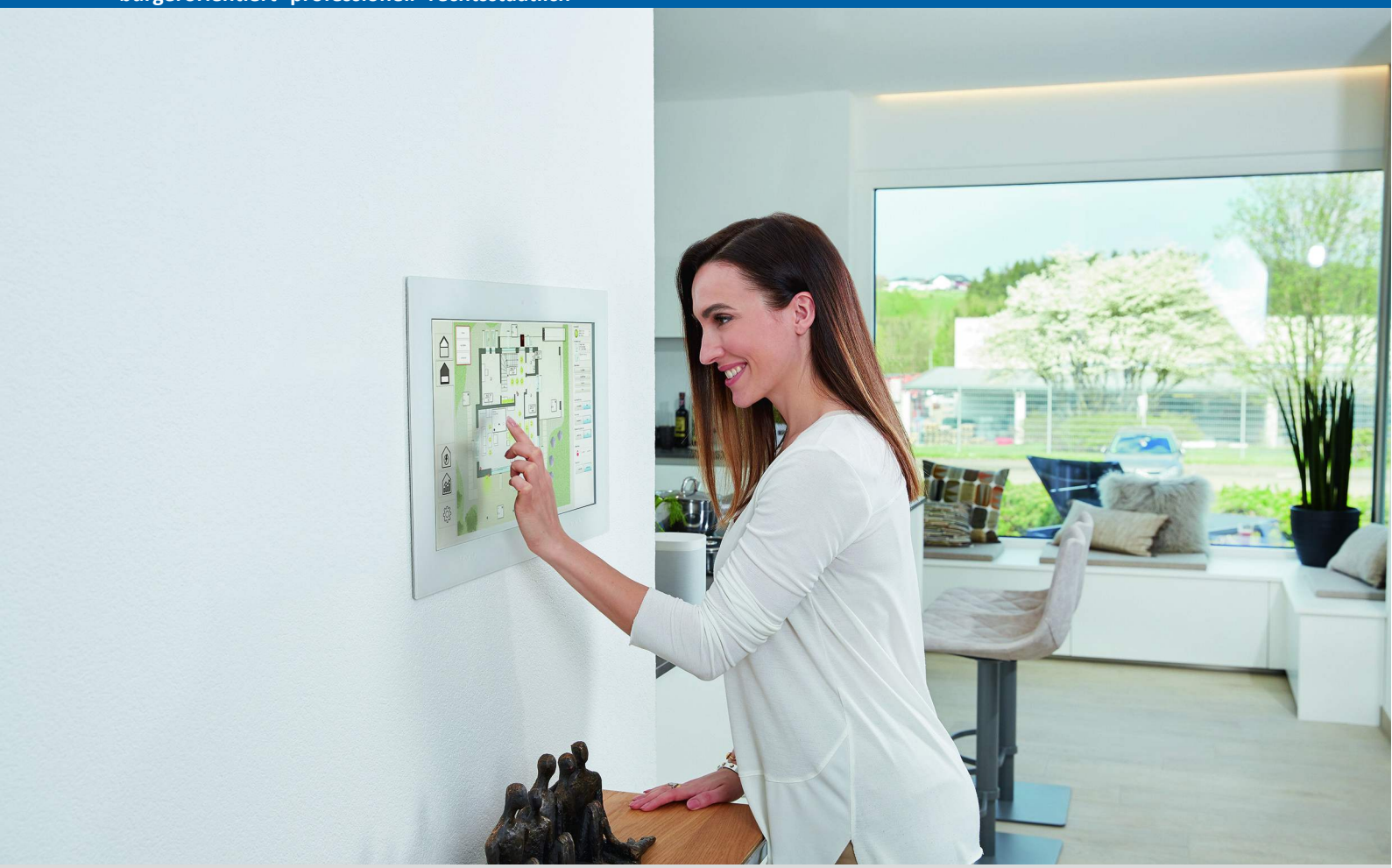
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Smart Home und Internet der Dinge (IoT)

Empfehlungen zur Sicherung digitaler Haustechnik

VdS Vertrauen durch Sicherheit

SMARTHOME DEUTSCHLAND

Stand: Februar 2019

Sicherheit für Ihre digitale Haustechnik

Nicht nur die Unterhaltungselektronik, sondern auch alle Arten von Haushaltsgeräten, automatisierte Beleuchtung, Schließsysteme, Türen, Tore, Fenster, Rollläden, Markisen und die Heizungssteuerung werden zunehmend mit digitalen Steuerelementen ausgestattet. Grundsätzlich könnten digitale Signale durch Angriffe Dritter „mitgelesen“, manipuliert und damit für illegale Zwecke wie Ausspähen der Wohnungsinhaber, Sabotage und Einbruch genutzt werden. Mit geeigneten Schutzmaßnahmen schieben Sie solchen Angriffen den „digitalen Riegel“ vor.

Mit diesem Merkblatt möchten die Polizei NRW, die VdS Schadenverhütung GmbH und die SmartHome Initiative Deutschland e.V. Sie über mögliche Gefahren und Schutzmöglichkeiten im Hinblick auf digital gesteuerte und vernetzte Systeme informieren.

Nutzen

Der Nutzen „intelligenter“ Hausgeräte und deren digitaler Vernetzung liegt auf der Hand. Durch automatisierte Abläufe, wie beispielsweise die bedarfsgerechte Steuerung von Markisen, Rollläden, Temperatur und Licht gewinnen die Bewohner Zeit und Komfort. Die Fernabfrage und -steuerung über mobile Endgeräte vermittelt zusätzlich das gute Gefühl, dass Zuhause „alles in Ordnung ist“.

Richtig geplant, fachgerecht installiert und regelmäßig aktualisiert, können digital vernetzte Sensoren durch frühzeitige Warnung vor Einbruch-, Brand-, Gas- und Wassergefahren warnen und durch automatische Abläufe im Gefahrenfall Ihre Sicherheit deutlich verbessern und dabei helfen, Ihre Sachwerte in Haus und Wohnung zu schützen.

Risiken

Unsichere und fehlerhaft installierte digitale Steuerungssysteme bergen allerdings auch Risiken.

Vermeiden Sie, dass Ihre Daten durch Dritte mitgelesen und Sie dadurch ausgespäht werden.

Durch unberechtigt erlangten Zugriff Dritter auf Videokameras und das Mitlesen von Daten, die zwischen einem Endgerät in der Wohnung und der Smart Home Zentrale oder der Cloud-Anwendung ausgetauscht werden, können Täter Einblicke in die Privatsphäre der Bewohner nehmen. Neben Erkenntnissen über Ihre Gewohnheiten und Ihr Verhalten könnten Straftäter Ihre An- oder Abwesenheit ausspähen und dies zur Vorbereitung einer Straftat, beispielsweise eines Einbruchs, nutzen.

Sichern Sie ihre digital gesteuerten Fenster, Rollläden etc. gegen die unbefugte Betätigung.

Neben klassischen Einbruchsmethoden, wie dem Aufhebeln von Türen und Fenstern, könnten Straftäter in unzureichend geschützte elektronische Schließsysteme eingreifen. Vandalismusschäden sind ebenfalls denkbar, wenn z. B. elektrisch betätigte Dachfenster oder Markisen bei Regen oder Sturm geöffnet bzw. ausgefahren werden.

Gefahren durch das Internet

Neben den klassischen Systemen mit einer Smart Home Zentrale im Haus oder Wohnung werden sogenannte IoT-Geräte (Internet of Things) angeboten. Diese Produkte verzichten auf die lokale Zentrale und nutzen stattdessen das Internet für die Signalübertragung und Speicherung der Daten auf dem Server eines externen Anbieters (Cloud). Diese Anbieter befinden sich innerhalb aber auch außerhalb des europäischen Rechtsraums. Zu bedenken ist hierbei, dass ein Geschäftszweck des Anbieters die Erlangung von Profildaten für Marketingzwecke sein kann. Der Nutzen und damit auch die Sicherheit der eigentlichen Funktion müssen für ihn nicht im Vordergrund stehen. Zudem ist zu bedenken, dass viele IoT-/Cloudlösungen bei ausgefallener Internetverbindung nicht mehr funktionieren.

Empfehlungen zum Schutz Ihrer digital gesteuerten Haustechnik

Informieren Sie sich über Ihre Haustechnik

Verstehen Sie Smart Home als das Zusammenspiel mehrerer Systeme und Komponenten, die jeweils spezifischen Nutzen, aber auch Risiken und damit Schutzerfordernisse haben.

Verlassen Sie sich bei vernetzten Geräten nicht darauf, dass an einzelnen Komponenten Sicherheitselemente installiert wurden. Ein einzelnes Sicherheitsprodukt ergibt noch kein schlüssiges Sicherungskonzept; denn gerade bei zusammen wirkenden technischen Systemen ist „eine Kette immer nur so stark wie ihr schwächstes Glied“.

Sicherheit bedeutet manchmal Einbußen beim Komfort, aber die Sicherheit Ihrer Daten und Ihres Heims sollte es Ihnen wert sein.

Informieren Sie sich über die technischen Geräte in Ihrem Haushalt und deren digitale Steuerung und Vernetzung.

Erkundigen Sie sich im Internet über bereits bekannte Sicherheitslücken. Aktualisieren Sie, soweit vom Hersteller vorgesehen, regelmäßig die Betriebssoftware Ihrer Komponenten und installieren Sie stets aktuelle Sicherheitsupdates.

Smart Home ist Informationstechnik. Es gelten die gleichen Sicherheitsregeln.

Lesen Sie die Betriebsanleitung des Produktes und die Sicherheitshinweise aufmerksam und beachten Sie die Empfehlungen des Herstellers. Nutzen Sie alle vorhandenen Sicherheitselemente und Einstellungen ihrer Geräte.

Nutzen Sie sichere Passwörter.

Setzen Sie Ihre Passwörter aus möglichst vielen Zeichen zusammen und verwenden Sie Kombinationen von großen und kleinen Buchstaben, Ziffern und Sonderzeichen. Nutzen Sie für verschiedene Zugänge unterschiedliche Passwörter. Ein sogenannter Passwortmanager kann Ihnen helfen, sich die Vielzahl Ihrer Passwörter zu merken. Dies ist eine Software, welche Ihre Passwort-Daten verschlüsselt speichert. Sie brauchen sich dann nur noch ein Passwort für den Zugang zum Passwortmanager zu merken. Passwortmanager gibt es auch für Mobiltelefone. Informieren Sie sich hierzu im Internet oder Fachhandel.

Installieren Sie eine Firewall und ein Virenschutzprogramm.

Installieren Sie stets aktuelle Versionen einer Virenschutzsoftware und nutzen Sie eine Firewall auf Ihren digitalen Endgeräten, wie Smartphones, Tablets, PCs, Routern und vernetzter Haustechnik. Ziehen Sie einen Experten hinzu, wenn Sie sich in der Handhabung nicht sicher fühlen.

Weitere Informationen bietet Ihnen das BSI (Bundesamt für Sicherheit in der Informationstechnik) www.bsi-fuer-buerger.de

Nutzen Sie nur die Geräte und Komponenten, die Sie wirklich brauchen.

Schalten Sie Geräte immer vollständig aus, wenn diese nicht benötigt werden. Dies spart nicht nur Strom, sondern schützt Sie auch vor unberechtigten Zugriffen. IoT-Smart Home Produkte benötigen allerdings ständigen Internetzugang und können dadurch mehr gefährdet sein, als Systeme mit Smart Home Zentralen. Letztere funktionieren auch ohne Internet.

Minimieren Sie Ihre Daten soweit wie möglich. Speichern oder verwenden Sie nur die Daten, die für eine gewünschte Funktion wirklich notwendig sind.

Deaktivieren Sie nicht benötigte Funktionen und Schnittstellen in den Konfigurationseinstellungen des Gerätes. Verbinden Sie Ihre Geräte nur dann mit dem Internet, wenn dies wirklich nötig ist, z.B. für Updates oder wenn Sie entsprechende Funktionen nutzen wollen. Stellen Sie sicher, dass Ihre Geräte nicht automatisch, sondern nur dann mit dem Internet verbunden werden, wenn Sie das wollen.

Schützen Sie Ihr WLAN.

Nutzen Sie WLAN-Verschlüsselung, damit Daten nicht von jedermann mitgelesen werden können. Dazu sollte der höchste vorhandene Standard in den Einstellungen gewählt und ein sicheres Zugangskennwort verwendet werden. Einige Hersteller verwenden inzwischen sichere und individuelle voreingestellten Kennwörter. Einfache Passwörter wie „admin“ oder „1234“ müssen Sie umgehend ändern.

Seien Sie auch unterwegs wachsam.

Achten Sie bei der Nutzung von digitalen Geräten im öffentlichen Raum (Flughafen, Hotel, etc.) darauf, dass niemand die Eingabe Ihrer Daten ausspähen kann (z.B. Sitznachbarn im Bus oder Cafe).

Einbruchschutz

Grundlage eines individuellen Sicherungskonzeptes gegen Einbruchdiebstahl sollten immer mechanisch-bauliche Sicherungseinrichtungen sein. Smart-Home-Lösungen allein stellen kein Einbruchmelde- bzw. Gefahrenwarnsystem im Sinne der DIN VDE V 0826-1 oder DIN VDE 0833-1 und -3 dar. Fragen Sie Ihre Polizei nach dem Faltblatt "Tipps für mehr Sicherheit: Schlagen Sie Alarm!" und der Broschüre "Sicher wohnen" des Programms Polizeiliche Kriminalprävention der Länder und des Bundes

(ProPK).Weitere Informationen zum Einbruchschutz:

www.vds-home.de
www.riegelvor.nrw.de
www.polizei-beratung.de
www.smarthome-deutschland.de
www.k-einbruch.de

Impressum

Herausgeber

Landeskriminalamt Nordrhein Westfalen
Sachgebiet 32.2 - Technische Prävention,
Prävention von Vermögens- u. Eigentumsdelikten
Völklinger Str. 49
40221 Düsseldorf
Tel.: (0211) 939 0
Fax: (0211) 939 3209
E-Mail: einbruchschutz@polizei.nrw.de
www.lka.nrw.de

Titelbild: SmartHome Initiative Deutschland e.V.

Mit freundlicher Unterstützung durch:

VdS Schadenverhütung GmbH
Geschäftsbereich Produkte &
Unternehmen
Amsterdamer Straße 172
50735 Köln
Tel.: 0221 7766 0
Fax: 0221 7766 341
E-Mail: security@vds.de

www.vds.de
Verbraucherportal: www.vds-home.de

SmartHome Initiative Deutschland e.V.
Rathausstraße 48
12105 Berlin
Tel.: 030 60 98 62 43
E-Mail.: info@smarthome-deutschland.de
www.smarthome-deutschland.org