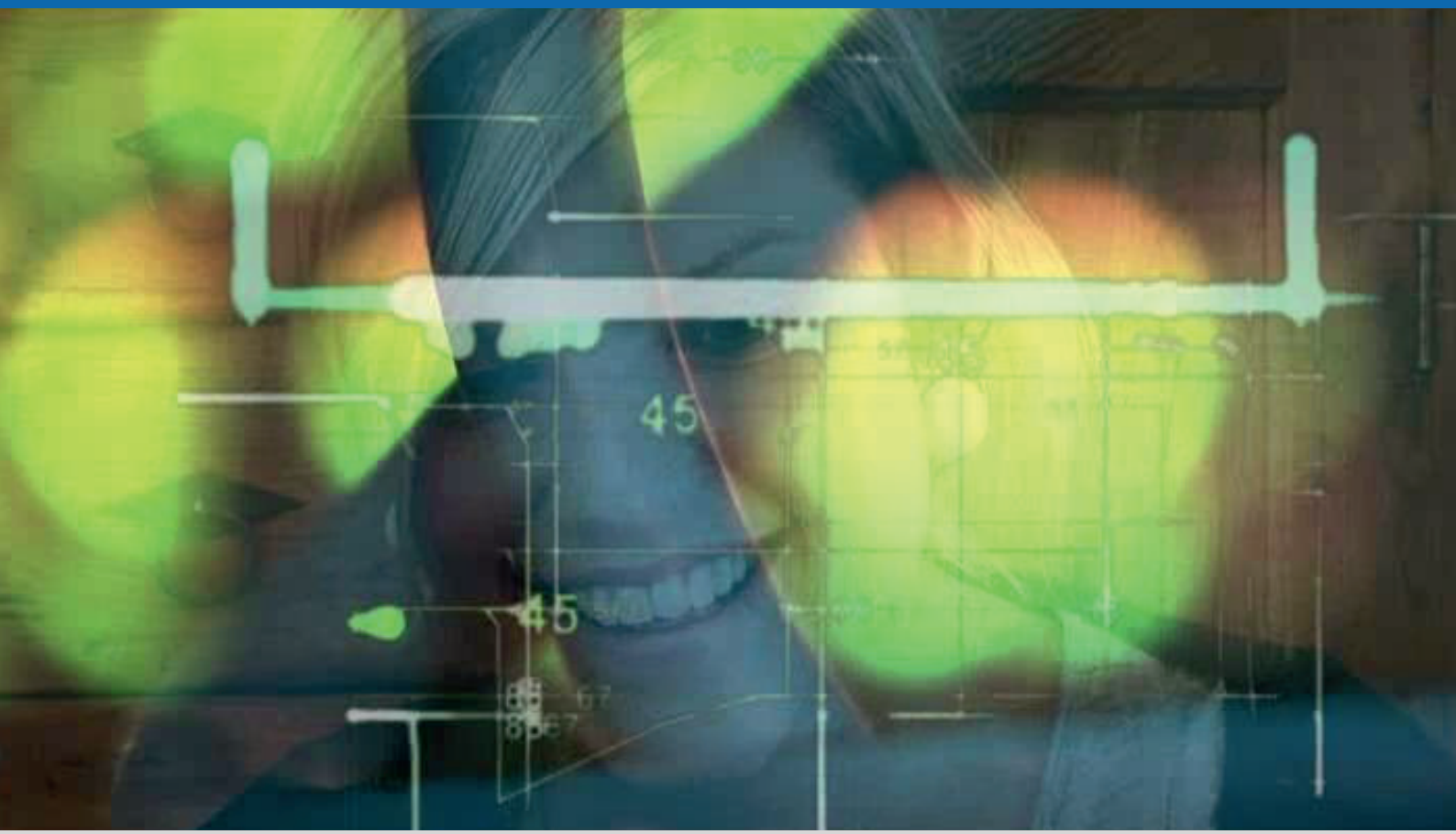
POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich



Smart Home und Connected Home

Sicherheitsempfehlungen für Hersteller, Fachhändler und Handwerker

polizei.nrw.de

if(is) internet-sicherheit.

VdS Vertrauen durch Sicherheit

SMARTHOME DEUTSCHLAND

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 939-4119
E-Mail: einbruchschutz@polizei.nrw.de

www.lka.nrw.de

Alle Rechte vorbehalten.

Stand

September 2014

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

Institut für Internet-Sicherheit - if(is)
Westfälische Hochschule
Fachbereich Informatik und Kommunikation
Neidenburger Str. 43
45897 Gelsenkirchen
Tel.: 0209 9596-763
Fax: 0209 9596-490
E-Mail: office@internet-sicherheit.de

www.internet-sicherheit.de

Inhalt

Abbildungen

Sichere Haustechnik vom professionellen Anbieter

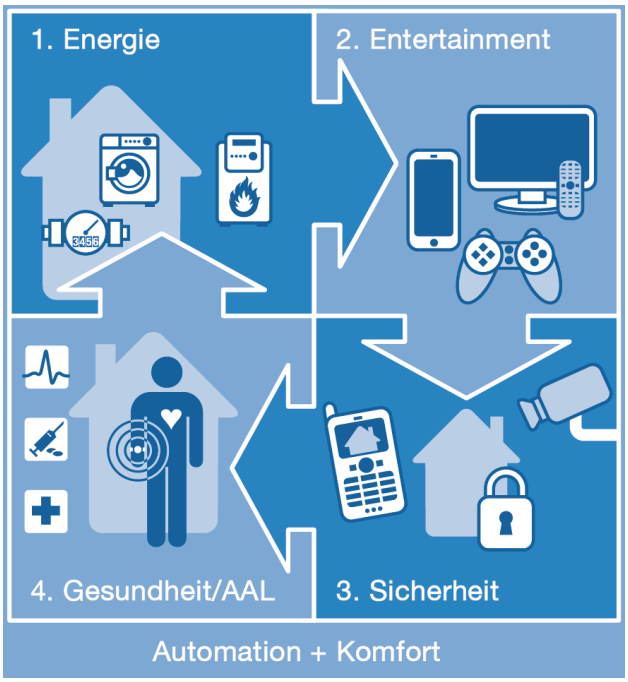
Nicht nur die Unterhaltungselektronik, sondern auch alle Arten von Haushaltsgeräten, automatisierte Beleuchtung, Schließsysteme, Türen, Tore, Fenster, Rollläden, Markisen, die Heizungssteuerung und sogar medizinische Geräte zur Messung von Vitalparametern werden zunehmend mit digitalen Steuerelementen ausgestattet und untereinander vernetzt. Dies wird zusammengefasst durch den Begriff „Smart Home“.

Sie sind Hersteller, Handwerker, Groß- oder Fachhändler und produzieren, vertreiben bzw. installieren digitale Steuersysteme? Dann haben Sie sicher auch Interesse an der Sicherheit Ihrer Produkte bzw. Dienstleistungen. Bedenken Sie, dass digitale Signale auch durch Angriffe Dritter „mitgelesen“ oder manipuliert und damit für illegale Zwecke wie Ausspähen der Wohnungsinhaber, Sabotage oder Einbruch genutzt werden könnten. Mit geeigneten Schutzmaßnahmen schieben Sie solchen Angriffen einen „digitalen Riegel“ vor.

Mit dieser Broschüre möchten die Polizei Nordrhein-Westfalen, die VdS Schadenverhütung GmbH, das Institut für Internet-Sicherheit und die SmartHome Initiative Deutschland e.V. speziell Hersteller, Handwerker, sowie Groß- und Fachhändler über mögliche Gefahren und Schutzmöglichkeiten im Hinblick auf digital gesteuerte und vernetzte Systeme informieren.

Abbildung 01

Anwendungsbereiche und Vernetzung in einem Smart Home



Komplexe Systeme mit angepasster Sicherheit

Smart Home ist stets 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 zusammenwirkenden technischen Systemen ist „eine Kette immer nur so stark wie ihr schwächstes Glied“.

Sicherheitsfunktionen beeinträchtigen in manchen Fällen den Bedienkomfort, aber die Sicherheit Ihrer Kunden und deren Vertrauen in das Produkt sollte im Zweifel im Vordergrund stehen und Anreiz sein, auch bei Sicherheitsmechanismen komfortable Lösungen zu entwickeln. Nur dann werden Sicherungen auch genutzt.

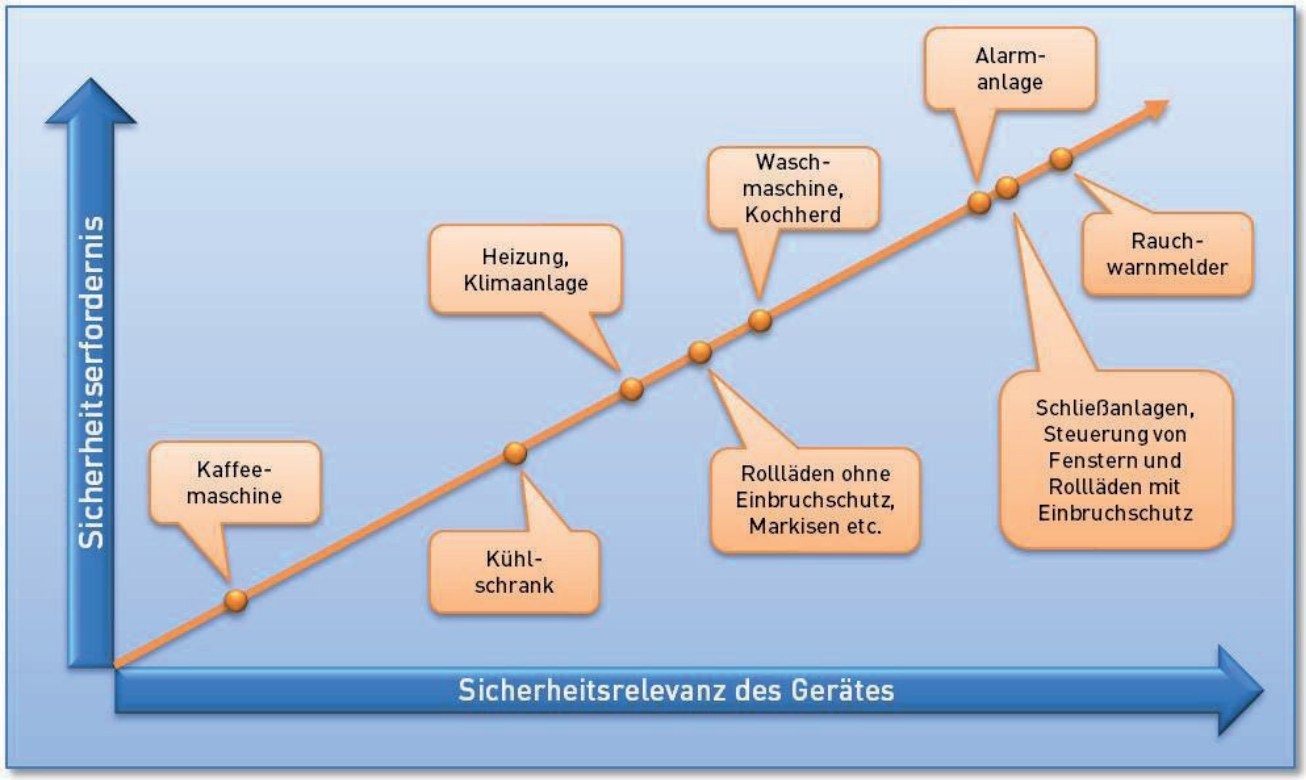
Zu einem hochwertigen Produkt und einer professionellen Dienstleistung gehören die Berücksichtigung von Sicherheitsinteressen und die diesbezügliche Informations- bzw. Aufklärungspflicht des Anbieters. Setzen Sie auf Qualität und zeigen Sie Ihrem Kunden, dass Sie neben Komfortaspekten auch an seine Sicherheit denken!

Nicht jedes Produkt bedarf immer maximaler Sicherheitsausstattung. Passen Sie die Sicherungskomponenten bzw. -funktionen an den Gefährdungsgrad an. Je größer der potentielle Schaden ist, desto höher sind die Sicherheitsanforderungen (vgl. Abbildung 02).

Erläuterungen zu den Fachbegriffen finden Sie im Glossar ab Seite 12!

Abbildung 02

Sicherheitsrelevanz von Smart Home-Geräten



Software sicher programmieren und stetig aktualisieren

Bereits bei der Erstellung des Quellcodes sollte neben der Funktionalität auch der Aspekt IT-Sicherheit berücksichtigt werden.

Jede Software sollte so angelegt werden, dass Programmabläufe und Zugriffe dokumentiert und die Protokolle - vor unberechtigtem Zugriff und Manipulation durch unbekannte Dritte sicher geschützt - abgelegt werden. Damit können Angriffsszenarien minimiert werden.

IT-Sicherheitsmechanismen, die schon bei der Planung einer neuen Software bedacht wurden sind i. d. R. besser als solche, die erst nachträglich implementiert werden müssen. Hochwertige Verschlüsselungen benötigen beispielsweise Rechenleistung und Speicherplatz, der oft knapp bemessen und in bestehenden Designs kaum nachzurüsten ist.

Hersteller sollten hochwertige Verschlüsselungen nach dem Stand der Technik (z. B. AES 128 Bit oder gleichwertig) für zugangsrelevante Produkte und Systemanteile, z. B. User-Interfaces, verwenden.

Insbesondere, wenn Daten zwischen verschiedenen Geräten ausgetauscht werden, sollte die Verschlüsselung der Daten obligatorisch sein.

IT-Sicherheitsmechanismen sollten schon in der Werkseinstellung aktiviert sein, spätestens aber mit Übergabe an den Endkunden aktiviert werden.

Die für die Verschlüsselung notwendigen Informationen müssen dokumentiert werden. Der Kunde ist darauf hinzuweisen, dass diese Daten manipulationsgeschützt und sicher verwahrt werden müssen.

Hersteller, Handwerker, Groß- oder Fachhändler sollten grundsätzlich die aktuelle Soft- und Firmware anbieten, verwenden bzw. in Umlauf bringen und spätestens vor der Übergabe an den Endkunden die ggf. angebotenen Updates installieren.

Prüfen Sie regelmäßig, ob Updates angeboten werden bzw. nutzen Sie die Funktion automatischer Updates. Konfigurieren Sie die Update-Funktion stets so, dass Sie und/oder Ihr Kunde die Kontrolle behalten. Der Endkunde bzw. Anwender muss immer erkennen können, ob ein angebotenes Update lediglich neue Funktionen beinhaltet, auf die ggf. verzichtet werden kann oder ob es sich um ein sicherheitsrelevantes Pflichtupdate handelt. Letzteres sollte immer besonders hervorgehoben und ggf. automatisch installiert werden. Updates, die lediglich die Funktionalität verbessern oder verändern, sollten vom Kunden vor der Installation

freigegeben werden. Damit ein Kunde erkennen kann welche Software-Version aktuell zum Einsatz kommt, sollten Ihre Produkte so konfiguriert werden können, dass die aktuelle Versions-Nummer der aufgespielten Software im Geräte-Display immer sichtbar oder zumindest einfach aufzurufen ist.

Sie als Hersteller oder Dienstleister tragen die Verantwortung dafür, dass Ihre Kunden über erforderliche Sicherheits-Updates umgehend informiert werden und diese zeitnah auf betroffenen Geräten einspielen können.

Bieten Sie Ihren Kunden aktuelle Produktinformationen und Unterstützung bei Software-Updates an. Dazu können Sie beispielsweise eine Verbraucherplattform im Internet einrichten. Nach Selbstregistrierung durch den jeweiligen Kunden, wird dieser z. B. per E-Mail informiert, wenn neue Updates verfügbar sind. Sie könnten Ihren Kunden für die Registrierung ggf. einen Bonus, beispielsweise in Form einer Supportleistung oder der Verlängerung der Gewährleistung, anbieten.

Sicherheitsrelevante Software-Updates sollten im Rahmen Ihrer Produktverantwortung grundsätzlich kostenlos angeboten werden. Hilfe beim Aufspielen sicherheitsrelevanter Updates sollten Sie möglichst kostengünstig anbieten. Nur so erhalten Sie auf Dauer das Vertrauen Ihrer Kunden.

Abbildung 03

Steuerungsmodul und Zugangskontrolle

Grundlagen für ein sicheres Heimnetzwerk schaffen

Je größer die Sicherheitsrelevanz eines Gerätes und je größer der durch unberechtigten Fremdzugriff zu verursachende Schaden, desto sicherer muss der Übertragungsweg gewählt werden (vgl. Abbildung 02). Bei den Übertragungswegen bieten Glas-/Plastikfasern die höchste Manipulations- und Abhörsicherheit, separate Kupferkabel und sog. Powerline-Übertragung mittlere Sicherheit. In Powerline-Adaptern muss die Verschlüsselungsfunktion aktiviert sein.

Im Zweifel ist ein leitungsgebundener Übertragungsweg dem WLAN oder anderen Funk-Übertragungswegen immer vorzuziehen. Ist der Einsatz eines WLAN-Netzwerkes durch bestimmte bautechnische Umstände unausweichlich, sollte mindestens eine WPA2-Verschlüsselung mit komplexem und langem Passwort verwendet werden.

Mobile Endgeräte wie Mobiltelefone, Smartphones und Tablet-PCs, die über eine WLAN-Verbindung des Hausnetzes auf das Internet zugreifen oder über eine App Steuerungsfunktionen im Haus bedienen, sind - ungeschützt - ein offenes Tor für Angreifer. Daher sind Sicherheitsfunktionen auch auf allen Endgeräten und in der jeweiligen App vorzusehen und zu nutzen.

Klären Sie den Endkunden darüber auf, dass jedes Endgerät mit einer aktuellen Firewall und stets aktuellem Virenschutz versehen sein muss, sofern das technisch umzusetzen ist.

Konfigurieren Sie das Hausnetz so, dass der WLAN-Zugriff nur mit einem sicheren Passwort möglich ist, das der Kunde nur an berechtigte Personen weitergeben darf.

Geben Sie Ihrem Kunden den Hinweis, dass er den Kreis der Personen, die Detailwissen zur Sicherheitsarchitektur, Benutzernamen und Kennwörtern erhalten, so klein wie möglich halten soll. Ggf. sollte der Administrator (Hausbesitzer) beim erstmaligen „einloggen“ von neuen Benutzern oder neuen Endgeräten - z. B. in ein WLAN - die Kennworteingabe selbst vornehmen und das Kennwort dabei nicht bekannt geben.

Sichere Hardware verwenden

Geräte-Hardware sollte bei erkannter Gefahr (unberechtigter Fremdzugriff, Manipulation, Sabotage etc.) automatisch eine physikalische Trennung vom Internet vornehmen und ggf. das Gerät herunterfahren. Die Trennung sollte nach Ablauf einer vorgegebenen Zeit automatisch wieder aufgehoben werden, um berechtigte Zugriffe wieder zu erlauben.

Bei häufigen und unberechtigten Zugriffsversuchen können auch einzelne Netzwerkteilnehmer gesperrt bzw. mit einer Zeitsperre belegt werden.

Digitale Technik sicher planen und installieren

Bevor Sie mit der Installation beginnen, muss die digitale Haussteuerung, insbesondere deren Vernetzung unter Einbindung des Endkunden sorgfältig geplant werden. Erstellen Sie hierzu für sich und Ihren Kunden einen Netzwerk- und Installationsplan als Arbeitsgrundlage und für Dokumentationszwecke.

Klären Sie bei der Planung mit dem Endkunden, welche Funktionen er jetzt oder ggf. später benötigt. Berücksichtigen Sie auch Aspekte des Alterns. So kann z. B. ein Dachfenster, das für junge Menschen noch gut zu bedienen ist, im Alter unerreichbar werden. Wer dann schon eine elektrische Bedienung vorgesehen hat, spart sich aufwändige Nachbesserungen. Auch die Möglichkeit des Einbindens persönlicher Notfallmelder von Anbietern der Notfallhilfe und Altenfürsorge sollte frühzeitig bedacht und ggf. vorbereitet werden.

Klären Sie, wo Netzwerkkabel wirklich erforderlich sind oder wo ggf. bloße Steuerleitungen ausreichen. Verlegen Sie Netzwerkkabel und andere sicherheitsrelevante Leitungen immer verdeckt und schützen Sie frei zugängliche Leitungen durch Metallrohre o. Ä. Vor allem im Außenbereich sollten keine Netzwerkanschlüsse zugänglich sein. Auch BUS-Leitungen der Gebäudetechnik sind im Außenbereich nach Möglichkeit zu vermeiden, um die Angriffsmöglichkeiten zu minimieren.

Die Geräte der digitalen Steuerungs- und Netzsysteme müssen sicher untergebracht werden. Dazu sollten sie immer im Gebäude, beispielsweise in einem gesonderten, abschließbaren Schaltschrank oder in einem abschließbaren Raum des Hauses platziert werden. Die Geräte sollten niemals in Schuppen oder Garagen und - wo immer es vermeidbar ist - nicht an Außenwänden montiert werden. Achten Sie bei der Planung darauf, dass die Schaltschränke und andere Installationen im Falle von Hochwasser oder Leitungswasserschäden nicht sofort beeinträchtigt werden können.

Zur Funktionssicherheit und zum Schutz vor Sabotage und unberechtigten Fremdzugriffen, sollten

- Leitungen nicht mit Steckanschlüssen, sondern mit Schraubverbindungen angeschlossen werden,
- Gehäuse mit besonderen Schrauben gesichert werden, die spezielle - nicht für jedermann verfügbare - Öffnungswerkzeuge erfordern,

und

- für Unbefugte leicht zugängliche Kabel z. B. durch verdeckte Verlegung und/oder Metallrohre geschützt werden.

Die komplette Hauselektrik und insbesondere die digitalen Steuerungs- und Netzsysteme müssen vor Überspannung und Blitzeinschlag geschützt werden, um Fehlfunktionen und Ausfall zu verhindern.

Die digitalen Steuerungs- und Netzsysteme, sowie die Außenelektrik sollten jeweils mit separaten Fehlerstrom-Schutzschaltern abgesichert werden. Außensteckdosen sind zudem stets vollständig vom Netz zu trennen, wenn sie nicht benötigt werden. Dazu sind zweipolige Schalter geeignet, die sowohl den „stromführenden“ Leiter als auch den Nullleiter schalten.

Ein modernes Hausnetzwerk sollte über einen zentralen Schalter verfügen, dessen Funktion beim Verlassen des Hauses nur noch die unbedingt notwendigen Geräte eingeschaltet lässt und ansonsten alle Geräte ausschaltet und ggf. sogar die Wasserleitungen verschließt. Dadurch kann nicht nur der unberechtigte Fremdzugriff auf Steuerungstechnik, sondern auch die Gefahr von Feuer- und Wasserschäden deutlich reduziert und der Energieverbrauch merklich verringert werden.

Netzwerke sicher konfigurieren und erhalten

In IT-Netzwerken hat jedes eingebundene Gerät eine sog. MAC-Adresse. Als Basisschutz eines WLAN-Netzwerkes sollte in der Firewall des Routers ein sog. MAC-Filter eingerichtet werden. Dabei handelt es sich um einen Zugangsschutz, der nur Geräten mit vorab registrierter MAC-Adresse - also nur vom Nutzer freigegebnen Geräten - Zugang zum Netzwerk gestattet. Vermeiden Sie wenn möglich das sog. DHCP zur automatischen Einbindung von Rechnern in das Hausnetzwerk. Vergeben Sie stets feste IP-Adressen und weisen Sie diese jedem Endgerät zu.

Trennen Sie Netzwerke in sinnvolle Gruppen. So kann beispielsweise jeder berechtigte Nutzer im Haus Zugriff auf das Internet und die Unterhaltungselektronik bekommen, aber nur bestimmte Personen Zugriff auf das Netz für die übrige Hausteuerung. Sicherheitsrelevante Technik wie Videoüberwachung und Einbruchmeldeanlagen sollte immer in einer separaten Gruppe von der übrigen Technik administriert werden.

Network Video Recorder (NVR) sollten in einem eigenen Netzwerk betrieben werden, um Zugriffe auf andere Netzkomponenten über die Videoverkabelung zu verhindern

Topologische Planung in der Heimvernetzung

In der Informationstechnik wird zwischen physischen und logischen Netztopologien unterschieden. Die physische und die logische Topologie eines Netzes sind nicht notwendig identisch. Bei der logischen Netztopologie handelt es sich um die Zuordnung von Datenflüssen. Sie kann durch die Konfiguration der aktiven Netzkomponenten fast beliebig gestaltet werden. Durch „virtuelle“ lokale Netze lassen sich zusätzliche logische Strukturen in Netzen bilden.

Heim-Netzwerke sollten möglichst nach dem Einsatzzweck der jeweiligen Gerätegruppe strukturiert werden. Orientieren Sie sich dabei an folgenden Überlegungen:

- Welche Geräte, z. B. Hausgeräte, Videotechnik, Gebäudetechnik, sollen bzw. müssen direkt miteinander kommunizieren und sollen daher in einem Netzwerkbereich zusammengefasst werden?
- Welche Geräte müssen mit dem Internet kommunizieren und welche Geräte können ggf. vom Internet getrennt bleiben?
- Welche Netzwerkteilnehmer haben ein hohes Datenaufkommen und sollten z. B. über einen „Gigabit-Switch“ in einem gesonderten „schnellen“ Netzwerkbereich zusammengefasst werden?

Funktions- und Adressbereiche für Heimnetzwerke

Wenn Sie den elektronischen Geräten (Notebooks, Smartphones, Tablet-PCs, IP-Kameras, Spielekonsolen, Smart-TVs etc.) feste IP-Adressen zuweisen, können Sie Ihr Netzwerk klar strukturieren und verwalten. Die interne IP-Adresse besteht dabei aus vier Zahlenblöcken, die sich aus einem Netzwerk-Teil (die ersten drei Zahlenblöcke) und dem eigentlichen Gerät - dem sog. Host - zusammensetzen. Um den Überblick über die Geräte- und Verwendungsarten zu behalten, sollte man die Einteilung in Segmente außerhalb des ggf. noch bestehenden DHCP-Bereiches vornehmen.

Abbildung 04

Beispiel für die Struktur von Funktions- und Adressbereichen in einem Heimnetzwerk

Nr.	Gerätename	IP-Adresse	Subnetzmaske	Hinweise (Beispiele)
Systemgeräte		Netzwerk | Host		
01	WLAN-Router mit DSL- / Kabel-Modem	192.168.1. 1	255.255.255.0	
Mobile Endgeräte über WLAN				
04	Black Berry Vater	192.168.1.30	255.255.255.0	
05	iOS Smartphone Mutter	192.168.1.32	255.255.255.0	
06	Android Smartphone Kind	192.168.1.33	255.255.255.0	Kinderschutz u. Nachtschaltung
07	Android Tablet	192.168.1.34	255.255.255.0	Kinderschutz u. Nachtschaltung
Unterhaltungselektronik				
08	Smart-TV Wohnzimmer	192.168.1.50	255.255.255.0	
09	Smart-TV Kinderzimmer	192.168.1.51	255.255.255.0	Kinderschutz u. Nachtschaltung
10	BluRay-Player Wohnzimmer	192.168.1.52	255.255.255.0	
11	Spielekonsole Kinderzimmer	192.168.1.53	255.255.255.0	Kinderschutz u. Nachtschaltung
12	NAS–Netzwerkfestplatte „Media-Server“	192.168.1.54	255.255.255.0	Nachtschaltung
Sicherheitstechnik ohne Zugriff auf das Internet				
13	Network Video Recorder (NVR)	192.168.1.60	255.255.255.0	Zugriff über Web-Interface
14	PTZ IP-Kamera Hinterhof	192.168.1.61	255.255.255.0	Zugriff über App
15	Fixed Dome IP-Kamera-Treppenhaus	192.168.1.62	255.255.255.0	Zugriff über App
16	IP-Kamera in der Türkommunikation	192.168.1.63	255.255.255.0	Zugriff über App

Durch die Verwendung einer solchen Struktur (vgl. Abbildungen 01 und 04) behalten Sie und Ihr Kunde die Übersicht über das Heimnetzwerk und dessen Teilnehmer. Des Weiteren fallen Geräte schneller auf, die ggf. nicht in das Netzwerk gehören.

Neben der Strukturierung über die IP-Adresse kann ein lokales Netzwerk mit einem geeigneten Router und der Nutzung von virtuellen Netzwerken (VLAN) in mehrere kleinere Netzwerke aufgeteilt werden. So lassen sich einzelne Netzwerkbereiche klar voneinander abgrenzen, um beispielsweise einzelne Bereiche oder Geräte aus Sicherheitsgründen voneinander zu trennen und/oder den Netzwerkverkehr zu beschleunigen.

Sichere Passwörter erstellen und verwalten

Viele Geräte sind schon mit Passwörtern gegen unberechtigte Zugriffe und Manipulation geschützt. Passwörter werden aber leider allzu oft als lästiges Übel betrachtet und aus Gründen der Bequemlichkeit zu kurz und zu einfach gewählt oder nicht sicher verwahrt. Sorgloser Umgang mit Passwörtern ist eine der größten Schwachstellen bei der Nutzung digitaler Geräte.

Die beste Verschlüsselung wird wertlos, wenn kein sicheres Passwort benutzt wird!

Sichere Passwörter sind aus möglichst vielen Zeichen zusammengesetzt und verwenden Kombinationen von großen und kleinen Buchstaben, Ziffern und Sonderzeichen.

Nutzen Sie für verschiedene Geräte und Zugänge auch unterschiedliche Passwörter. Ändern Sie besonders sensible Passwörter regelmäßig.

Hersteller sollten in der Grundkonfiguration ihrer Geräte niemals allgemeine Herstellerpasswörter verwenden, sondern immer ein individuelles Passwort für jedes ausgelieferte Gerät vergeben.

Ein integrierter **Passwortgenerator** - sprich eine Softwarekomponente, die Passwörter erstellt und vorschlägt - kann dem Handwerker und/oder Endkunden das Einrichten eines sicheren Passwortes bei der Erstkonfiguration und der regelmäßigen Passwortänderung erleichtern.

Ein sogenannter **Passwortmanager** kann helfen, die Vielzahl der Passwörter sicher zu verwahren, resp. zu speichern. Diese Software speichert Ihre Passwort-Daten verschlüsselt. 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.

Nutzen Sie selbst sichere Passwörter und klären Sie Ihre Kunden hinsichtlich sicherer Passwörter und deren Aufbewahrung auf. Passwörter gehören niemals in die Bedienungsanleitung oder an das Gerät, sondern sind immer davon getrennt und sicher aufzubewahren. Weisen Sie Ihren Kunden darauf hin!

Mit Übergabe der Anlage bzw. des Gerätes gehören auch die Passwörter dem Kunden. Die sichere Aufbewahrung eines Servicepasswortes beim Hersteller oder Handwerker muss gesondert mit dem Kunden vereinbart werden, wenn der Kunde dies wünscht.

Passwörter für den Service-Zugriff auf Kundengeräte sollten beim Handwerker nicht digital verwaltet werden, sondern z. B. in verschlossenen Umschlägen in einem Wertbehältnis aufbewahrt werden. Dokumentieren Sie auf dem Umschlag wer diesen wann und zu welchem Zweck geöffnet hat. Digitale Steuerungssysteme, die eine Fernwartungsfunktion haben, sollten mit einer Freigabetaste versehen sein, mit deren Betätigung der betroffene Endkunde den Fernzugriff vor Ort manuell zulassen muss. Der Endkunde behält somit die Kontrolle über sein System. Das kann auch das Vertrauen des Kunden in die Technik und den verantwortlichen Dienstleistungsbetrieb stärken.

Erforderliche Funktionen prüfen und beschränken

Hersteller sollten schon bei der Programmierung vorsehen, dass einzelne Funktionen optional de-/aktiviert werden können. Handwerker sollten zusammen mit dem Kunden prüfen, welche Funktion der Steuerungstechnik wirklich benötigt werden.

Für jedes Gerät ist insbesondere zu klären, ob eine Verbindung zum Netzwerk oder Internet erforderlich ist. Benötigt der Kunde wirklich Fernzugriff über das Internet oder reicht ihm die Information über relevante Prozesse und Warnmeldungen per SMS oder E-Mail?

Spätestens nach einer Nutzungsdauer von einem Jahr sollte durch den Endkunden nochmals kritisch geprüft werden, ob und welche Funktionen in der täglichen Praxis tatsächlich genutzt und benötigt wurden resp. werden. Bieten Sie Ihrem Kunden spätestens nach einem Jahr einen Sicherheitscheck an, der auch diese Frage klärt. Raten Sie Ihrem Kunden, nicht benötigte Funktionen zu deaktivieren, wenn dadurch ein Sicherheitsgewinn erreicht werden kann. Geräte und Netzwerkkomponenten sollten immer ausgeschaltet werden, wenn Sie nicht in Funktion sind. WLAN-Router und Funktionen sollten immer nur eingeschaltet werden, wenn sie tatsächlich von einem berechtigten Nutzer benötigt werden. Oft bieten Router Zeitsteuerungen an, welche das WLAN zu bestimmten Uhrzeiten (z. B. nachts) automatisch aus- und einschalten können.

Verantwortlich handeln und umfassend informieren

Nehmen Sie Ihre Informations-/Aufklärungspflicht als Hersteller, Fachhändler oder Handwerker wahr und tragen Sie dafür Sorge, dass Ihr Kunde in das Gesamtsystem so umfassend eingewiesen wurde, dass er sich mit der Bedienung der wesentlichen Funktionen auskennt und auch wohlfühlt.

Dokumentieren Sie die Übergabe an den Kunden, z. B. in einem Übergabeprotokoll.

Stellen Sie Ihrem Kunden alle erforderlichen Produktinformationen, eine leicht verständliche Bedienungsanleitung und Sicherheitsinformationen zur Verfügung. Nutzen Sie dazu auch das Merkblatt „Empfehlungen zur Sicherung digitaler Haustechnik“ für Anwender, welches vom LKA NRW gemeinsam mit der VdS Schadenverhütung GmbH und der SmartHome Initiative Deutschland e.V. herausgegeben wird.

In Hausnetzwerken, die von mehreren Personen genutzt werden, ist es grundsätzlich auch möglich, Aktivitäten einzelner Nutzer zu überwachen. Sprechen Sie mit Ihren Kunden über Sicherheit von Computersystemen und Datenschutz auch in der Familie. Klären Sie darüber auf, wie Kindersicherungen installiert und Nutzerprofile eingerichtet und geschützt werden können.

Ihr Kunde muss nach der Übergabe und Bezahlung über die weitere Verwendung des gekauften Gerätes selbst bestimmen können. Dazu gehört auch die Entscheidung, wem er die Wartung oder Reparaturaufträge erteilt. Bleiben Sie fair! Halten Sie keine Informationen - insbesondere keine Passwörter - zurück, wenn der Kunde das nicht ausdrücklich mit Ihnen vereinbart, z. B. im Rahmen eines Wartungsvertrages.

Nach der Übergabe trägt natürlich auch der Kunde Verantwortung für die Sicherheit seiner digitalen Haustechnik. Lassen Sie Ihren Kunden damit nicht allein, sondern bieten Sie ihm auch nach der Übergabe noch Unterstützungsleistungen an.

Lassen Sie Ihren Kunden bedarfsgerechte aktuelle Informationen z. B. als Newsletter per E-Mail zukommen.

Sicherheitsrelevante Informationen sollten dabei immer besonders gekennzeichnet und hervorgehoben werden. Gerade die professionelle Betreuung „nach dem Verkauf“ wird von Kunden häufig als besonders wichtig empfunden und geschätzt, worin auch hohes Bindungspotential liegt. Beweisen Sie Ihren Kunden, dass Ihr Service nicht mit der Rechnungsstellung endet.

Weiterbilden und Fachkompetenz erlangen

Bieten Sie nur Produkte und Dienstleistungen an, mit denen Sie sich wirklich auskennen und die Sie Ihren Kunden mit gutem Gewissen verkaufen können. Wenn Sie mit einzelnen Produkten keine ausreichende Erfahrung haben oder für bestimmte Leistungen nicht die erforderliche Qualifikation besitzen, suchen Sie sich bitte kompetente Unterstützung.

Bilden Sie mit anderen Anbietern Netzwerke und Kooperationen, um Ihren Kunden Komplettlösungen anbieten zu können. Das spart Ihnen auch Kosten, weil Ihre Techniker nicht „stundenlang“ Systeme konfigurieren oder darin Fehler suchen müssen, auf denen sie nicht geschult sind.

Der Experte sollte mehr können als Geräte mit „Plug & Play“-Funktionalität zu installieren. „Plug & Play“ ist in der Regel auf maximale Kompatibilität und einfache Inbetriebnahme ausgerichtet. Dabei werden mitunter viele IT-Sicherheitsmechanismen nicht aktiviert und Sie haben keinen Überblick über die durchgeführten Einstellungen. Hersteller sollten Installations-Checklisten zur manuellen Inbetriebnahme bzw. Konfiguration durch den Handwerker oder Fachhändler anbieten. Vermeiden Sie die „Plug & Play“-Funktion, wenn sich daraus ein Sicherheitsrisiko ergeben könnte. Richten Sie die Software besser manuell ein.

Stellen Sie ggf. geeignetes Fachpersonal ein und bieten Sie auch Ihren Angestellten die Teilnahme an Fortbildungen an. Einschlägige Seminare bieten Fachverbände oder Hersteller an.

Weitere Informationen zum Thema IT-Fortbildung für Handwerksbetriebe oder Betriebe des Fachhandels finden Sie im Internet z. B. unter:
https://www.it-sicherheit-handwerk.de/

Allgemeine Informationen zur IT-Sicherheit finden Sie unter:

www.bsi.de (Suchbegriff: IT-Grundschutz)

www.bsi-fuer-buerger.de

www.internet-sicherheit.de

Wenn Sie nicht selbst oder wenigstens einer Ihrer Mitarbeiter einschlägig aus- bzw. fortgebildet sind, suchen Sie professionelle Hilfe beim Hersteller oder einem kompetenten Partner vor Ort. Dies gilt insbesondere auch, wenn Sie auf Hard- oder Software-Probleme stoßen, die Sie selbst nicht lösen können.

Einbruchschutz als Grundlage eines sicheren Smart Home

Grundlage eines individuellen Sicherungskonzeptes gegen Einbruchdiebstahl sollten immer mechanisch-bauliche Sicherungseinrichtungen sein.

Zeigen Sie, dass Sie mehr wissen! Informieren Sie Ihre Kunden über das kostenlose Beratungsangebot der Polizei zum Einbruchschutz. Weisen Sie auch auf die Informationsangebote, wie z. B. das Faltblatt "Tipps für mehr Sicherheit: Schlagen Sie Alarm!" und die Broschüre "Ungebetene Gäste" des Programms Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) hin, welche detaillierte Informationen zum Einbruchschutz enthalten.

Insbesondere, wenn das Smart Home auch eine Alarmfunktion beinhaltet, sollte Ihr Kunde im Vorfeld mit dem Versicherer sprechen, denn: In manchen Fällen fordern Versicherer die Installation einer Überfall-/Einbruchmeldeanlage mit sogenanntem “VdS-Attest”. Dann werden an den Errichter sowie an die eingesetzten Produkte sowie Planung und Einbau der Anlage besondere Anforderungen gestellt.

Weitere Informationen zum Einbruchschutz finden Sie im Internet unter:

www.vds-home.de

www.k-einbruch.de

www.riegelvor.nrw.de

www.polizei-beratung.de

www.smarthome-deutschland.de

Glossar

AES

Der Advanced Encryption Standard (AES) ist eine Blockchiffre. Die Bezeichnungen der drei AES-Varianten AES-128, AES-192 und AES-256 beziehen sich jeweils auf die gewählte Schlüssellänge.

BUS

Ein „BUS“ (englische Abkürzung von Binary Unit System) ist ein Datenübertragungssystem zwischen mehreren Endstellen (Teilnehmern) über einen gemeinsamen Übertragungsweg, wobei jede Endstelle nur die für sie bestimmten Informationen erhält bzw. abrufen kann.

DHCP

Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Computertechnik. Durch DHCP ist die automatische Einbindung eines Computers in ein bestehendes Netzwerk ohne dessen manuelle Konfiguration möglich. An dem Computer, dem Client, muss dann i. d. R. lediglich der automatische Bezug der IP-Adresse eingestellt sein. Ohne DHCP sind dazu häufig einige Einstellungen nötig.

Einloggen

Als Login oder Log-in (von engl. to log in = „einloggen“, „anmelden“ wird der Vorgang bezeichnet, bei dem Benutzer sich in einem Computersystem bzw. bei einem speziellen Dienst anmelden. Das sog. „Einloggen“ in ein System erfolgt i. d. R. durch Abfrage eines Benutzernamens und eines Passwortes. Nach erfolgter Authentifizierung erhält der Benutzer Zugang zu dem System.

E-Mail

Eine E-Mail oder (engl. electronic mail für elektronische Post) ist eine auf elektronischem Weg in Computernetzwerken übertragene Nachricht. Per E-Mail können Textnachrichten und digitale Dokumente typischerweise in Sekunden weltweit zugestellt werden.

Firewall

Eine Firewall (von englisch firewall für „Brandmauer“) ist ein Sicherungssystem, das einen Computer oder ein Netzwerk vor unerwünschten Zugriffen schützt.

Gigabit-Switch

In Computer-Netzwerken wird als Gigabit-Switch (Switch = engl. für „Schalter“) ein Kopplungselement bezeichnet, das Netzwerksegmente miteinander verbindet und Datenströme größer als 1000-Mbit/s ermöglicht.

IP

Über das Internetprotokoll (IP) erfolgt die Adressierung (IP-Adresse) von Rechnern im Internet.

IT

Informationstechnik (oder engl. information technology) ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software.

LAN

Als Local Area Network (deutsch wörtlich „lokales Netzwerk“) wird ein lokales Netz zur Datenübertragung bezeichnet.

MAC-Adresse

Die MAC-Adresse (MAC von engl. Media-Access-Control) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters. Sie dient zur eindeutigen Identifizierung von Geräten in einem Computernetz.

MAC-Filter

Ein MAC-Filter ist ein Netzwerk-Zugangsschutz, der nur Geräten mit bestimmter MAC-Adresse Zugang zum Netzwerk gestattet. Typischerweise wird ein MAC-Filter in einem LAN oder WLAN eingesetzt und in Form einer Tabelle in der Firewall des Routers abgelegt.

Network Video Recorder

Ein Network Video Recorder (NVR) ist ein Gerät zur Aufzeichnung von digitalen Videosequenzen, die von Netzwerkkameras bereitgestellt werden, auf einer integrierten Festplatte. Manche Geräte bieten auch zusätzliche Anschlussmöglichkeiten für externe Speichermedien.

Plug & Play

Mit Plug and Play (englisch für „einstecken und abspielen“ oder „anschließen und loslegen“), auch Plug’n Play oder Plug and Play (kurz PnP) wird die Eigenschaft eines Computers beschrieben, neue, meist Peripherie-Geräte anschließen zu können, ohne Gerätetreiber zu installieren oder Einstellungen vornehmen zu müssen.

Powerline-Übertragung

Bei der sog. Powerline-Übertragung werden digitale Signale über das allgemeine Hausstromnetz, die Powerline (engl. Stromleitung), übertragen

Ports

Während die IP-Adresse sicherstellt, dass der richtige Rechner die Datenpakete erhält, können über die Ports den verschiedene Anwendungen auf einem Rechner (z. B. Browser und E-Mail-Software) Datenpakete zugewiesen werden.

Router

Router sind Netzwerkgeräte, die Daten zwischen unterschiedlichen Netzen weiterleiten können. Sie werden u. a. zur Anbindung eines Heimnetzwerks oder Rechners an das Internet eingesetzt.

Smart Home

Unter dem Begriff Smart Home (engl. für "intelligentes Zuhause") wird zusammenfassend die digitale Steuerung und Vernetzung von Unterhaltungselektronik, Gebäudetechnik und sogar medizinischer Geräte verstanden.

Smartphone

Ein Smartphone ist ein Mobiltelefon (umgangssprachlich *Handy*), das mehr Computer-Funktionalität und -konnektivität als ein herkömmliches Mobiltelefon zur Verfügung stellt.

SMS

Short Message Service (engl. für Kurznachrichtendienst) ist ein Telekommunikationsdienst zur Übertragung von Textnachrichten, die meist Kurzmitteilungen oder ebenfalls SMS genannt werden.

Tablet-PC

Ein Tablet-PC (engl. für Schreibtafel oder Notizblock) ist ein tragbarer, flacher Computer in besonders leichter Ausführung mit einem Touchscreen und ohne ausklappbare mechanische Tastatur.

Touchscreen

Ein Touchscreen (engl. etwa für „berührungsempfindlicher Bildschirm") ist ein kombiniertes Ein- und Ausgabegerät, bei dem durch Berührung von Teilen eines Bildes der Programmablauf eines technischen Gerätes, meist eines Computers, direkt gesteuert werden kann.

User-Interface

Die Benutzerschnittstelle, mit der ein Mensch mit einer Maschine in Kontakt tritt, z. B. Tastatur, Maus oder Touchscreen.

VdS-Attest

Die ordnungemäße Planung und Errichtung der Gefahrenmeldeanlage wird im Installationsattest dokumentiert. Das Formular ist elementarer Bestandteil von VdS-anerkannten Einbruchmeldeanlagen. Es dient sowohl zur Beschreibung der Anlage, als auch zur Absicherung aller Beteiligten.

VLAN

Ein Virtual Local Area Network (deutsch wörtlich „virtuelles lokales Netzwerk“) ist eine logisches Teilnetz, welches von weiteren Teilnetzen durch ein Switch oder einem VLAN-fähigen Router getrennt werden kann.

WLAN

Als Wireless Local Area Network (deutsch wörtlich „drahtloses lokales Netzwerk“) wird ein lokales Funknetz zur Datenübertragung bezeichnet.

WPA2 ist der gängige WLAN-Verschlüsselungsstandard und muss mit einem komplexen Passwort versehen werden.

Notizen

Landeskriminalamt Nordrhein-Westfalen

Völklinger Straße 49 I 40221 Düsseldorf
Tel.: 0211 939 0
poststelle@lka.nrw.de I www.lka.nrw.de

Diese Broschüre wurde überreicht durch: