

## Methodik

Die kontinuierliche Technologiebeobachtung des HPI hat die Aufgabe, die für die handwerkliche Leistungserbringung relevanten (technologischen) Innovationen frühzeitig zu erkennen. Mittels Qualifikationsmonitoring ist zu prüfen, ob die bestehenden technischen Qualifizierungen im Handwerk die aus dem Umgang mit Innovationen entstehenden Anforderungen abdecken. Hierfür beobachtet die Zentrale Leitstelle für Technologietransfer im Handwerk (ZLS) aus betrieblicher Sicht, welche technologischen Neuerungen und Innovationen relevant für den Erhalt künftiger Wettbewerbsfähigkeit sind. Das HPI analysiert aus berufsqualifikatorischer Sicht, welche Qualifikationsanforderungen sich aus technologischen Neuerungen ergeben.



Abb.1: Ermittlung des Qualifikationsbedarfs

Die ZLS stützt sich für die technologische Bewertung aus betrieblicher Sicht auf das Netzwerk der Beauftragten für Innovation und Technologie (BIT) und bezieht damit die betriebliche Perspektive mit ein. Neben der formalen Analyse von Qualifikationsbedarfen und vorhandenen Bildungsangeboten basiert das Qualifikationsmonitoring des HPI insbesondere auf Informationen aus der Fachverbandsebene, wissenschaftlichen Netzwerken und der gewerblich-technischen Berufsbildung.

## Technische Verfahren/Funktionsprinzip

Die Umschreibung Smart Home, häufig auch mit Begriffen wie "Intelligentes Wohnen" oder "Smart Living" in Verbindung gebracht, steht für eine intelligente Verknüpfung von technischen Komponenten im privaten Wohnraum. Basis für ein Smart Home ist die gezielte Vernetzung von Komponenten aus den Bereichen Haustechnik, Haushaltsgeräte oder Entertainment (Abbildung 2). Sie ermöglicht eine automatische Kommunikation der einzelnen Komponenten untereinander, bei Bedarf auch das zentrale Steuern oder Regeln einzelner Komponenten. Wesentliche Aufgaben von Smart Home-Anwendungen sind unter anderem, den Komfort zu steigern, mehr Sicherheit für die Bewohner zu gewährleisten oder Energie zu sparen (Saena 2016). In diesem Technologie-Steckbrief wird speziell der Bereich „Smart Home – Sicherheit“ betrachtet.

Grundsätzlich sollte zu Beginn entschieden werden, ob es sich um eine VdS-zertifizierte (Vds = Verband der Sachversicherer) Anlage oder um eine nicht zertifizierte Anlage handeln soll. VdS-zertifizierte Anlagen haben den Vorteil, dass alle verwendeten Bauteile, Systeme, Dienstleistungen und Geräte dem Stand der Technik und den höchsten Prüfanforderungen entsprechen. So verlangen Versicherungsunternehmen im Zusammenhang mit der Versicherung hoher Sachwerte zur Verringerung ihres Risikos häufig eine Objektsicherung durch eine VdS-zertifizierte Anlage. Des Weiteren sind ggf. verschiedene Normen und Richtlinien zum Thema Einbruchmeldetechnik wie z.B. DIN VDE 0833 (2014), DIN EN 50131 (2017), DIN EN 50136 (2012) sowie VDS 2311 (2017) und Anforderungen an Leitungsnetze wie z.B. LAR, DIN EN 50174-2 (2015) sowie Blitz- und Überspannungsschutz einzuhalten.

Für ein voll funktionsfähiges Smart Home ist eine Gebäudeautomation mit einer Vernetzung der technischen Komponenten notwendig. Der logische Aufbau der Gebäudeautomation kann in die drei Bereiche Feldebene, Automationsebene und Managementebene unterteilt werden.

Die Feldebene bildet das Fundament der Gebäudeautomation. Hier werden alle Daten erfasst und Funktionen ausgeführt. Das Erfassen der Daten erfolgt durch Sensoren. Dies können z.B. Bewegungsmelder, Temperaturfühler oder Fensterkontakte sein. Ausgeführt werden die Funktionen von Aktoren. Es handelt sich dabei u.a. um Stellmotoren für Ventile und Klappen, Schalt- und Dimmeinrichtungen für die Beleuchtung oder Antriebe für den Sonnenschutz. Des Weiteren werden der Feldebene noch Bedieneinrichtungen wie z.B. Schalter, Raumbediengeräte oder Touchpanels zugeordnet.

Um die Informationen der Sensoren an die Aktoren weitergeben zu können, müssen alle Feldgeräte (Sensoren, Aktoren, Bedieneinrichtungen) in ein gemeinsames Netzwerk zusammengeführt werden. Die meist verwendete Netzwerktopologie ist hierbei der Bus, in der alle Geräte direkt mit demselben Übertragungsmedium, d.h. dem Bus verbunden sind. Die Sensoren wandeln dabei physikalische Größen in elektrische Signale um.

Die Aktoren werden über die intelligente Steuerung einbezogen und führen erhaltene Befehle aus, z.B. Temperaturänderung eines Heizkörpers durch Steuern des entsprechenden Stellantriebes (Schäfer 2012).

Die Automationsebene ist das intelligente Bindeglied zwischen der Feldebene und Managementebene. Sie verfügt über alle notwendigen Regelprogramme und bündelt die Informationen aller angeschlossenen und vernetzten gebäudetechnischen Anlagen. Hier werden von ein oder mehreren Recheneinheiten Daten der Sensoren und Aktoren gesammelt, aufbereitet und anschließend Regel- und Steuerungsmechanismen ausgelöst. Die Feldgeräte werden hierfür entweder über einen Feldbus zusammengefasst und über eine höherwertige Schnittstelle in die Recheneinheit eingelesen oder es werden physikalische Datenpunkte direkt über analoge und digitale Eingänge angeschlossen. Bestimmte Daten werden an den Leitrechner der Managementebene weitergeleitet. Die zentrale Recheneinheit wird dabei auch als Direct Digital Control (DDC) bezeichnet (Palmer 2016, Schäfer 2012).

Der Managementebene oder auch Leitebene sind alle übergeordneten Funktionen wie die Visualisierung, Überwachung, Bedienung und Ausgabe von Störmeldungen des Gebäudes usw. zuzuordnen. In der Regel stellt sie über einen Desktop mit der benötigten Anwendungssoftware das „Human Machine Interface“ (HMI), also die Schnittstelle zum Menschen, zur Verfügung (Aschendorf 2014).

Nachfolgend werden einige Beispiele zum Bereich „Smart Home – Sicherheit“ aufgeführt:



Abb. 2: Smart Home – Sicherheit: Anwendungsbeispiele



### Gefahrenvermeidung

Die Gefahrenvermeidung beschreibt z.B. Abschreckung durch Bewegungsmelder und Kameras oder Regelung von Leuchten, Musikanlagen und Jalousien zur Anwesenheitssimulation.



### Elektronische Schließtechniken

Elektronische Schließtechniken werden u.a. zur Gebäudesicherung genutzt. Sie können z.B. berührungslos oder kontaktbehaftet durch biometrische Systeme oder anhand von Smart Home-Bedienelementen gesteuert werden.



### Mechanische Sicherung

Hierunter sind Mechanische Sicherungen für Türen, Fenster und Rollläden zu verstehen, um ein Eindringen in das Haus zu verhindern/erschweren.



### Einbruchmeldeanlagen (EMA)

Einbruchmeldeanlagen sind Alarmsysteme, die z.B. durch Kontaktmelder an Türen und Fenstern, intelligente Sensoren oder Kameras etc. angesteuert werden und bei einem unbefugten Zutritt reagieren.



### Automatisierte Rufsysteme

Automatisierte Rufsysteme werden z.B. zur Meldung von möglichen Gefahren durch Feuer, Wasser, Gas oder unbefugten Zutritt eingesetzt.



### Smart Home-Plattformen

Mittlerweile existieren zahlreiche internetbasierte Plattformen zur Steuerung von Gebäudeautomationskomponenten, z.B. Qivicon, innogy Smart Home oder Conrad Connect, auf dem Markt. Sie ermöglichen es, Smart Home-Komponenten von verschiedenen Herstellern miteinander zu kombinieren, zu steuern, zu kontrollieren und zu automatisieren. Mit OpenHAB 2 wurde eine kostenfreie, quelloffene Software entwickelt, mit dem Ansatz, auf der Managementebene herstellerübergreifend die unterschiedlichsten Komponenten zu einem Smart Home zu vernetzen.



### IT-Sicherheit & Datenschutz

Vermeidung ungewollter Zugriffe externer Personen auf persönliche Daten und von Hacker-Zugriffen auf die Haussteuerung. Gefahrenpotenziale liegen u.a. bei der Übertragung von Daten an Dritte (z.B. Stromverbräuche), Steuerung des Systems über W-LAN oder der externen Speicherung der Daten (z.B. in Clouds). Hierbei sind rechtliche Vorschriften sowie bestehende Normen zu beachten/einzuhalten.



### Vernetzung

Hierunter ist die physikalische Vernetzung der Gebäudeautomatisierungskomponenten zu verstehen. Bestehende Systeme sind z.B. KNX, LON und LCN. Im KNX System kann die Übertragung der Daten über verschiedene Medien erfolgen. Dies wäre eine Zweidrahtleitung (KNX Twisted Pair), das vorhandene Stromnetz (KNX Power Line), eine Übertragung über Funk (KNX Radio Frequency) sowie über das Ethernet (KNX IP) (KNX 2013). LON steht für Local Operating Network. Die Datenübertragung kann über Zweidrahtleitung, Funk, Glasfaser oder Powerline erfolgen. LCN steht für Local Control Network. Für die Datenübertragung zwischen den Gebäudekomponenten wird eine freie Ader des vorhandenen Stromnetzes genutzt.



### Fernüberwachung

Fernüberwachung durch Dritte (Dienstleister) wie z.B. Sicherheitsdienst (Einbruch) oder Pflegekräfte (Sturzerkennung, Überprüfung von Vitalwerten).



### Multimedia/Kommunikationstechnologien

Anwendung und Integration von Multimedia wie z.B. mobile Endgeräte oder Heimgeräte in das Smart Home Netz bzw. in die Gebäudeautomation.

## Veranstaltungen an den Handwerkskammern

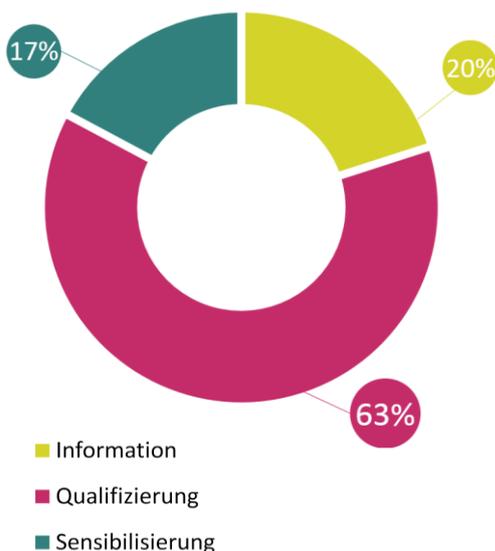


Abb. 3: Veranstaltungen an den Handwerkskammern

An den Handwerkskammern haben im Jahr 2017 zum Thema Smart Home zum größten Teil (63 %) Qualifizierungsveranstaltungen stattgefunden (Abbildung 3). Darüber hinaus bieten das Elektro- und Informationstechnische Kompetenznetzwerk ([www.elkonet.de](http://www.elkonet.de)), bestehend aus den Partnern BFE-Oldenburg, BZE Hamburg, BZL in Lauterbach, EBZ Dresden, etz Stuttgart und Z.E.I.T. Nürnberg/Fürth, sowie der Zentralverband Elektrohandwerk (ZVEH) über die E-Akademie ([www.zveh.de/e-akademie](http://www.zveh.de/e-akademie)) ein umfassendes Schulungsprogramm zum Thema Smart Home/ Gebäudeautomation an. Auch die Smart Home Initiative Deutschland e.V. ([www.smarthome-deutschland.de](http://www.smarthome-deutschland.de)) vermittelt Schulungen und Weiterbildungen für den Auf- und Ausbau von fundiertem Expertenwissen zu allen Themen rund um SmartHome, SmartBuilding, Smart Grid und AAL.

## Anwendungsgebiete und betroffene Berufe

Einige Berufe, für die das Thema „Smart Home – Sicherheit“ relevant ist, sind beispielhaft in Abbildung 4 dargestellt. Für weitere Berufe, speziell Berufe aus dem Ausbau, kann die Thematik ebenfalls interessant werden. Neue Einsatzgebiete bzw. Geschäftsfelder, z.B. der Aufbau einer gewerkeübergreifenden Beratungskompetenz oder der Sicherheitsberater, der den Kunden bzgl. Einbruchschutz sowie Sicherheit von Daten beim intelligenten Wohnen berät, können sich erschließen.

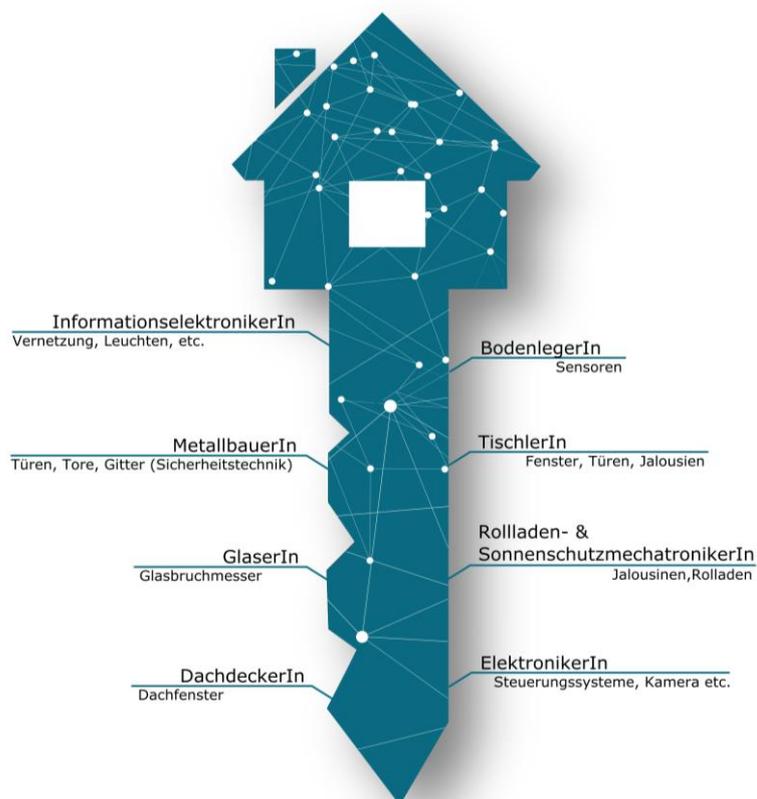


Abb. 4: Beispiele für betroffene Berufe und Anwendungsbeispiele

## Bestehende Hemmnisse für gewerblichen Einsatz

Für zahlreiche Betriebe ist die Unübersichtlichkeit des Marktes zum Thema Smart Home das größte Hemmnis, welches sie davon abhält Kunden proaktiv zu diesem Thema zu beraten. Es existiert eine große Anzahl von Systemen, die sich neben den zur Verfügung stehenden Komponenten und Funktionen vor allem hinsichtlich der verwendeten Übertragungsprotokolle und -medien unterscheiden und nur bedingt eine herstellerübergreifende Kompatibilität bieten. Viele Systeme bedienen dabei nur spezielle Märkte. Somit muss der Handwerker zwischen einer Vielzahl verschiedener Systeme differenzieren. Um hier zielgerichtet beraten zu können, sollten sich Multiplikatoren (u.a. Architekten, Elektroinstallateure, Energieberater) einen Wissensvorsprung aneignen.

Auf Kundenseite bestehen bzgl. einer Anschaffung von Smart Home-Systemen die größten Hemmnisse in den hohen Kosten der Anschaffung, des Einbaus und des Betriebs. Als weiteres Hemmnis aus Kundensicht wird häufig der Mangel an Informationen hinsichtlich der Datensicherheit angeführt. So können häufig Fragen wie etwa "Können persönliche Daten ausgelesen werden?", "Wie wird bei Anlagen mit Internetanbindung der Zugriff durch nicht autorisierte Personen verhindert?" oder "Könnte von außen die Anwesenheit festgestellt werden oder kann ein kontaktloses Türschloss durch Dritte von außen geöffnet werden?" nur unzureichend beantwortet werden (Bretschneider 2016, Splendid Research 2016).

## Durchdringungsgrad der Technologie

Laut der Studie "Smart Home Monitor 2016" des Marktforschungsunternehmens Dr. Grieger & Cie. (Splendid Research 2016) besitzen aktuell 29 % der Deutschen Smart Home-Produkte, 50 % interessieren sich dafür und lediglich 20 % lehnen diese ab. 53 % der Smart Home-Anwender nutzen Produkte für die Gebäude- und Wohnungssicherheit. In Deutschland ist demnach das Marktpotenzial an Smart Home Produkten in Höhe von 30 Milliarden Euro geschätzt.

Dem Statistik-Portal statista zufolge wird in 2017 ein Umsatz an Smart Home-Produkten in Höhe von 1.296 Millionen Euro generiert (Statista 2017). Davon entfallen 249,6 Mio. € auf den Bereich der Gebäudesicherheit. Da mit einem stetigen Wachstum zu rechnen ist, kann bis 2021 ein Umsatz von 4.146 Mio. € erwartet werden. Davon entfallen 872,9 Mio. € auf den Bereich der Gebäudesicherheit. Dies entspricht einem jährlichen Umsatzwachstum von 37 %.

Der Studie „Smarthome – Potenzial durch fehlende Unterstützung von Multiplikatoren gehemmt“ (Ludewig 2016) zufolge besitzen lediglich ca. 1/3 der Multiplikatoren „eher gute“ Kenntnisse im Bereich der Smart Home-Technologie, 1/3 der befragten Multiplikatoren gab an, schon mal mit Smart Home Produkten in Kontakt gekommen zu sein und ca. 1/3 der Befragten hatte noch keinen Kontakt zu Smart Home-Produkten.

Es besteht jedoch bei allen Befragten ein Interesse, zukünftig derartige Lösungen zu planen oder zu installieren. Die bisherigen Kenntnisse wurden zumeist durch eine eigene Internetrecherche sowie dem Austausch mit Kollegen erzielt.

## Wettbewerbsfähigkeit

Wie hoch die Bedeutung der Technologie Smart Home – Sicherheit für die künftige Wettbewerbsfähigkeit eines Unternehmens ist und in welchem Umfang bestimmte Gewerke betroffen sind, ist in Tabelle 1 für neun ausgewählte Berufe unter dem Punkt „Betroffenheit“ dargestellt. Hier zeigt sich, dass vor allem die Berufe ElektronikerIn und InformationselektronikerIn sehr stark von der betrachteten Technologie betroffen sind.

Tab. 1: Betroffenheit der einzelnen Gewerke sowie Qualifizierungsangebot in der Gesellinnen- und Gesellenausbildung (Grundlage: Ausbildungsordnung, Rahmenlehrplan, ÜLU)

|                      | ElektronikerIn | TischlerIn | InformationselektronikerIn | Rollladen- und SonnenschutzmechanikerIn | AnlagenmechanikerIn für SHK-Technik | MetallbauerIn | DachdeckerIn | GlaserIn | BodenlegerIn |
|----------------------|----------------|------------|----------------------------|---|-------------------------------------|---------------|--------------|----------|--------------|
| <b>Betroffenheit</b> | ++             | +          | ++                         | +                                       | +                                   | 0             | 0            | 0        | 0            |

Betroffenheit: ++ = hoch, + = durchschnittlich, 0 = gering

## Fazit

Durch intelligente Vernetzung verschiedener Komponenten können z.B. Komfort, Sicherheit und Energieeffizienz eines Gebäudes oder einer Wohnung gesteigert werden. Die Nachfrage nach smarten Lösungen wird in den nächsten Jahren im gewerblichen sowie im privaten Bereich stetig wachsen. Das Thema Sicherheit spielt dabei eine zentrale Rolle. Bedenken seitens der Endverbraucher bestehen im Zusammenhang mit Smart Home-Lösungen vor allem hinsichtlich des Datenschutzes und der IT-Sicherheit. Hemmnisse seitens der Handwerksbetriebe Smart Home-Systeme aktiv anzubieten liegen, aufgrund der zahlreichen verschiedenen Systeme und Anbieter in der Unübersichtlichkeit des Marktes. Von den Elektrohandwerken werden zunehmend Smart Home-Lösungen angeboten. Aus berufsqualifikatorischer Sicht sind diese Gewerke auch grundlegend für die Beratung, Installation und Wartung entsprechender Systeme vorbereitet. Dennoch besteht insbesondere hinsichtlich der Markttransparenz sowie der Daten- und IT-Sicherheit ein Bedarf an über die Erstausbildung hinausgehender Anpassungsqualifizierung. Ein Teil des Bedarfes wird bereits von einigen Bildungszentren des Handwerks, insbesondere von den im ELKONet zusammengeschlossenen, abgedeckt. Hier gilt es, Bedarf und Angebot abzugleichen.

## Literatur

**Aschendorf B (2014)** Energiemanagement durch Gebäudeautomation. Springer, Berlin

**DIN EN 50131-1 (2017)** Alarmanlagen - Einbruch- und Überfallmeldeanlagen - Teil 1: Systemanforderungen. Beuth, Berlin

**DIN EN 50174-2 (2011)** Informationstechnik - Installation von Kommunikationsverkabelung - Teil 2: Installationsplanung und Installationspraktiken in Gebäuden. Beuth, Berlin

**KNX (2013)** Grundlagenwissen zum KNX Standard. KNX, Frankfurt

**Palmer (2016)** Grundlagen der Gebäudeautomation für die Klima- und Lüftungstechnik. VDE, Berlin

**Schäfer (2012)** Grundlagen, Technologien und Normenüberblick für die Gebäudeautomation. Ergänzung zum Vorlesungsskript „Gebäudeautomation“. Hochschule Rosenheim

**Statista (2017)** Outlook Report. Smart Home  
<https://de.statista.com/outlook/279/137/smart-home/deutschland#marketStudy> (Abgerufen am: 12.12.18)

**Bretschneider R (2016)** Chancen und Hindernisse für Smart Home-Anwendungen aus verschiedenen Blickwinkeln. In: Forschungsbeiträge der eresult GmbH, Göttingen

**DIN EN 50136-1 (2012)** Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen - Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen. Beuth, Berlin.

**DIN VDE 0833-1 (2014)** Gefahrenmeldeanlagen für Brand, Einbruch und Überfall. VDE Verlag GMBH, Berlin

**Ludwig, E (2016)** Smarthome-Potenzial durch fehlende Unterstützung von Multiplikatoren gehemmt. In: Forschungsbeiträge der eresult GmbH, Göttingen

**Saena (2016)** Smart Home – Wohngebäude intelligent vernetzt. Sächsische Energieagentur GmbH, Dresden

**Splendid Research (2016)** Smart Home Monitor 2016.  
<https://www.splendid-research.com/statistiken/item/studie-smart-home.html> (Abgerufen am: 12.12.18)

**VdS 2311 (2017)** „Planung und Einbau von Einbruchmeldeanlagen“. VdS Schadenverhütung GmbH, Köln