ist es ratsam die Option „automatisches Update“ auszuwählen.

2

Back-ups
Regelmäßige Backups sind besonders wichtig, um bei Problemen jederzeit auf das Projekt zurückgreifen zu können.

Die (automatisierte) Back-up-Erstellung ist in der Regel mit einer Anbindung der Smart Home Lösung an eine zugehörige Cloud verbunden. Ob dies der Fall ist und wie eine sichere Einrichtung erfolgen kann, klärt in der Regel ein Blick in die Bestimmungen des jeweiligen Herstellers und die Anleitungen des Smart Home Systems.

In eigener Sache: Die von Nutzern innerhalb der myBusch-Jaeger Cloud hinterlegten Daten befinden sich nicht auf den Servern des Unternehmens, sondern verschlüsselt bei einem in Deutschland ansässigen Partner, der die myBusch-Jaeger Cloud verwaltet. Busch-Jaeger hat zu keinem Zeitpunkt Zugriff auf und Einblick in die Daten der Kunden.

3

Verschlüsselung
In jedem Fall sollten die Geräte bzw. Systeme mit einem sicheren Passwort geschützt sein. Dabei ist darauf zu achten, dass die Passwörter nicht mehrfach verwendet werden. Zudem sollten die Passwörter in regelmäßigen Abständen gewechselt werden. Hierbei sind die hohen Anforderungen wie Groß- und Kleinschreibung, Zahlen, Sonderzeichen und Länge zu berücksichtigen. Nur so kann das Smart Home System vor Manipulation und fremden Zugriffen geschützt werden. Darüber hinaus sollte die Smart Home Kommunikation verschlüsselt sein.

In eigener Sache: Busch-Jaeger vergibt jeder Smart Home Anlage einen individuellen Code für die Telegramme, die zwischen den jeweiligen Geräten innerhalb einer Anlage versendet werden. Dies sorgt für zusätzlichen Schutz.

4

Absicherung des Heimnetzwerks
Das Netzwerk des Smart Home Nutzers sollte stets mit einem Passwort versehen sein, das nicht mit anderen geteilt wird. Für Gäste empfiehlt es sich, ein Gäste-WLAN innerhalb des Routers aufzubauen, um so das Netzwerkpasswort nicht teilen zu müssen.

TIPP: Bei modernen Netzwerkroutern lassen sich auch die MAC-Adressen aller im Netzwerk erlaubten Geräte hinterlegen.

Es ist zudem hilfreich, sein WLAN-Signal zu verbergen oder aber das Netzwerk so zu benennen, dass es dem Eigentümer nicht zuzuordnen ist. Darüber hinaus sollte das Netzwerkpasswort nie mit dem Passwort der Smart Home Anlage identisch sein.

Ein weiteres Schlupfloch befindet sich im Smartphone. Auch hier sollte unbedingt darauf geachtet werden, dass es entsprechend vor unbefugtem Zugriff geschützt ist.

TIPP: Vermeide einfache Zahlen- und Strichcodes, da sonst bei Diebstahl des Smartphones das Risiko besteht, dass Dritte auf die Smart Home Anlage oder die Haustür zugreifen können

Fragen und Antworten
FAQ

Wieso sind die Themen Datenschutz und Datensicherheit im Smart Home Kontext relevant?

Smart Home Systeme stellen einen Trend der heutigen Zeit dar. Wer sich diesem anschließen möchte, sollte im Umgang mit Daten aufgeklärt sein. Regelmäßige Updates, Absicherung der Systeme, Verschlüsselungen und Backups sind wichtige Schritte, mit denen die Smart Home Nutzer zusätzliche Sicherheit schaffen können.

Was sind die häufigsten Fehler von Endverbrauchern im Umgang mit Datensicherheit?

Der mangelnde Schutz des Heimnetzwerkes stellt einen der häufigsten Fehler im Umgang mit Datensicherheit dar. Denn auch hier gilt: Eine Kette ist nur so stark wie ihr schwächstes Glied. Einfache Passwörter, offene Netzwerke und ungesicherte Geräte ermöglichen einfachen Zugang zu sensiblen Daten. Um dem entgegen zu wirken, sollte neben der Smart Home Beratung auch über die Gefahren und deren Lösungen im Netzwerk hingewiesen werden, um für den Kunden ein "Rundum sorglos"-Paket zu schaffen.

Wo finde ich Informationen zum Thema Datenschutz und -sicherheit?

Die Verbraucherzentrale des Bundes und der Bundesländer sind grundsätzlich ein guter Anlaufpunkt.

—
Verbraucherzentrale: Informationen zum Smart Home.

—
Verbraucherzentrale Baden-Württemberg: Datenschutz im Smart Home

Sobald es technischer wird, empfehlen wir entsprechende Schulungen.

Was kann ich als Elektroinstallateur und Systemintegrator zur Verbesserung beitragen?

Regelmäßige fachliche Weiterbildungen zur Installation und Programmierung sind entscheidend. Die Anforderungen an die Cybersicherheit für Smart Buildings, egal ob Privatgebäude oder kommerzielle, steigen. Das sorgt auch für eine zunehmende Komplexität der Systeme und damit der Einrichtung und Konfiguration. Regelmäßige Weiterbildungen sind daher wichtig, um auf dem neusten Stand zu bleiben und Deinen Kunden die bestmögliche Leistung bieten zu können.

Wieso ist es herstellerseitig so schwierig die Datenschutzmaßnahmen den Nutzern transparent zu Verfügung zu stellen?

Je mehr Informationen über eine Sicherheitsmaßnahme bekannt sind, desto leichter lässt sich diese umgehen oder hacken. Um dies zu verhindern, können Unternehmen mit entsprechenden smarten Services nicht im Detail Auskunft darüber geben, wie sie die Systeme schützen, sondern meist nur, dass sie es tun, welche Maßnahmen grob getroffen wurden und (abhängig von der Anwendung) welche Zertifizierungen das jeweilige System hat (z.B. VDE-Zertifizierung für Informationsicherheit).

ABB STOTZ-KONTAKT GmbH
Kundencenter
Eppelheimer Straße 82
69123 Heidelberg, Deutschland
Tel.: +49 (0) 6221 701-777
Fax: +49 (0) 6221 701-771
info.stotz@de.abb.com

Busch-Jaeger Elektro GmbH
Zentraler Vertriebsservice
Freisenbergstraße 2
58513 Lüdenscheid, Deutschland
Tel.: 02351 956-1600
Fax: 02351 956-1700
info.bje@de.abb.com

—
Hier geht es zur Online-Version.