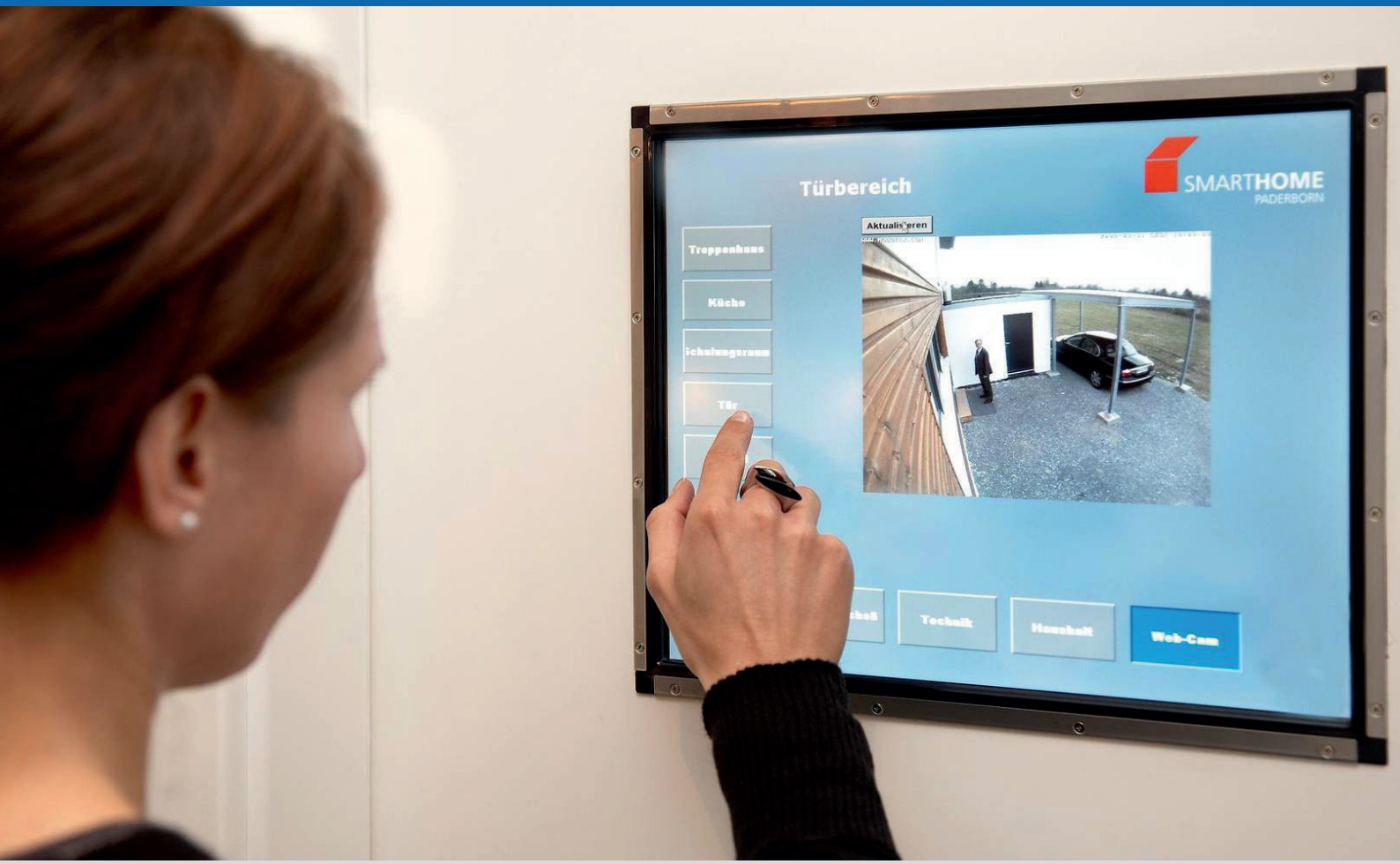
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Smart Home und Connected Home

Empfehlungen zur Sicherung digitaler Haustechnik

VdS Vertrauen durch Sicherheit

SMARTHOME DEUTSCHLAND

Stand: Dezember 2023

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. Digitale Signale können aber auch 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 und Fenstern 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 projektiert, fachgerecht installiert und regelmäßig aktualisiert und instandgehalten, können digital vernetzte Sensoren durch frühzeitige Warnung vor Einbruch-, Brand-, Gas- und Wassergefahren warnen und durch automatisierte Schaltprozesse im Gefahrenfall Ihre Sicherheit deutlich verbessern und helfen Ihre Sachwerte in Haus und Wohnung zu schützen.

Risiken

Ungeschützte digitale Steuerungssysteme, ob mit oder ohne Zugang zum Internet, 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 online zwischen einem Endgerät des Verbrauchers und der Steuerungszentrale 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 - z. B. eines Einbruchs - nutzen.

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

Einbrecher erhalten gegebenenfalls neue Möglichkeiten, sich Zutritt zu verschaffen. Neben klassischen Einbruchsmethoden, wie dem Aufhebeln von Türen und Fenstern, könnte in unzureichend geschützte elektronische Schließsysteme eingegriffen werden.

Auch Vandalismusschäden sind denkbar, wenn z. B. in Ihrer Abwesenheit elektrisch betätigte Dachfenster oder Markisen bei Regen oder Sturm geöffnet bzw. ausgefahren werden.

Sichern Sie Ihre digital gesteuerten Hausgeräte zuverlässig gegen Fremdsignale, Stromausfall und Fehlfunktionen.

Mögliche Fremdsignale anderer technischer Geräte können die Haussteuerung ggf. beeinträchtigen. Außerdem können technische Defekte, Batterieausfall oder Netzprobleme Fehl- und Falschfunktionen verursachen. Durch häufig wiederkehrende Störungen geht der erhoffte Komfort verloren und das Vertrauen in die hilfreiche Technik schwindet.

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 spezifische Risiken und 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. Informieren Sie sich im Internet über

bereits bekannte Sicherheitslücken. Aktualisieren Sie, soweit vom Hersteller vorgesehen, regelmäßig die Betriebssoftware Ihrer Komponenten und installieren Sie aktuelle Sicherheitsupdates.

Nutzen Sie vorhandene Sicherheitskomponenten.

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

Nutzen Sie sichere Passwörter.

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 auch unterschiedliche Passwörter. Ändern Sie besonders sensible Passwörter häufig.

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. Derartige Software gibt es auch für Mobiltelefone. Informieren Sie sich hierzu im Internet oder Fachhandel über die verschiedenen Produkte und deren Sicherheit.

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.

Viele Geräte bieten Konfigurationsoberflächen an, die einen Zugriff über das Internet ermöglichen und im Werkzustand nur mit Primitivcodes geschützt sind. Diese Geräte sollten Sie nur ans Internet anschließen, wenn Sie neue, sicherere Passwörter vergeben haben.

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 auch vor unberechtigten Zugriffen.

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 sog. WPA2 (WAP3)-Standard in den Einstellungen gewählt und ein sicheres Zugangskennwort (siehe Passwörter) verwendet werden. Nutzen Sie auf keinen Fall die von Herstellern voreingestellten Kennwörter.

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. Fragen Sie Ihre Polizei nach dem Faltblatt "Tipps für mehr Sicherheit: Schlagen Sie Alarm!" und der Broschüre "Ungebetene Gäste" des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK), welche detaillierte Informationen zum Einbruchschutz enthalten.

Weitere Informationen zum Einbruchschutz finden Sie im Internet unter:

www.vds-home.de

www.polizei-beratung.de

www.smarthome-deutschland.de

Impressum

Herausgeber

Landeskriminalamt Nordrhein Westfalen
Sachgebiet 32.1 - Kriminalprävention/Opferschutz
Völklinger Str. 49
40221 Düsseldorf
Tel.: 0211 939 0
Fax: 0211 939 4119
E-Mail: einbruchschutz@polizei.nrw.de

https://lka.polizei.nrw/

Titelbild: SmartHome Initiative Deutschland e.V.

Mit freundlicher Unterstützung durch:

VdS Schadenverhütung GmbH
Fachbereich Security
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.
Petersburger Str. 94
10247 Berlin
Tel.: 030 60 98 62 43
E-Mail.: info@smarthome-deutschland.de

www.smarthome-deutschland.de