Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 01.10.2022

DIGITALISIERUNG IM GEBÄUDE

Grundlagen zu Interoperabilität und Informationssicherheit im Gebäude

Auftraggeber:

Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

Auftragnehmer:

Verein energie-cluster.ch
Gutenbergstrasse 21
3011 Bern
+41 31 381 24 80
sekreteriat@energie-cluster.ch

Autoren / Projektteam

Daniel Stauffer, Technologievermittler energie-cluster.ch, INEXTR GmbH, Bahnhofstrasse 36, 6210 Sursee

Peter Scherer, Leiter MAS Digitales Bauen an der FHNW, Hofackerstrasse 30, 4132 Muttenz

Philipp Heer, StV. Leiter Urban Energy Systems Lab bei Empa, Überlandstrasse 129, 8600 Dübendorf

Beat Steiner, Inhaber bestec AG, Breiten 16, 3232 Ins

Andreas Rumsch, Leiter Forschungsgruppe, iHomeLab, HSLU, Technikumstrasse 21, 6048 Horw

BFE-Bereichsleitung: Lucas Tochtermann, lucas.tochtermann@bfe.admin.ch

BFE-Programmleitung: Dr. Matthias Galus, matthias.galus@bfe.admin.ch

BFE-Vertragsnummer: SH/8100360-02-01-03

Inhaltsverzeichnis

1 Management Summary (D)

Die Schweiz soll ab 2050 nicht mehr Treibhausgase in die Atmosphäre ausstossen, als durch natürliche und technische Speicher aufgenommen werden (Netto-Null-Ziel). Um das Netto-Null-Ziel bis 2050 zu erreichen, müssen hauptsächlich die Emissionen im Gebäudebereich, im Verkehr und in der Industrie umfassend vermindert werden.

Die Digitalisierung kann als Instrument einen wichtigen Beitrag im Gebäudebereich leisten. Um die Digitalisierung im Gebäude und die damit verbundenen Potenziale bezüglich Energieeffizienz und Emissionsreduktion auszuschöpfen, müssen zunehmend grundsätzliche Fragen zu Interoperabilität, Datenschutz und Cybersicherheit gestellt und beantwortet werden. Diese Themen sind Grundvoraussetzung für eine erfolgreiche Digitalisierung im Gebäude, wirken aber unter anderem wegen der damit verbundenen Komplexität und weiteren Herausforderungen derzeit als Hemmnisse.

Um Hemmnisse zu identifizieren und Grundlagen zu den Themen Digitalisierung, Interoperabilität, Datenschutz und Cybersicherheit im Gebäude zu schaffen, sollten Grundlagen zum Thema Konnektivität im Gebäude (KiG) erstellt und die Themen analysiert werden.

In einer ersten Arbeitsphase wurden eine Markt- und Bedarfsanalyse zu den Themen Interoperabilität, Cybersicherheit und Datenschutz im Gebäude durchgeführt. Die Ergebnisse der Analyse zeigen, dass die Wichtigkeit der Konnektivität im Gebäude durchaus erkannt wird, um mit integrierten Systemen die Effizienz zu steigern. Auch die damit verbundenen Risiken in den Bereichen Cybersicherheit und Datenschutz werden erkannt. Teilweise nutzen die in der Analyse Befragten bereits die in Gebäuden anfallenden Daten, um den Betrieb effizienter zu gestalten, sehen aber noch Verbesserungspotential. Als wesentliche Hemmnisse erkennen die Befragten die hohe Komplexität der Systeme, das oft fehlende Know-how der Fachleute in Bezug auf Themen der Konnektivität und die hohe Anzahl an Standards, Normen, Richtlinien und Protokollen.

Die Analyse zeigt, dass interdisziplinäre Zusammenarbeit vielfach nicht stattfindet und ein starkes Silodenken der Beteiligten vorherrscht. Dies führt dazu, dass die einzelnen Gewerke nicht gut aufeinander abgestimmt oder gar nicht miteinander vernetzt sind. Gründe für die fehlende Zusammenarbeit sind fehlende oder zu geringe Anreize, die Gewerke im Gebäude als Gesamtsystem zu betrachten. Oft ist der Nutzen der Zusammenarbeit nicht oder zu wenig bekannt. Die Wahrnehmung ist zudem, dass die interdisziplinäre Zusammenarbeit die Komplexität erhöht.

Die Wichtigkeit der Themen Cybersicherheit und Datenschutz ist bei den in der Analyse Befragten erkannt. Das Verhalten im Umgang mit vernetzten Geräten und Daten ist allerdings oft nicht angemessen, um den Risiken durch Cyberangriffe und Datenmissbrauch zu begegnen. Standards, Normen oder Richtlinien enthalten Lösungsansätze oder Verhaltensregeln, um den Risiken zu begegnen, sind aber zu wenig bekannt oder werden als zu komplex angesehen. Der Aufwand von Massnahmen für die Erhöhung der Maturität in den Bereichen Datenschutz und Cybersicherheit wird als hoch eingestuft.

In der zweiten Phase der Arbeiten wurde mit den teilnehmenden Firmen, Hochschulen und Verbänden ein Soll-Zustand erarbeitet. Eine wesentliche Komponente des Soll-Zustandes ist die Befähigung aller an Planung, Bau und Betrieb beteiligten Fachleute hinsichtlich eines digitalisierten Betriebes der Gebäude. Für Nutzende in der Betriebsphase des Gebäudes ist die Unterstützung durch Digitalisierung wichtig. So sollen die Themen der Konnektivität, der Cybersicherheit und des Datenschutzes in die Aus- und Weiterbildung einfliessen und so sicherstellen, dass die Absolvierenden die erforderlichen Kompetenzen mitbringen, um diese in Planung, Bau und im Betrieb einzubringen. Zudem soll ein integraler Planungsansatz vermittelt werden, welcher aufzeigt, dass die interdisziplinäre Zusammenarbeit über alle Phasen (Planung, Bau und Betrieb) die Effizienz im Gebäudebereich steigern kann und wie diese Steigerung aussieht. Dabei spielen noch zu erstellende Leitfäden für spezifische Anwendungsfälle in Planung, Bau, Betrieb und Nutzung eine wichtige Rolle. Dadurch, dass die Leitfäden für die wichtigsten Anwendungsfälle von digitalen Lösungen im Gebäude das Vorgehen, die involvierten Stakeholder und Vorgehensweisen skizzieren, kann das Potential der Digitalisierung von Anfang an berücksichtigt werden. Die Leitfäden unterstützen die Beteiligten bei der Integration der Systeme im Gebäude und bei der Einhaltung des Datenschutzes oder der Sicherstellung der Cybersicherheit.

Um den Soll-Zustand zu erreichen, sind verschiedene Massnahmen nötig. Diese zielen insbesondere auf die Unterstützung der in Planung, Bau und Nutzung beteiligten Personen ab. Dazu ist zunächst eine Aus- und Weiterbildung wichtig, die insbesondere auf die Potentiale der Digitalisierung im Gebäudebereich und in deren Betrieb ausgerichtet ist. Weiter ist die Unterstützung der interdisziplinären

Zusammenarbeit zwischen den verschiedenen Beteiligten wichtig, welche durch Leitfäden katalysiert werden kann. Auch gilt es einen vereinfachten Zugang zu Standards zu ermöglichen.

Die gewerkeübergreifende Vernetzung soll schon in der Planungsphase durch eine integrale Planung berücksichtigt werden. Um dies zu fördern, muss auch in der Aus- und Weiterbildung angesetzt werden. Die Bildungsangebote in den klassischen Branchen rund um Gebäude müssen erweitert werden. Dazu müssen die für die Gestaltung der Bildungsangebote Verantwortlichen auf die Thematik aufmerksam gemacht werden. Diese benötigen Unterstützung z.B. in Form von Vorgaben, welche Kompetenzen die Absolvierenden zu erlangen haben.

Um die Digitalisierung im Gebäude und dadurch die Energieeffizienz und den Komfort der Gebäude zu verbessern, kann die Verwendung von standardisierten Instrumenten Hilfe bieten. Mit dem von der europäischen Kommission definierten *Smart Readiness Indicator (SRI)* steht ein Werkzeug bereit, welches Gebäude hinsichtlich ihrer Intelligenz messen und bewerten kann. Der SRI erhöht die Bestellerkompetenz. Mit ihm weiss der Auftraggeber auf transparenter und intuitiver Art und Weise welches Mass an Intelligenz sein Gebäude erhalten wird und welchen Mehrwert dies bringt. Das Werkzeug ist so gestaltet, dass es von allen an Planung, Bau und Betrieb Beteiligten genutzt werden kann. Mit dem SRI können die Beteiligten Massnahmen der Digitalisierung an Gebäude, wie z.B. auch die Nutzung von Energiemanagementsystemen, bewerten und vergleichen. Das kann langfristig einen Mehrwert am Immobilienmarkt generieren. Es gilt den SRI in einem nächsten Schritt für die Schweiz anzuwenden. Hierzu soll zunächst im Rahmen einer Vorstudie unter Einbezug der Branche, sowohl die Anwendbarkeit in der Schweiz gezeigt bzw. geprüft werden als auch inwiefern der SRI in bestehende Labels (Minergie, SNBS) integriert werden kann.

Der SRI alleine reicht jedoch nicht aus. Die Komplexität des Themas Gebäudeautomation und Energiemanagementsysteme an sich sowie ein schwer zu überblickendes und einzuschätzendes Angebot an technischen Lösungen stellen Nachfrager und Benutzer vor grosse Herausforderungen. Zum einen schreckt die technische Komplexität und der Integrationsaufwand ab, zum anderen ist das Nutzenversprechen nicht immer klar. Während der SRI letzteres klarer machen wird, kann die Bestellerkompetenz durch eine verbesserte Markttransparenz im Bereich Gebäudeautomation und insbesondere im Bereich von Energiemanagementsystemen erhöht werden. Oftmals wissen Bestellende nicht, welche Lösungen auf dem Markt verfügbar sind, was diese leisten und wie interoperabel sie sind bzw. auf welchen Standards sie beruhen. Eine regelmässige Marktübersicht und für jedermann einfach zugängliche Analysen, z.B. in Form einer einfach verständlichen Webapplikation, können dieses deutlich Hemmnis reduzieren und Orientierung bieten. Die durch Energie Schweiz unterstützte erste Marktübersicht aus dem Jahre 2020 bietet eine hervorragende Grundlage und sollte ausgebaut und mit nachvollziehbaren und auf Bedürfnisse der Besteller basierenden Key-Performance-Indikatoren angereichert werden. Schliesslich sollen Leitfäden erarbeitet werden, welche die Interoperabilität der digitalen Lösungen unterstützen, den Integrationsaufwand reduzieren und die interdisziplinäre Zusammenarbeit forcieren.

Um den Anspruchsgruppen rund um die Entwicklung, den Betrieb und die Nutzung von Gebäuden eine wirksame Hilfestellung zu bieten, sollen kontextbezogene Informationen zu Datenschutz und Cybersicherheit zur Verfügung gestellt werden. Je nach Problemstellung und je nach Anspruchsgruppe ausgerichtete Leitfäden würden Unsicherheiten reduzieren. Mit dem NIST Cybersecurity Framework steht eine Basis zur Verfügung, die hilft das Cybersecurity-Risiko besser zu verstehen, zu verwalten, zu reduzieren und Netzwerke und Daten zu schützen. Basierend auf dem NIST Cybersecurity Framework und durch Erweiterungen mit verschiedenen Standards und Normen könnte eine digitale (Web-)Lösung anwenderspezifische Leitfäden nach der Eingabe von einigen Parametern erstellen. Durch eine einfache und intuitive Möglichkeit anwenderspezifische Leitfäden zu erstellen, können Hemmnisse zur Digitalisierung im Gebäude abgebaut werden, die aus der Komplexität und Unüberschaubarkeit aus den Bereichen der Informationssicherheit entstehen.

Weitere vorgeschlagenen Massnahmen betreffen die Sensibilisierung zum Erhalt von Cybersicherheit und Datenschutz. Bestellende, Planende und Personen zuständig für den die Betriebsphase sollen durch Informationskampagnen, durch Aus- und Weiterbildung und Roadshows auf das Thema Informationssicherheit rund ums Gebäude sensibilisiert werden. Für Aus- und Weiterbildung sind noch Konzepte über Inhalt und Zielgruppen zu definieren, um die Kompetenzen im Bereich Informationssicherheit in der Branche zu stärken. Für die Stärkung der Aus- und Weiterbildung müssen sowohl bestehende Angebote ergänzt werden, sowie neue Lehr- und Studienangebote erschaffen werden. Durch Zertifizierung und Labeling von vertrauenswürdiger Digitalisierung im Gebäude kann die Bestellerkompetenz zusätzlich im Bereich Informationssicherheit erhöht werden. Durch die Definition eines Zertifizierungsverfahren, soll klar werden welche Richtlinien befolgt werden müssen, um

vertrauenswürdige Digitalisierung im Gebäude zu erreichen. Auch hier müssten bei einer Realisierung bestehende Gebäudelabels berücksichtigt werden.

Management Summary (F)

D'ici 2050, la Suisse ne devra plus rejeter dans l'atmosphère davantage de gaz à effet de serre que ce que les réservoirs naturels et artificiels sont capables d'absorber (zéro émission nette). Pour atteindre l'objectif de zéro émission nette d'ici 2050, les émissions des domaines du bâtiment, des transports et de l'industrie en particulier doivent être drastiquement réduites.
La numérisation peut apporter une contribution importante dans le domaine du bâtiment en servant d'instrument. Afin de tirer parti de la numérisation dans le bâtiment et d'exploiter le potentiel qui en découle en matière d'efficacité énergétique et de réduction des émissions, il faudra répondre à un nombre croissant de questions fondamentales en lien avec l'interopérabilité, la protection des données et la cybersécurité. Ces thèmes sont indispensables à une numérisation réussie dans le bâtiment, bien qu'ils constituent aujourd'hui des obstacles du fait notamment de leur complexité et d'autres défis.
Pour identifier ces obstacles et créer une base pour les thèmes de la numérisation, l'interopérabilité, la protection des données et la cybersécurité dans le bâtiment, des principes doivent être établis sur le thème de la connectivité des bâtiments (Konnektivität im Gebäude [KiG]) et les thèmes analysés.
Une analyse de marché et des besoins sur les thèmes de l'interopérabilité, de la cybersécurité et de la protection des données dans le bâtiment a été menée lors d'une première phase de projet. Les résultats de cette analyse montrent que les acteurs ont conscience de l'importance de la connectivité dans le bâtiment pour augmenter l'efficacité au moyen de systèmes intégrés. Les risques associés dans les domaines de la cybersécurité et de la protection des données sont eux aussi identifiés. Il arrive que les personnes interrogées dans le cadre de l'analyse utilisent déjà les données recueillies dans les bâtiments pour favoriser une exploitation plus efficace, bien qu'elles y voient encore un potentiel d'amélioration. Elles considèrent que les principaux obstacles sont la grande complexité des systèmes, le manque de connaissances des spécialistes en matière de connectivité et le grand nombre de standards, normes, directives et protocoles.

Il ressort également que trop souvent, la collaboration interdisciplinaire est inexistante et qu'une mentalité fortement cloisonnée des participants prédomine. Cela entraîne une mauvaise coordination des différents métiers du bâtiment, voire une absence totale de coordination. Cette situation s'explique par le manque d'incitations à considérer les services du bâtiment comme un système global. Bien souvent, le potentiel de la collaboration n'est pas ou peu connu. La collaboration interdisciplinaire donne en outre l'impression d'augmenter la complexité.

Les personnes interrogées reconnaissent l'importance de la cybersécurité et de la protection des données. Les comportements vis-à-vis des appareils connectés et des données ne sont toutefois souvent pas appropriés pour faire face aux risques de cyberattaques et d'utilisation frauduleuse des données. Les standards, normes et directives existantes comprennent des solutions ou des règles de bonne conduite visant à faire face aux risques, mais ils sont trop peu connus ou considérés comme trop complexes. Les coûts des mesures visant à améliorer le degré d'aboutissement dans les domaines de la protection des données et de la cybersécurité sont considérés comme élevés.

Les entreprises, hautes écoles et associations participantes ont défini un état idéal lors de la deuxième étape des travaux. Une composante importante de cet état idéal est l'acquisition de compétences par les spécialistes impliqués dans la planification, la construction et l'exploitation en vue d'une exploitation numérique des bâtiments. Le soutien aux personnes recourant à la numérisation dans l'entreprise joue un rôle important. C'est pourquoi les thèmes de la connectivité, de la cybersécurité et de la protection des données doivent être intégrés aux formations et perfectionnements, de façon à permettre aux diplômés de détenir les compétences de planification, de construction et d'exploitation nécessaires. Une approche de planification complète doit en outre être transmise et montrer la façon dont la collaboration interdisciplinaire peut améliorer l'efficacité dans le domaine du bâtiment pendant toutes les phases (planification, construction et exploitation) et à quoi ressemble cette augmentation concrètement. Des guides qui doivent encore être établis pour certains cas d'application spécifiques relevant de la planification, de la construction, de l'exploitation et de l'utilisation ont un rôle déterminant. Dans la mesure où les guides esquissent les procédures et les parties prenantes pour les cas les plus importants de solutions numériques, le potentiel de numérisation peut être pris en compte dès le départ. Ils aident les participants dans l'intégration des systèmes au sein du bâtiment, le respect de la protection des données et la garantie de la cybersécurité.

Pour atteindre l'état idéal, diverses mesures sont nécessaires. Elles visent notamment à soutenir les personnes impliquées dans la planification, la construction et l'utilisation. Il est important de proposer une formation et un perfectionnement axés sur le potentiel de la numérisation dans le domaine du bâtiment et sur son exploitation. Il convient également de soutenir la collaboration interdisciplinaire entre

les différentes parties impliquées, qui peut être catalysée par le biais de guides. L'accès aux standards doit aussi être simplifié.

La mise en réseau de divers secteurs du bâtiment doit être prise en compte dès la phase de planification grâce à une planification intégrale. Pour encourager cette démarche, celle-ci doit être intégrée à la formation et au perfectionnement. L'offre de formation dans les branches classiques du bâtiment doit être élargie. Les responsables de l'offre de formation doivent pour ce faire être sensibilisés à ce sujet. Ils ont besoin de soutien, notamment sous forme de prescriptions quant aux compétences que les diplômés doivent acquérir.

Pour améliorer la numérisation dans le bâtiment et de ce fait l'efficacité énergétique et le confort du bâtiment, le recours à des instruments standardisés peut s'avérer utile. Le *Smart Readiness Indicator (SRI)* défini par la Commission européenne est un outil permettant de mesurer et d'évaluer l'intelligence d'un bâtiment. Le SRI augmente la compétence du mandant. Il permet au client de connaître l'intelligence de son bâtiment et la valeur ajoutée qu'il peut apporter de manière transparente et intuitive. L'outil est conçu de sorte que toutes les personnes impliquées dans la planification, la construction et l'exploitation puissent l'utiliser. Le SRI permet aux participants d'évaluer et de comparer les mesures de numérisation dans les bâtiments, comme par exemple l'utilisation de systèmes de gestion de l'énergie. Cette démarche peut générer une valeur ajoutée sur le marché de l'immobilier à long terme. Il faut utiliser le SRI dans une prochaine étape en Suisse. Pour cela, il convient tout d'abord de montrer et de vérifier l'applicabilité du SRI en Suisse dans le cadre d'une étude préliminaire avec la participation, mais aussi de déterminer comment le SRI peut être intégré dans les labels déjà existants (Minergie, SNBS).

Cependant, le SRI seul ne suffit pas. La complexité du sujet de l'automatisation des bâtiments et des systèmes de gestion de l'énergie en soi, ainsi qu'une offre de solutions techniques difficile à appréhender et à évaluer, posent de grands défis aux demandeurs et aux utilisateurs. D'une part, la complexité technique et l'effort d'intégration sont dissuasifs et, d'autre part, la promesse d'avantages n'est pas toujours claire. Alors que le SRI rendra ce dernier point plus clair, les compétences des acheteurs peuvent être améliorées par une meilleure transparence du marché dans le domaine de l'automatisation des bâtiments et en particulier dans le domaine des systèmes de gestion de l'énergie. Souvent, les acheteurs ne savent pas quelles solutions sont disponibles sur le marché, quelles sont leurs performances et quel est leur degré d'interopérabilité ou sur quelles normes elles reposent. Une vue d'ensemble régulière du marché et des analyses facilement accessibles à tous, par exemple sous la forme d'une application web simple à comprendre, peuvent réduire cet obstacle et fournir des informations. La première vue d'ensemble du marché de 2020, soutenue par SuisseÉnergie, offre une excellente base et devrait être développée et enrichie d'indicateurs de performance clés compréhensibles et basés sur les besoins des acheteurs. Pour finir, des guides soutenant l'interopérabilité des solutions numériques, réduisant les coûts d'intégration et favorisant la collaboration interdisciplinaire doivent voir le jour.

Pour offrir aux groupes d'intérêts une aide efficace en matière de développement, d'exploitation et d'utilisation des bâtiments, il convient de mettre à disposition des informations sur la protection des données et la cybersécurité en lien avec le contexte. Des guides spécifiques en fonction du problème rencontré et des parties prenantes réduiraient les incertitudes. Le NIST Cybersecurity Framework offre un cadre qui aide à mieux comprendre, gérer et réduire les risques de cybersécurité et à protéger les réseaux et les données. En se basant sur le cadre de cybersécurité du NIST et en l'enrichissant de différents standards et normes, une solution numérique (web) peut créer des guides spécifiques à l'utilisateur après avoir saisi certains paramètres. En offrant une possibilité simple et intuitive de créer des guides spécifiques aux utilisateurs, il est possible de réduire les obstacles à la numérisation des bâtiments qui résultent de la complexité et de l'opacité des domaines de la sécurité de l'information.

D'autres mesures proposées concernent la sensibilisation au maintien de la cybersécurité et de la protection des données. Les commanditaires, les planificateurs et les personnes responsables de la phase d'exploitation doivent être sensibilisés au thème de la sécurité de l'information autour du bâtiment par des campagnes d'information, des formations et des roadshows. En ce qui concerne la formation et le perfectionnement, des concepts relatifs au contenu et aux groupes cibles doivent encore être définis afin de renforcer les compétences dans le domaine de la sécurité de l'information au sein du secteur. Pour renforcer la formation initiale et continue, il faut compléter les offres existantes et créer de nouvelles offres d'enseignement et d'études. La certification et la labellisation de la numérisation de confiance dans le bâtiment permettent d'augmenter les compétences des acheteurs dans le domaine de la sécurité de l'information. En définissant une procédure de certification, les directives à suivre pour obtenir une numérisation de confiance dans le bâtiment doivent être claires. Ici aussi, il faudrait tenir compte des labels existants pour les bâtiments en cas de réalisation.

Management Summary (I)

A partire dal 2050, la Svizzera non dovrà emettere una quantità di gas serra maggiore di quella che possa essere assorbita da sistemi di stoccaggio naturali e tecnici (obiettivo del saldo netto di emissioni pari a zero). Per raggiungere l'obiettivo delle emissioni nette pari a zero entro il 2050, è necessario ridurre in modo significativo le emissioni nel settore degli edifici, nei trasporti e nell'industria.

Nel settore degli edifici, la digitalizzazione può essere uno strumento in grado di fornire un contributo importante. Per sfruttare la digitalizzazione negli edifici e il relativo potenziale di incremento dell'efficienza energetica e di riduzione delle emissioni, è necessario rispondere a una serie di questioni di fondo concernenti l'interoperabilità, la protezione dei dati e la cibersicurezza. Affrontare questi temi è una condizione fondamentale per il successo della digitalizzazione negli edifici; tuttavia attualmente essi rappresentano un ostacolo, tra l'altro a causa della loro complessità e delle ulteriori sfide che pongono.

Per identificare gli ostacoli e porre le basi sui temi della digitalizzazione, dell'interoperabilità, della protezione dei dati e della cibersicurezza negli edifici, è necessario creare basi sulla questione della connettività negli edifici e analizzare i diversi temi.

In una prima fase del progetto, è stata condotta un'analisi del mercato e delle esigenze sui temi dell'interoperabilità, della cibersicurezza e della protezione dei dati negli edifici. I risultati dell'analisi mostrano che è chiaramente riconosciuta l'importanza della connettività negli edifici quale fattore determinante per aumentare l'efficienza attraverso l'integrazione dei sistemi. Vengono riconosciuti anche i rischi che ne derivano nei settori della cibersicurezza e della protezione dei dati. Alcuni dei partecipanti all'analisi utilizzano già i dati generati negli edifici per rendere l'esercizio più efficiente, ma ritengono che vi sia ancora un potenziale di miglioramento. Fra gli ostacoli principali vengono indicati l'elevata complessità dei sistemi, le competenze in materia di connettività spesso carenti degli esperti e l'elevato numero di standard, norme, direttive e protocolli.

Dall'analisi emerge che spesso la collaborazione interdisciplinare non ha luogo e che prevale una forte tendenza dei soggetti coinvolti a pensare per comparti separati. Di conseguenza, i singoli impianti non sono ben coordinati o addirittura non sono collegati in rete tra loro. Le ragioni della mancanza di cooperazione sono l'assenza o la scarsità di incentivi a considerare gli impianti dell'edificio come un sistema complessivo. Spesso i benefici della collaborazione non sono noti o non sono sufficientemente conosciuti. La percezione è anche che la collaborazione interdisciplinare aumenti la complessità.

L'importanza dei temi della sicurezza informatica e della protezione dei dati è riconosciuta dalle persone intervistate nell'ambito dell'analisi. Tuttavia, il comportamento nella gestione dei dispositivi e dei dati in rete spesso non è idoneo a contrastare i rischi posti dagli attacchi informatici e dall'uso improprio dei dati. Gli standard, le norme o le direttive contengono approcci o regole di condotta per contrastare i rischi, ma sono troppo poco conosciuti o considerati troppo complessi. L'onere delle misure per aumentare la maturità nei settori della protezione dei dati e della cibersicurezza è considerato elevato.

Nella seconda fase del lavoro, con le aziende, le università e le associazioni partecipanti è stato elaborato uno «stato auspicato». Una componente essenziale dello «stato auspicato» è l'acquisizione, da parte di tutti i professionisti coinvolti nella progettazione, nella costruzione e nella gestione, della capacità di garantire un esercizio digitalizzato degli edifici. In questo contesto, è importante il supporto di coloro che utilizzano la digitalizzazione nell'esercizio. I temi della connettività, della cibersicurezza e della protezione dei dati devono confluire nella formazione di base e nella formazione continua, in modo da assicurare che chi porta a termine un iter formativo abbia le competenze necessarie per integrarli nella progettazione, nella costruzione ma anche nell'esercizio. Inoltre, deve essere perseguito un approccio progettuale integrale che evidenzi come la collaborazione interdisciplinare in tutte le fasi (progettazione, costruzione ed esercizio) possa aumentare l'efficienza nel settore degli edifici e come questo aumento si manifesti in termini concreti. A questo riguardo un ruolo importante sarà svolto dall'elaborazione di linee guida per applicazioni specifiche in materia di pianificazione, costruzione, esercizio e utilizzo. Delineando l'approccio, gli stakeholder interessati e le procedure per i principali casi di applicazione delle soluzioni digitali nell'edificio, le linee guida consentiranno di tenere fin dall'inizio conto del potenziale della digitalizzazione. Le linee guida dovranno supportare le parti interessate nell'integrazione dei sistemi nell'edificio, nel rispetto della protezione dei dati o nel garantire la cibersicurezza.

Per raggiungere lo stato auspicato sono necessarie diverse misure finalizzate in particolare a supportare le persone coinvolte nella pianificazione, nella costruzione e nell'utilizzo. A tal fine, sono innanzitutto importanti una formazione di base e una formazione continua particolarmente orientate alle potenzialità

della digitalizzazione nel settore degli edifici e al suo esercizio. Inoltre, è importante sostenere la collaborazione interdisciplinare tra le diverse parti interessate, che può essere catalizzata attraverso linee guida. È inoltre necessario consentire un accesso semplificato agli standard.

La collaborazione interdisciplinare deve essere presa in considerazione già nella fase di pianificazione attraverso una progettazione integrale. Per promuoverla, è necessario affrontare questo aspetto anche in sede di formazione di base e di formazione continua. L'offerta formativa nei settori tradizionali che ruotano intorno all'edilizia deve essere ampliata. A tal fine, occorre sensibilizzare al riguardo coloro che progettano le offerte formative e offrire loro supporto, ad esempio sotto forma di prescrizioni sulle competenze che i soggetti in formazione devono acquisire.

Per migliorare la digitalizzazione negli edifici e quindi l'efficienza energetica e il comfort degli edifici stessi, può essere d'aiuto l'uso di strumenti standardizzati. Con lo *Smart Readiness Indicator (SRI)* definito dalla Commissione Europea, è disponibile uno strumento in grado di misurare e valutare gli edifici in termini di intelligenza. L'SRI aumenta la competenza di ordinazione, in quanto consente al committente di sapere di quale livello di intelligenza disporrà il suo edificio e quale valore aggiunto ciò comporterà in modo trasparente e intuitivo. Lo strumento è stato progettato in modo da poter essere utilizzato da tutti coloro che sono coinvolti nella pianificazione, nella costruzione e nell'esercizio. L'SRI consente alle parti interessate di valutare e confrontare le misure di digitalizzazione degli edifici, come l'uso di sistemi di gestione dell'energia. Questo può generare a lungo termine un valore aggiunto sul mercato immobiliare. Il prossimo passo sarà quello di applicare l'SRI in Svizzera. A tal fine, l'applicabilità dell'ISR in Svizzera deve essere dimostrata e testata nell'ambito di uno studio preliminare che coinvolga il settore, e si deve indagare in che modo l'SRI possa essere integrato nei marchi esistenti (Minergie, SNBS).

Tuttavia, l'ISR da solo non è sufficiente. La complessità del tema dell'automazione degli edifici e dei sistemi di gestione dell'energia in quanto tali, così come la gamma di soluzioni tecniche difficili da censire e valutare, pongono sfide importanti per i richiedenti e gli utenti. Da un lato, la complessità tecnica e lo sforzo di integrazione sono un deterrente, dall'altro la proposta di valore non è sempre chiara. Mentre l'ISR renderà quest'ultimo aspetto più chiaro, la competenza di ordinazione può essere aumentata attraverso una migliore trasparenza del mercato nell'area dell'automazione degli edifici e soprattutto nell'area dei sistemi di gestione dell'energia. Spesso i committenti non sanno quali soluzioni sono disponibili sul mercato, cosa fanno e quanto sono interoperabili o su quali standard si basano. Una panoramica regolare del mercato e analisi facilmente accessibili a tutti, ad esempio sotto forma di un'applicazione web di facile comprensione, possono ridurre questo ostacolo significativo e fornire un orientamento. La prima panoramica del mercato dal 2020, sostenuta da Energia Svizzera, fornisce una base eccellente e dovrebbe essere ampliata e arricchita con indicatori di performance chiave comprensibili, basati sulle esigenze degli acquirenti. Infine, dovranno essere elaborate linee guida per supportare l'interoperabilità delle soluzioni digitali, ridurre lo sforzo di integrazione e promuovere la cooperazione interdisciplinare.

Per fornire un'assistenza efficace alle parti interessate in merito allo sviluppo, all'esercizio e all'utilizzo degli edifici, si dovranno rendere disponibili informazioni contestuali sulla protezione dei dati e sulla cibersicurezza. Le guide orientate a specifici problemi e gruppi di stakeholder ridurrebbero le incertezze. Il NIST Cybersecurity Framework fornisce un quadro di riferimento che aiuta a comprendere, gestire e ridurre meglio il rischio di cibersicurezza e a proteggere reti e dati. Basata sul NIST Cybersecurity Framework ed estesa con diversi standard e norme, una soluzione digitale (web) può creare guide specifiche per l'utente dopo aver inserito alcuni parametri. Grazie alla possibilità semplice e intuitiva di creare linee guida specifiche per l'utente, è possibile ridurre le barriere alla digitalizzazione nell'edificio, che derivano dalla complessità e dall'ingestibilità delle aree di sicurezza delle informazioni.

Altre misure proposte riguardano la sensibilizzazione alla cibersicurezza e alla protezione dei dati. I committenti, i progettisti e i responsabili della fase operativa devono essere sensibilizzati sul tema della sicurezza delle informazioni intorno all'edificio attraverso campagne informative, istruzione e formazione e roadshows. Per quanto riguarda l'istruzione e la formazione, devono ancora essere definiti i concetti di contenuto e i gruppi target, al fine di rafforzare le competenze nel campo della sicurezza informatica nel settore. Per rafforzare l'istruzione e la formazione, è necessario integrare le offerte esistenti e creare nuove offerte di insegnamento e di studio. La certificazione e l'etichettatura della digitalizzazione affidabile nell'edificio possono inoltre aumentare la competenza dell'ordine nell'area della sicurezza delle informazioni. Definendo una procedura di certificazione, dovrebbe essere chiaro quali linee guida devono essere seguite per ottenere una digitalizzazione affidabile nell'edificio. Anche in questo caso, le etichette degli edifici esistenti dovrebbero essere prese in considerazione in qualsiasi realizzazione.

Management Summary (E)

By 2050, Switzerland aims to have stopped emitting more greenhouse gases into the atmosphere than are absorbed by natural and technical storage (the Net Zero Target). Achieving the Net Zero target by 2050 will primarily require emissions in the building sector, transport and industry to be comprehensively reduced.

In the building sector, digitalisation can be play a crucial role. The use of digitalisation in buildings to potentially increase energy efficiency and reduce emissions raises an increasing number of fundamental questions about interoperability, data protection and cybersecurity that need to be addressed. Considering these issues is a primary requirement for successful digitalisation in buildings. However, at present, the complexity and challenges of these issues also make them obstacles.

In order to identify any further obstacles and lay the foundations for digitalisation in buildings, guidelines on connectivity in buildings must be drawn up and the issues of interoperability, data protection and cybersecurity must be analysed.

A first project phase included a market analysis and needs assessment focusing on interoperability, cybersecurity and data protection in buildings. The analysis and assessment reveal a general awareness of the importance of connectivity in a building when it comes to increasing efficiency through integrated systems. The risks related to cybersecurity and data protection are also recognised. Some of the respondents in the analysis already use the data collected in buildings to streamline their operations, but still see room for improvement. The respondents identify the high complexity of the systems, the frequent lack of know-how among professionals with regard to connectivity issues, and the high number of standards, norms, guidelines and protocols as major obstacles.

Analysis shows that often there is no interdisciplinary cooperation, as a silo mentality prevails among those involved. As a result, the individual systems are not well coordinated, or not even networked with each other at all. The reason for the lack of cooperation is the absence or inadequacy of incentives to consider the various systems in a building as an overall system. Often the benefits of cooperation are not known or poorly understood. Respondents also have the impression that collaboration between different groups of professionals makes the job more complex.

The respondents in the analysis recognise the importance of cybersecurity and data protection. However, the approach to dealing with networked devices and data is often not suitable for countering the risks posed by cyber attacks and data misuse. Standards and guidelines contain approaches to solutions or rules of conduct to counter the risks, but respondents are not aware of them or consider them too complex. The cost of measures to increase data protection and cybersecurity is rated as high.

In the second phase of the project, a target state was developed with the participating companies, universities and associations. An essential component of the target state is ensuring the capabilities of all professionals involved in planning, construction and operation with regard to the digitalised operation of the buildings. Support for those using digitalisation when the building is in operation is important. This should make it possible to incorporate connectivity, cybersecurity and data protection into education and training, thus ensuring that graduates have the necessary skills to use them in planning, construction and operation. In addition, the introduction of an integrated planning approach will demonstrate that interdisciplinary cooperation across all phases (planning, construction and operation) can increase efficiency in the building sector, and show what such an increase looks like. Guidelines for specific applications in planning, construction, operation and use, which have yet to be drawn up, will play an important role. By outlining the approach, the stakeholders involved and the procedures for the most important applications of digital solutions in the building, the guidelines allow the potential of digitalisation to be taken into account from the very beginning. The guidelines are intended to support those concerned in their efforts to integrate the systems in the building, to comply with data protection requirements and ensure cybersecurity.

Various measures are necessary to achieve the target state. These aim in particular to support all those involved in the planning, construction and use of the digitalised systems. This is why it is important to start by providing education and training specifically geared towards the potentials of digitalisation for the building sector and in its operation. Furthermore, it is important to support interdisciplinary cooperation between the different stakeholders, which can be encouraged in guidelines. Simplified access to standards is also crucial.

Interdisciplinary networking should already be taken into account in the planning phase through integrated planning. In order to encourage this, it must also be tackled in education and training. Education and training programmes in the traditional sectors relating to buildings need to be expanded. This requires that those responsible for developing education and training programmes must be made aware of the changes. They need support, e.g. by specifying the skills that graduates need to acquire.

Standardised tools can offer help to improve digitalisation in buildings, thereby increasing the energy efficiency and comfort of those buildings. The European Commission's *Smart Readiness Indicator* (SRI) is a tool that can measure and evaluate the intelligence of buildings. The SRI increases the capabilities of the person ordering the work; it provides the user in a transparent and intuitive way with key information about a building's level of intelligence and the potential benefit that it brings. The tool is designed so that it can be used by all those involved in the planning, construction and operation of buildings. The SRI makes it possible for those concerned to evaluate and compare a building's level of digitalisation, such as the use made of energy management systems. A significant level of digitalisation can add value to a building on the real estate market in the long term. The next step is for Switzerland to adopt and use the SRI. To this end, the applicability of the SRI in Switzerland is to be demonstrated and tested as part of a preliminary study involving the sector, and the feasibility of integrating the SRI into existing labels (Minergie, SNBS) is to be investigated.

However, the SRI alone is not enough. The complexity of the subject of building automation and energy management systems in itself, and the range of technical solutions on offer, which is hard to get to grips with and assess the merits of, present serious challenges both to potential buyers and to users. The technical complexity and the cost of installation acts as a deterrent, while at the same time it is not always clear what the benefits will be. While the SRI can make the latter clearer, the buyer’s knowledge can be improved by providing greater market transparency in relation to building automation, particularly with regard to energy management systems. Often customers are unaware what solutions are available on the market, what the systems actually do and how interoperable they are, or what standard they are based on. A regular review of the market and analyses that are available to everyone, e.g. in the form of an easily understandable web application, can reduce this obvious barrier and provide some guidance. The first market review, issued in 2020 with support from Energie Schweiz provides an excellent basis and should be expanded and enhanced with clear key performance indicators tailored to the needs of customers. Guidelines will need to be developed to support the interoperability of digital solutions, reduce the integration effort and encourage interdisciplinary cooperation.

Information on data protection and cybersecurity in specific contexts should be made available in the form of guidelines to support those involved in the development, operation and use of buildings. Guidelines geared to the problem and to the stakeholder group would reduce uncertainties. The NIST Cybersecurity Framework provides a basis, which helps in understanding, managing and reducing cybersecurity risks and protecting networks and data. Based on the NIST Cybersecurity Framework, and expanded to include various standards and norms, a digital (web) solution can produce user-specific guidelines once certain parameters have been entered into it. With this simple and intuitive possibility for producing user-specific guidelines, resistance to digitalisation in buildings due to the complexity and intractability of aspects of information security can be reduced.

Other measures that have been proposed relate to raising awareness of the need to maintain cybersecurity and data protection. People purchasing or developing systems, and those responsible for running them should be helped to understand the importance of information security in relation to a building, through information campaigns, education and training, and roadshows. In the case of education and training, the content and target groups still need to be defined in order to improve capabilities in relation to information security in the industry. The existing courses on offer must be expanded and new teaching and study programmes must be created. The certification and labelling of an approved standard of digitalisation in buildings can also increase customer’s abilities related information security. A certification procedure will make it clear which guidelines must be followed in order to achieve the requisite standard of digitisation in a building. Here, too, existing building labels would have to be taken into account in the event of realisation.

2 Ausgangslage und Problemstellung

Die Schweiz soll ab 2050 nicht mehr Treibhausgase in die Atmosphäre ausstossen, als durch natürliche und technische Speicher aufgenommen werden (Netto-Null-Emissionen). Der Bundesrat hat dieses Ziel im August 2019 als Reaktion auf den Sonderbericht des Weltklimarats (IPCC[1], Lit. 14) über eine Erderwärmung von 1.5 °C beschlossen.

Um das Netto-Null-Ziel bis 2050 zu erreichen, müssen hauptsächlich die Emissionen im Gebäudebereich, im Verkehr und in der Industrie umfassend vermindert werden.

Diese Ziele werden ebenfalls in der Energiestrategie 2050 berücksichtigt, welche die Dekarbonisierung durch die Steigerung von Energieeffizienz und durch den Ausbau von (neuen) erneuerbaren Energien vorantreiben möchte.

Der Begriff Dekarbonisierung steht für die Umstellung auf eine Lebens- und Wirtschaftsweise, welche den Ausstoss von Kohlendioxid nachhaltig reduziert. Das Endziel ist eine CO_2 freie Weltwirtschaft, um den Klimawandel aufzuhalten.

Gebäude sind ein immens wichtiger Bereich, wenn es darum geht, diese Klimaziele zu erreichen und Energie effizient einzusetzen. Die Digitalisierung bietet mit neuen Technologien wie IoT, BigData, Künstliche Intelligenz, BIM usw. wichtige Werkzeuge, um die Dekarbonisierung des Gebäudeparks zu unterstützen.

Damit aus den neuen Technologien ein Nutzen für die angestrebten Ziele erreicht werden kann, müssen sich zunehmend grundsätzliche Fragen zu Interoperabilität, Datenschutz und Cybersicherheit - welche immer mehr als Hemmnisse wirken - gestellt werden. In den nachfolgenden Kapiteln werden die bestehenden Barrieren bei der Systemintegration aufgezeigt.

Neben den Technologien sind die Interessen aller relevanten Akteure, insbesondere der Gebäudebetreiber, ebenso wichtig. Weiter zeigt dieser Bericht auf, wie die interdisziplinäre Zusammenarbeit der einzelnen Gewerke, Disziplinen und Technologien stärker ins Zentrum gerückt werden kann, um die gewünschte Qualität, Sicherheit und Effektivität im Technologieeinsatz zu erreichen.

Dieser Bericht soll als Grundlage dienen, um ein disziplinenübergreifendes Verständnis für digitale Funktionen und Prozesse zwischen den Gewerken, Disziplinen und Technologien im Gebäude zu verbessern und die Vernetzung innerhalb der Anspruchsgruppen zu stärken.

Wesentliche Akteure im Projekt waren Gebäudeinvestoren, -eigentümer, -betreiber und marktrelevante Unternehmen, Verbände und Vereine aus der Gebäudebranche (SmartGridReady, Building Excellence, DIE PLANER-SWKI, GNI, BELIMO Automation, SAG Software Systems, BuildingMinds, Siemens Schweiz, Schneider Electric Schweiz, ENGIE Services, Griesser, Planzer Transport, Roche Diagnostics, Microsoft Schweiz, bonacasa, BKW Energie, Swiss Life Asset Management, Helbling Technik Bern). Neben dem energie-cluster.ch und Energie Schweiz waren weitere Akteure die HSLU, die FHNW und die Empa.

2.1 Die Energiepolitischen Ziele im Gebäudebereich

Der Gebäudepark ist für rund einen Viertel des inländischen CO_2-Ausstosses verantwortlich (Abbildung 1). Wobei rund 70% des Gebäudeenergieverbrauchs auf die Heizung entfallen. Heizungen werden noch zu 55% mit fossilen Brennstoffen (Heizöl und Erdgas) betrieben (Lit. 5).

Zudem verbrauchen Immobilien während ihres Lebenszyklus (Bau und Betrieb) etwa 100 TWh oder rund 45% des Endenergiebedarfs der Schweiz (Lit. 4).

Gemäss Energiestrategie 2050 soll der Endenergieverbrauch bis 2050 auf 65 TWh sinken und eine CO_2 Bilanz von Netto-Null aufweisen.

[1] IPCC = Intergovernmental Panel on Climate Change

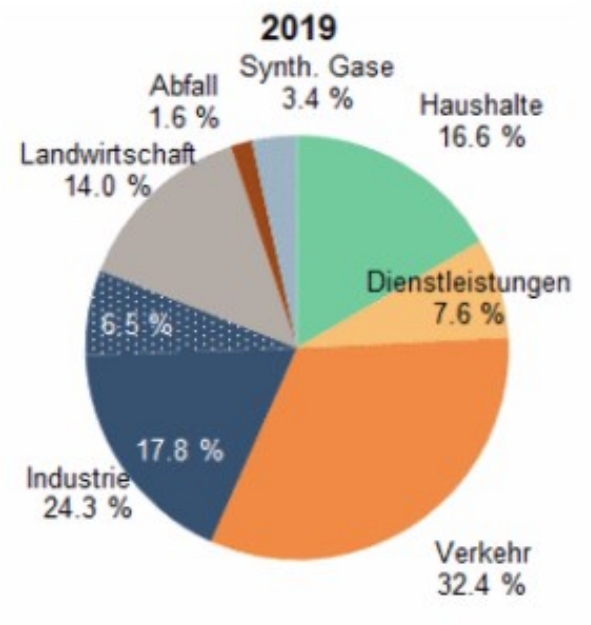


Abbildung 1 Treibhausgasinventar der Schweiz 2019. Die Bereiche Haushalte plus Dienstleistungen ergeben zusammen den Sektor "Gebäude" mit 24.2 % Quelle: BAFU Treibhausgasinventar (Lit. 6)

Um zu überprüfen, ob sich die verschiedenen Sektoren hinsichtlich der Reduktion der Treibhausgasemissionen auf Zielkurs befinden, wurden für das Jahr 2020 indikative Ziele festgelegt. Das Ziel für den Sektor Gebäude beträgt bis dahin eine Reduktion von 40 % gegenüber 1990.

Der Gebäudesektor wird sein Ziel höchstwahrscheinlich verfehlen, da trotz der Angebote der öffentlichen Hand (Förderbeiträge, Energieberatungen usw.) und einer Abgabe auf Brennstoffe, zu wenige Gebäude energetisch erneuert und zu wenige fossile Heizungen durch erneuerbare Alternativen ersetzt werden (Abbildung 2).

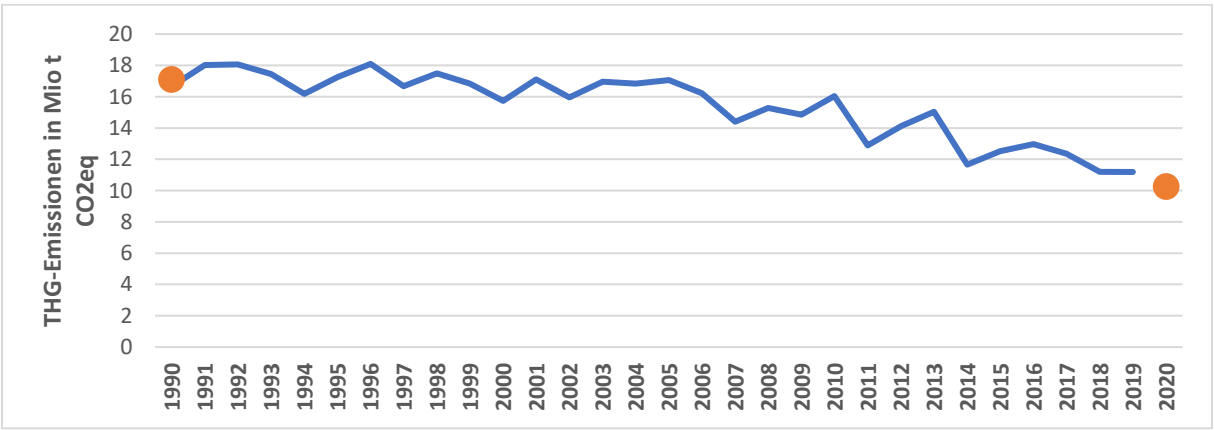


Abbildung 2: Treibhausgasemissionen Sektor Gebäude (blaue Linie); Basis 1990 und Zwischenziel 2020 (Punkte). Quelle: BAFU Treibhausgasinventar (Lit. 6)

2.2 Massnahmen zur Reduktion der CO_2 Emissionen im Gebäudebereich

Für die Reduktion der CO_2 Emissionen im Gebäudeberiech existieren aktuell folgende klimapolitischen Instrumente:

- CO_2 Abgabe auf fossile Brennstoffe,
- Gebäudeprogramm,
- Kantonale Gebäudevorschriften auf Basis der Mustervorschriften der Energiedirektorenkonferenz (MuKEn 2014, Lit. 16).

Die CO_2-Abgaben für Brennstoffe wie Heizöl oder Erdgas wurden per 1. Januar 2022 von 96 auf 120 Franken pro Tonne CO_2 erhöht, da das Zwischenziel von minus 33% bis 2020 nicht erreicht wurde.

Ein Teil der Einnahmen aus diesen Abgaben fliesst in das Gebäudeprogramm.

Seit 2010 gewährt das Gebäudeprogramm Fördermittel für folgende Massnahmen:

- Wärmedämmung von Bestandsgebäuden;
- Installation von Haustechnikanlagen: Heizsysteme, die mit erneuerbarer Energie betrieben werden, aber auch Lüftungsanlagen mit Wärmerückgewinnung;
- Systemsanierungen, d.h. umfassende Gebäudesanierungen, sowie energetische Sanierungen in grösseren Etappen, bei denen das Haus als Gesamtsystem mit Massnahmen an Gebäudehülle und Haustechnik energetisch aufgewertet wird;
- Bau und Erweiterung von Anlagen zur zentralen, hausübergreifenden Wärmeversorgung von Gebäuden mit Wärme aus erneuerbaren Energien oder Abwärme;
- Hocheffiziente Neubauten.

Seit 2018 werden über das Gebäudeprogramm auch Beiträge an indirekte Massnahmen, d.h. Projekte im Bereich der Qualitätssicherung, Beratung, Information, Veranstaltungen sowie Aus- und Weiterbildung gewährt.

Die «Mustervorschriften der Kantone im Energiebereich» (MuKEn) bilden ein von den Schweizer Kantonen gemeinsam erarbeitetes Gesamtpaket energierechtlicher Vorschriften im Gebäudebereich. Die Vorschriften enthalten ein für die Kantone zwingendes Basismodul, das minimale Anforderungen definiert. Zusätzlich gibt es weitere zehn Module, die die Kantone auf freiwilliger Basis übernehmen können. Unter den freiwilligen Modulen befindet sich beispielsweise auch das Modul «Ausrüstungspflicht Gebäudeautomation bei Neubauten». In diesem Modul wird die Wichtigkeit von Digitalisierung in Form von Gebäudeautomation für die Steigerung von Energieeffizienz dargestellt.

2.3 Der Beitrag der Digitalisierung für Klimaschutz und Energieeffizienz im Gebäudebereich

Die Kurzstudie «Klimaschutz und Energieeffizienz durch digitale Gebäudetechnologien» der Bitkom e.V. (2021, Lit. 2) hat die Potenziale für Klimaschutz und Energieeffizienz in Deutschland erfasst, die sich durch digitale Technologien im Gebäudesektor erschliessen lassen. Dafür wurden einzelne Technologien und ihr möglicher Beitrag zum Klimaschutz und der Energieeffizienz in Gebäuden analysiert. In einem zweiten Schritt wurden Szenarien für Wohn- und Nicht-Wohngebäude für die Jahre 2030 und 2045 berechnet, die CO_2-Minderungspotenziale für ausgewählte Technologien ausweisen. Ein Schwerpunkt liegt dabei auf dem Potenzial von effizientem Energiemanagement durch Gebäudeautomation.

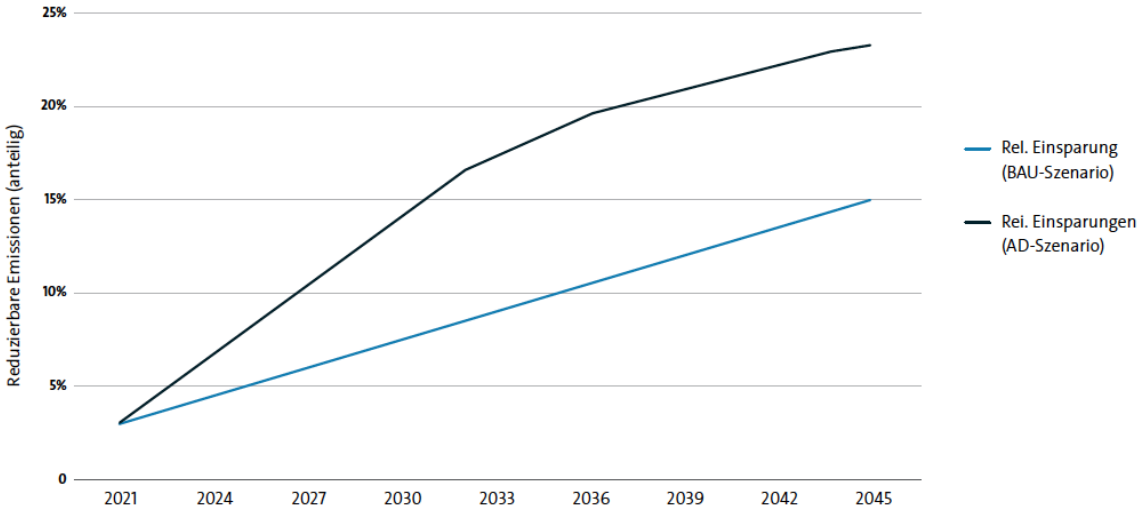
Insgesamt zeigt die Studie, dass durch einen ambitionierten Ausbau von Gebäudeautomation kurz- bis mittelfristig (2030) sieben bis acht Prozent der CO_2-Emissionen im Gebäudesektor eingespart werden können (Abbildung 3). Nicht nur im Betrieb, sondern auch entlang des Lebenszyklus von Gebäuden wurden hohe Potenziale identifiziert, um die CO_2-Emissionen durch den Einsatz verschiedener digitalen Technologien zu verringern. Beispielsweise kann Building Information Modelling (BIM) zur Analyse und Bewertung der Energie- und Rohstoffflüsse entlang des Lebenszyklus von Gebäuden verwendet werden.

Zentral für die Berechnung der Szenarien in dieser Studie ist, dass für die ausgewählten Technologien gesicherte Erkenntnisse zu den Einsparungen vorliegen. Dies ist für die Gebäudeautomation der Fall, da die hiermit erzielbaren Einsparungen bereits in zahlreichen Studien dokumentiert wurden.

Basierend auf den Effizienzklassen der Gebäudeautomation (gemäss DIN EN 15232, Lit. 1) können verlässliche CO_2-Einsparungen ermittelt werden, die bei unterschiedlichen Ausrüstungsgraden des Gebäudebestands erreicht werden. In der Norm wird beschrieben, wie Einspareffekte durch Gebäudeautomation ermittelt und welche Automationsgrade im Gebäude welchen Effizienzklassen zugeordnet werden können.

- Zur Reduktion des Wärmebedarfs und des Energieverbrauchs von Gebäuden wird Gebäudeautomation (GA) in Form von intelligenter Heizungssteuerung eingesetzt. Durch den Einsatz von GA-Systemen mit hoher Effizienz liegt das Sparpotenzial von Wärmeenergie für

Wohngebäude bei 19 Prozent und für Nicht-Wohngebäude je nach Typ zwischen 14 und 50 Prozent.



Quelle: Borderstep Institut 2021

Abbildung 3: Anteilige CO_2-Minderungspotenziale im Verhältnis zu den Gesamtemissionen. BAU-Szenario = Business As Usual (langsamer Ausbau der Gebäudeautomation); AD-Szenario = Ambitioniertes Digitalisierungsszenario mit einem schnellen Ausbau der Technologien.

- In den Bereichen Kühlung und Beleuchtung wird die Gebäudeautomation genutzt, um den Stromverbrauch in Gebäuden zu reduzieren. Grundsätzlich sind die CO_2-Minderungspotenziale aus der intelligenten Steuerung elektrischer Verbraucher derzeit niedriger als die aus der Reduktion des Wärmebedarfs. Dies liegt vor allem daran, dass Wärmeenergie derzeit einen Anteil von 70% des Gebäudeenergiebedarfs ausmacht. Das CO_2-Reduktionspotential für diesen Bereich lässt sich nur beschränkt auf die Schweiz übertragen. Während die Schweiz einen Anteil von ca. 75% an erneuerbaren Strom hat, besitzt Deutschland einen Anteil von rund 50%. Die Studie weist im «Ambitioniertes-Digitalisierungsszenario» eine CO_2-Reduktion von bis zu 8% aus, in den Jahren 2036 - 2045. Für die Schweiz würde sich die Einsparung um die 4% bewegen.

- In den Bereichen Sektorenkopplung und Flexibilität wird analysiert, wie der Anteil der neuen erneuerbaren Energien durch die Flexibilisierung in den Gebäuden gesteigert werden kann bzw. wie die volatile Produktion von Wind- und Solarstrom im Zusammenspiel mit Speichermöglichkeiten (Warmwasser/Heizung, Batterien) im Gebäude zu einem höheren Anteil genutzt werden kann. Dieses Potential ist sicher auch in der Schweiz vorhanden. Ein direkter Vergleich mit Deutschland in diesem Bereich ist schwierig, da die Ausgangslage auch hier sehr unterschiedlich ist. Während die volatile Stromproduktion aus Wind und Sonnenenergie in der Schweiz im Jahr 2020 knapp 4% (Lit. 15) des Strommixes ausmachte, war der Anteil in Deutschland rund 35% (Lit. 23).

Nebst der Gebäudeautomation besitzen auch andere digitale Technologien wie der Einsatz von BIM-Systemen ein hohes Potenzial für die Erhöhung von Energieeffizienz im Gebäudebereich. Nicht nur der Betrieb von Gebäuden, sondern auch Sanierung und Rückbau benötigen grosse Mengen an Energie und Ressourcen.

- In der Planung können mit BIM schnell und genaue Varianten bezüglich Energieverbrauch und Unterhalt simuliert werden. Auch die Nachhaltigkeit der Materialwahl kann bereits in dieser Phase abgebildet und somit optimiert werden.
- Während der Bauphase können mittels BIM Fehler frühzeitig erkennt werden. Die Fehlerquote wird gesenkt und Ressourcen effizienter eingesetzt.

- Im Betrieb hilft der digitale Zwilling dabei, den Betrieb zu überwachen, vorausschauende Wartungen durchzuführen und Erkenntnisse über die Verbesserung von Prozessen zu gewinnen.

Für die Erreichung der gesetzten Ziele betreffend Emissionen und Effizienz bis 2030 beziehungsweise 2050 ist eine Kombination von Massnahmen (Einsatz digitaler Gebäudetechnologien, energetische Sanierung unterstützt durch Fördergelder, Dekarbonisierung des Strommixes, CO_2-Abgabe) notwendig. Dieser Bericht leistet einen Beitrag zur Diskussion, wie Digitalisierung und eine bessere «Interoperabilität» einen Beitrag für die Klima- und Energieziele im Gebäudebereich leisten können.

2.4 Interoperabilität im Gebäude

Im vorherigen Kapitel wurde aufgezeigt, dass durch den Einsatz von digitalen Gebäudetechnologien sieben bis acht Prozent der CO_2-Emissionen im Gebäudesektor eingespart werden können. Damit das volle Potenzial in diesem Bereich ausgeschöpft werden kann, muss in den Gebäuden die Konnektivität gewährleistet werden.

Konnektivität wird mehrheitlich mit der Vernetzung von Geräten untereinander in Verbindung gebracht. Vielfach wird hierfür auch der Begriff Interoperabilität verwendet. Unter Interoperabilität wird das möglichst nahtlose Zusammenspiel verschiedener Systeme, Techniken oder Organisationen verstanden. Insgesamt werden vier Ebenen der Interoperabilität mit spezifischen Zielen, Aufgaben und Standards unterschieden:

1. Die organisatorische Ebene bezieht sich auf die effiziente Organisation der Prozesse.
2. Auf der semantischen Ebene geht es darum, die ausgetauschten Informationen korrekt zu interpretieren.
3. Auf der syntaktischen Ebene werden die gesuchten Informationseinheiten im Datenstrom identifiziert.
4. Die strukturelle Ebene betrifft den Datentransfer von einem zum anderen System.

Durch die zunehmende Technik in den Gebäuden, nimmt auch die Vernetzung der unterschiedlichen Geräte (z. B. Heizung, Kühlung, Lüftung, Beleuchtung, Storen, etc.) zu. Die Herausforderung hiervon ist, dass mit der Zunahme der Geräte, die miteinander vernetzt werden können, auch eine Zunahme der unterschiedlichen Protokolle und Schnittstellen einhergehen. Dies führt vielfach dazu, dass die Geräte untereinander nicht oder nur mit entsprechendem hohen Integrationsaufwand vernetzt werden können.

Auch findet im Gebäude ein zunehmender Wandel von «Consumer» zu «Prosumer» statt, unterstützt durch den vermehrten Einsatz von digitalen Technologien wie Energiemanagement in Kombination mit Photovoltaik und Batterieladestationen etc. Mit der Zunahme dieser Technologien, nimmt auch die entsprechende Datenmenge zu. Zudem werden diese Technologien zunehmend mit dem Internet verbunden. Dadurch steigen die Risiken bzgl. Datenschutz und Cybersicherheit, verbunden mit immer mehr Daten, welche in der Cloud aufgezeichnet und verarbeitet werden.

Die beschriebenen Ebenen der Interoperabilität zeigen, dass für eine ganzheitliche Betrachtungsweise die Interessen aller Beteiligten zu berücksichtigen sind. Daher sollten auch soziale, ökonomische und ökologische Aspekte, in die Definition von Konnektivität miteinfliessen. Erst durch eine ganzheitliche Betrachtungsweise kann das Verständnis für digitale Funktionen und Prozesse zwischen den Gewerken, Disziplinen und Technologien im Gebäude erhöht werden.

Das Projekt Konnektivität im Gebäude adressierte diese ganzheitliche Betrachtungsweise für die Themen Interoperabilität, Datenschutz und Cybersicherheit im Gebäude. Kapitel 3 beschreibt den im Projekt erarbeiteten Ist- und Soll-Zustand. Kapitel 4 geht auf die Lücken zwischen Ist- und Soll-Zustand ein. Die vom Projektteam empfohlenen Massnahmen beschreibt Kapitel 5. Und Kapitel 6 erläutert die nächsten Schritte.

2.5 Abgrenzungen

2.5.1 Smart Building versus Smart Home versus Energiemanagementsysteme

Im Zusammenhang mit dem Thema Konnektivität im Gebäude kommen die Begriffe Smart Building und Smart Home oft vor.

Smart Building kann als Weiterentwicklung der Gebäudeautomation verstanden werden. Neu können dank Messfühlern, die online verbunden sind, Sensordaten ständig per Software ausgewertet werden. Ebenso kann die Software aus diesen Daten optimale Betriebseinstellungen berechnen und gleich automatisch umsetzen, indem sie diese an die Antriebselemente der Haustechnik weitergibt.

Beim Thema Smart Home geht es um digitale Wohnkonzepte. Hier nehmen einfach bedienbare Systeme den Hausbewohnern Aufgaben ab und sorgen für mehr Komfort und Sicherheit.

Energiemanagementsysteme werden oft als Teil der oben genannten Konzepte verstanden. Das EMS ermöglicht neben systematischer Erfassung und Kommunikation der Energieströme (Verbrauch und Produktion) auch die automatische Steuerung von Einrichtungen und Apparaten (z.B. Wärmepumpen, Ladestationen, etc.). Das EMS kann mit mindestens zwei verschiedenen Einrichtungs-/Apparat-Typen (z.B. PV Anlage und Wärmepumpe) kommunizieren und diese steuern. Das EMS besteht aus Einrichtungen lokal beim Kunden und unter Umständen weiteren Systemen. Die Aufnahme von Daten erfolgt dezentral beim Kunden während die Bearbeitung und die Generation von Steuersignalen entweder zentral in einer Cloudlösung bzw. einem Server oder dezentral direkt innerhalb des beim Kunden installierten Systems erfolgen. Das EMS wird entweder unabhängig oder gekoppelt an die bestehenden Systeme von Energieversorgungsunternehmen, Netzbetreibern, Messdienstleistern, Installationsbetrieben oder anderen Anwendern, wie z.B. Energiedatenmanagement, etc. betrieben[2]

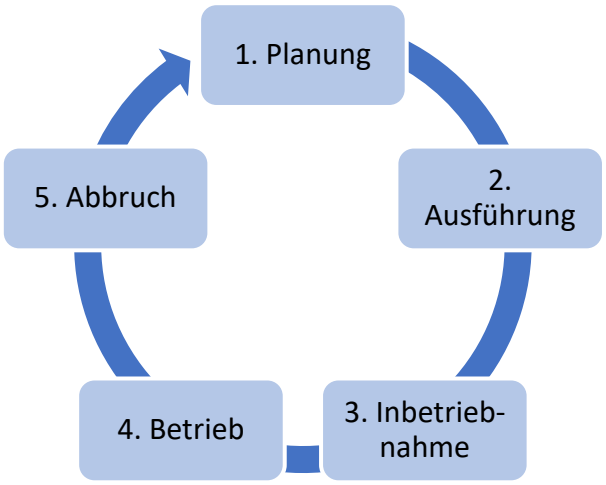
Die Ziele und die Technik dahinter überschneiden sich teilweise zwischen Smart Building und Smart Home. Die technische Grundlage ist in beiden Fällen Internet-of-Things-Geräte, die aus der Ferne ausgelesen und gesteuert werden können. Zentrale Ziele sind in beiden Fällen die Optimierung des Energieverbrauchs und der Betriebskosten sowie die Erhaltung oder Steigerung des Komforts.

Da eine Gebäudeautomation nur bei komplexerer Gebäudetechnik Sinn macht, werden unter Smart Building grösstenteils Geschäftsliegenschaften und Mehrfamilienhäuser verstanden, auf welche sich dieser Bericht fokussiert.

2.5.2 Lebenszyklusphasen von Gebäuden

Ein wichtiger Faktor beim Betrieb von Gebäuden sind die Betriebskosten. Die Betriebskosten, verursacht z.B. durch den Energieverbrauch des Gebäudes, aber auch der Komfort für den Nutzer können in der Planungsphase eines Gebäudes beeinflusst werden, unter anderem durch die Architektur, den Ausbaustandard, den Technologieeinsatz usw. Wie in Abbildung 4 ersichtlich, betreffen gewisse Technologien gleich alle Phasen, andere digitale Technologien finden nur in einzelne Stadien der Lebenszyklusphase eine Anwendung. Für das Projekt war es wichtig, dass alle Akteure, welche in die einzelnen Lebenszyklusphasen von einem Gebäude involviert sind, im Projekt vertreten sind. Die wichtigsten Bereiche sind die Planung und der Betrieb, dementsprechend nehmen sie im Bericht am meisten Raum ein. Das ist darin begründet, dass Entscheidungen in der Planung direkte Auswirkungen auf den Einsatz von digitalen Technologien haben, welche dann die Betriebskosten und den Energieverbrauch im Gebäude prägen.

[2] Lit.25



Technologie	Planung	Bau	Betrieb	Abbruch
IoT	+	+	+	
Advanced Data Analytics	+		+	
BIM	+	+	+	+
Robotik		+	+	+
Location based Services		+	+	
Plattformen	+	+	+	+

Abbildung 4: Lebenszyklusphasen von Gebäuden Vereinfachte Tabelle auf Basis von Schmidiger & Kraft (2018, Lit. 10)

3 Bestimmung IST- und SOLL Zustand

Wie in Kapitel 2 beschrieben, kann Digitalisierung für eine effizientere Nutzung von Ressourcen und Energie im Gebäudebereich eingesetzt werden. Das Potenzial für den Einsatz von digitalen Gebäudetechnologien und die Konnektivität ist gleichzeitig noch nicht ausgeschöpft. In diesem Kapitel wird der Frage nachgegangen, wie der aktuelle Stand bezüglich des Einsatzes von digitalen Technologien im Gebäude aussieht, welche Hemmnisse für deren Ausbau derzeit existieren und wie diese angegangen werden können.

Um den Ist- und Soll-Zustand bei den involvierten Anspruchsgruppen (Gebäudeeigentümer*innen, Gebäudeinvestoren*innen, Gebäudebetreiber*innen, Planer*innen, Integratoren*innen, Hersteller*innen) zu erfassen, wurde ein Fragebogen zu den Themen Bewirtschaftung, Funktionalität/Technologie, Datenschutz und Cybersicherheit erstellt. Der Fragebogen wurde verschiedenen Personen der erwähnten Anspruchsgruppen zugestellt. Insgesamt haben die Befragten 34 Fragebögen retourniert. Die Befragten hatten die Möglichkeit, ihre Identität offenzulegen. Unter den Teilnehmenden befanden sich Unternehmen aus verschiedenen Bereichen wie Industrie, Versicherungen, Pensionskassen, Wohnbaugenossenschaften, Behörden usw.

Innerhalb des Projektteams wurden zusätzlich Workshops mit Vertreter*innen von marktrelevanten Unternehmen und Verbänden aus der Gebäudebranche, Investierende, Eigentümer und Betreiber durchgeführt. In den Workshops wurden die Themen Interoperabilität, Cybersicherheit und Datenschutzbehandelt und diskutiert. Die Ziele dieser Workshops waren der Ist-Zustand sowie der Soll-Zustand für diese drei Themen zu erfassen und zu diskutieren. Die Ergebnisse der Umfrage konnten in den Workshops als Diskussionsbasis verwendet werden.

Für die Analyse des Ist- und Soll-Zustands wurden nebst der Umfrage und den Workshops zusätzliche Recherchen durch die Projektteilnehmenden durchgeführt. Insbesondere wurden zusätzliche Informationen zu Technologien, Standards, Normen und Richtlinien zusammenzutragen.

3.1 «IST-Zustand» Interoperabilität

Mit der zunehmenden Digitalisierung im Gebäude, wird ein funktionierendes Zusammenspiel zwischen verschiedenen Systemen, Techniken aber auch Organisationen und Disziplinen immer wichtiger. Wie die Situation bezüglich der Interoperabilität im Gebäude wahrgenommen wird, zeigt dieses Kapitel.

3.1.1 Umfrageergebnisse

Aus der durchgeführten Umfrage geht hervor, dass in Bezug auf die Interoperabilität Verbesserungspotenzial besteht, damit die Dekarbonisierung des Gebäudesparks beschleunigt werden kann. 91% der Befragten (52% = ja / 39% = eher ja) geben an, dass ihre Anlagen besser betrieben werden könnten, wenn die Gewerke besser aufeinander abgestimmt wären (Abbildung 5). 80% der Befragten (Mehrfachnennung) geben an, dass sie von einer Abstimmung der Gewerke absehen, weil die Technologien und Schnittstellen unterschiedlich, unklar oder zu kompliziert seien. Weitere 35% (Mehrfachnennung) finden, dass die Prozesse und Anforderungen unklar seien. 65% (Mehrfachnennung) der Befragten geben zusätzlich an, dass wegen zu hoher Komplexität der Thematik keine Gegenmassnahmen eingeleitet werden. Die Autoren intepretieren dies in die Richtung, dass innerhalb der eigenen Organisation zuwenig Fachwissen vorhanden ist. Auf die Frage «Wie betreiben Sie Ihre Gebäude?» haben nur 12% mit internem Fachpersonal geantwortet. Die anderen Antworten waren mit nur externe Dienstleister (24%), internes Fachpersonal im Zusammenspiel mit externen Dienstleistern (44%), externe Dienstleister mit Unterstützung internes Fachpersonal (12%). 76% (Mehrfachnennung) der Befragten geben an, dass Weiterbildungen im Bereich «vernetzte Systeme» in Zukunft wichtig für einen effizienten Gebäudebetrieb sein werden. Weitere 46% (Mehrfachnennung) geben an, dass sie ihre Mitarbeitenden bereits intern oder extern im Bereich Gebäudeautomationssysteme schulen lassen. Lediglich 3% (Mehrfachnennung) ist überzeugt, dass auf dem Arbeitsmarkt bereits genügend gut ausgebildetes Personal im Bereich «vernetzte Systeme» vorhanden ist, was klar aufzeigt, dass ein Fachkräftemangel vorhanden ist.

Obwohl lediglich 21% der Befragten angeben, dass die technischen Installationen gemäss ihren Erwartungen funktionieren, ist die Modernisierungsrate tendenziell eher tief. Gemäss Befragten liegt dies vorallem daran, dass es keine gesetzlichen Vorschriften oder Zwänge gibt (58% Mehrfachnennung). Weitere Argumente gegen eine Modernisierung sind das schlechte Kosten/Nutzenverhältnis (56%) und die fehlende Übersicht bezüglich Potenziale einer Modernisierung (56%). Die Autoren schliessen aus diesen Antworten, dass der finanzielle Mehrwert von den Entscheidungsträgern vielfach noch nicht gesehen wird. Nebst der tiefen Modernisierungsrate fällt ebenfalls auf, dass bei Gebäuden mehrheitlich (57%) frühestens nach zehn Jahren Anpassungen an den Gebäudeautomationssystemen vorgenommen werden. Gründe hierfür sind gemäss den Autoren die in der Umfrage aufgeführten Punkte wie zu aufwändig (45%), zu hohe Komplexität (65%) oder kein prioritäres Problem (48%).

Ein Grossteil der Befragten erkennt ein grosses Sparpotenzial im Energieverbrauch. 71% (Mehrfachnennung) der Befragten sehen das grösste Sparpotenzial beim Heizen gefolgt von Strom (65%), Kühlen (41%), Lüftung (32%) und Andere (6%). Die Antworten der Befragten lassen Massnahmen erkennen, um das Energiesparpotenzial ausschöpfen zu können: Durch eine zentrale Verfügbarkeit der Daten (74% Mehrfachnennung), bessere Aufbereitung der Daten (68% Mehrfachnennung) und einen besseren Datenzugriff (50% Mehrfachnennung) könnte der Energieverbrauch optimiert werden. Aus der Umfrage geht ebenfalls hervor, dass in den wenigsten Fällen die Gewerke untereinander vernetzt sind und dadurch ein Informationsautausch zwischen den Gewerken mehrheitlich nicht stattfindet.

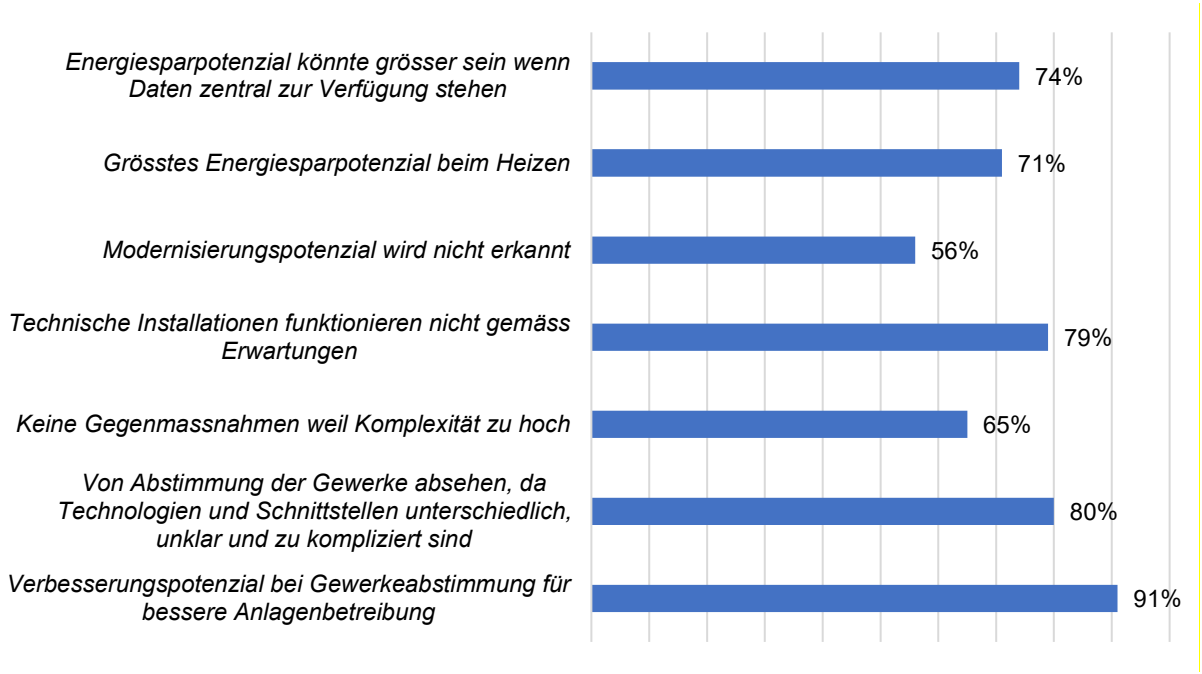


Abbildung 5: Die Ergebnisse der Befragung zum Thema Interoperabilität

3.1.2 Standards, Protokolle, Normen, Initiativen, Allianzen

Im Rahmen der Recherche zu den Protokollen, Standards, Normen, Initiativen und Richtlinien mit einem Bezug zu Gebäuden sind die Autoren auf mehr als 40 Protokolle und Standards und auf über 20 Allianzen und Initiativen gestossen. Der Eindruck der Autoren ist, dass die Anzahl der gefundenen Protokolle, Standard, Initiativen und Richtlinien nicht abschliessend ist und eher zunimmt. Dieser Umstand wird von mehr als 77% der Umfrageteilnehmenden als Problem benannt, weil für sie dadurch die Komplexität steigt. Das hat zur Folge, dass das Auffinden von relevanten Dokumenten als anspruchsvoll empfunden wird. Auch in den Workshop-Diskussionen wird die grosse technologische Vielfalt der in Gebäuden zum Einsatz kommenden Geräte und Systeme als Herausforderung benannt, weil dadurch die Komplexität steigt.

In den Diskussionen in den Workshops wird es als unrealistisch angesehen, dass sich der eine «Standard» oder dass eine «Protokoll» durchsetzt, obwohl eine Harmonisierung natürlich wünschenswert wäre. Hierfür gibt es zu viele unterschiedlich Interessen, schon nur von Herstellerseite her, um sich auf einen gemeinsamen Standard zu einigen. Auch von der Anwendung (z.B. gewerbliche Bauten oder Mehrfamilienhäuser) her entstehen unterschiedliche Anforderungen, welche kaum von nur einem Protokoll oder nur einem Standard erfüllt werden können. Festgestellt wurde auch, dass mehr Standards, Protokolle etc. zu mehr Integrationsaufwand führen, was höhere Projektkosten nach sich ziehen kann und so aus finanziellen Gründen eine stärkere Integration der einzelnen Gebäudetechnologien erschwert.

Von Herstellerseite besteht nur wenig Interesse an einer Harmonisierung, weil dies für einzelne Hersteller eine Umstellung der bisher verwendeten Standards oder Protokolle auf die harmonisierten bedeuten würde. Eine solche Umstellung ist mit Kosten verbunden, wofür für die Hersteller kaum ein Mehrwert entsteht. Auf regulatorischer Ebene lässt sich eine Harmonisierung ebenfalls kaum durchsetzen, da die technologische Entwicklung schneller fortschreitet als die politischen und regulatorischen Prozesse.

3.1.3 Resultat aus Workshops

Im Gebäudesektor ist es heute vielfach noch so, dass bei der Planung eher auf Bewährtes und weniger auf Innovatives gesetzt wird. Vielfach wird für eine möglichst günstige Realisierung geplant und die Betriebskosten werden als zweitrangig betrachtet. Dies ist unter anderem dem Umstand geschuldet, dass ein Teil der Gebäudeinvestoren gar nicht vorhat, das Gebäude längerfristig zu betreiben, sondern nach der Fertigstellung zu verkaufen. Deshalb sind für Investoren die Betriebskosten nicht von grosser Relevanz. Vielfach ist es auch so, dass die Gebäudeinvestoren auf die Planer und deren Vorschläge angewiesen sind, welche Gebäudetechnologie verbaut werden soll, da dieses Wissen innerhalb der Organisation fehlt. In den Workshop-Diskussionen hat sich gezeigt, dass Endnutzer (z. B. Mieter,

Wohnungseigentümer) nicht oder nur wenig in die Entscheidung bezüglich der geplanten digitalen Gebäudetechnologien miteinbezogen werden. In den Diskussionen hat sich herausgestellt, dass dies ein systemisches Problem ist, da die Planer vielfach über die Bausumme vergütet werden. Deshalb werden gegenwärtig vielfach schon mehrfach umgesetzte und bewährte Konzepte für die Planung wiederverwendet. Dieses Vorgehen hält den Planeraufwand so klein wie möglich, bei gleichbleibender Entschädigung. Mit dem Resultat, dass wenig neue innovative Konzepte entwickelt werden. Die gesamtheitlichen Lebenszyklusbetrachtung fehlt oft. Der Nutzen der Interoperabilität in der Planung und deren Auswirkung auf den Betrieb wird nicht erkannt und es fehlen durchgängige und kausale Prozesse. Oft wird die Integration der Gebäudetechnik spät im Prozess der Planung berücksichtigt und gewerkespezifisch durchgeführt. Das führt zu einer nicht optimalen oder gar fehlenden Abstimmung untereinander und zu einem höheren Aufwand bei der Integration der einzelnen Gewerke zum Gesamtsystem.

Nach Meinung der Teilnehmenden an den Workshops ist die isolierte Betrachtung der Gewerke mit ein Grund dafür, dass sich in den verschiedenen Branchen unterschiedliche "Sprachen» gebildet haben. Es bedeutet einen gewissen Aufwand, die Fachleute aus anderen Branchen zu verstehen. Dies wiederum erschwert die Kommunikation untereinander und somit auch die Integration der Gewerke.

Ein Ansatz, welcher oben genannte Probleme adressieren kann ist die integrale Planung (Lit. 13), welche heute aber immer noch nur bedingt angewendet wird.

Der Begriff integrale Planung steht für fachliche Integration (Gesamtkonzept über alle baulichen und technischen Gewerke), chronologische Integration (Gesamtkonzept unter Beachtung aller Lebenszyklen des Gebäudes: Ausführung, Betrieb, Umnutzung, Sanierung, Abbruch), perspektivische Integration (Gesamtkonzept unter gleichrangiger Beachtung der Aspekte Investitionen, laufende Kosten, Nutzerbehaglichkeit und -gesundheit, Ökologie).

Wie in der Umfrage hat sich auch bei den Workshop-Diskussionen gezeigt, dass digitale Gebäudetechnologien helfen können, den Energieverbrauch in Gebäuden zu reduzieren. Allerdings ist der effektive Nutzen solcher Lösungen bei Entscheidungsträgern wie Gebäudeinvestoren, Gebäudebesitzern und Gebäudebewirtschaftern noch zu wenig bekannt. Der finanzielle Mehrwert für Investitionen in gewerkübergreifende Gebäudetechnologien wird noch zu wenig erkannt. So fehlt z.B.das Bewusstsein, wie diese Investitionen den Energieverbrauch reduzieren und dadurch auch Kosten im Betrieb einsparen können.

Auch hat sich in der Befragung und in den Workshop gezeigt, dass ein Fachkräftemangel vorhanden ist. Gründe hierfür sind der demografischer Wandel, schlechtes Image, welchen Handwerksberufe anhaftet aber auch neue Fragestellungen, bedingt durch digitale Technologien, für welches das Fachpersonal erst ausgebildet werden muss. Auch die Studie von Deloitte «2020 commercial real estate industury outlook (Lit. 8)» kommt zum Schluss, dass neue Technologien, welche die Dekorbanisation unterstützen könnten, noch nicht richtig zum Einsatz kommt, da es an Fachspezialisten mangelt.

In den Workshops hat sich auch gezeigt, dass eine gewisse Abhängigkeit von den Herstellern herrscht. Einmal verbaute Gebäudetechnologie wird in den meisten Fällen wieder durch Produkte vom gleichen Hersteller ersetzt., Die Hersteller verwenden zwar vermehrt «standardisierte» Protokolle wie BACnet, KNX, Modbus, usw. aber diese werden zusätzlich herstellerspezifisch optimiert und modifiziert. Bei Ersatz durch einen anderen Hersteller muss deswegen mit einem entsprechenden Integrationsaufwand gerechnet werden.

Ein weiteres Resultat aus den Workshop ist, dass der Technologiewandel zwar sehr schnell voranschreitet, neue Lösungen und Ansätze in immer schnelleren Zyklen auf den Markt kommen, die Gebäudebranche aber nicht in Jahren sondern eher in Jahrzehnten denkt und handelt. Die Entscheidungen für oder gegen eine neue Technologie oder einen neuen Ansatz werden mehrheitlich noch immer unter dieser Denkweise gefällt, was dazu führt, dass neue und wenig erprobte Technologien und Ansätze wenig berücksichtigt werden.

3.1.4 Fazit

Die Herausforderungen für die Interoperabilität wurden in Abbildung 6 zusammengetragen.

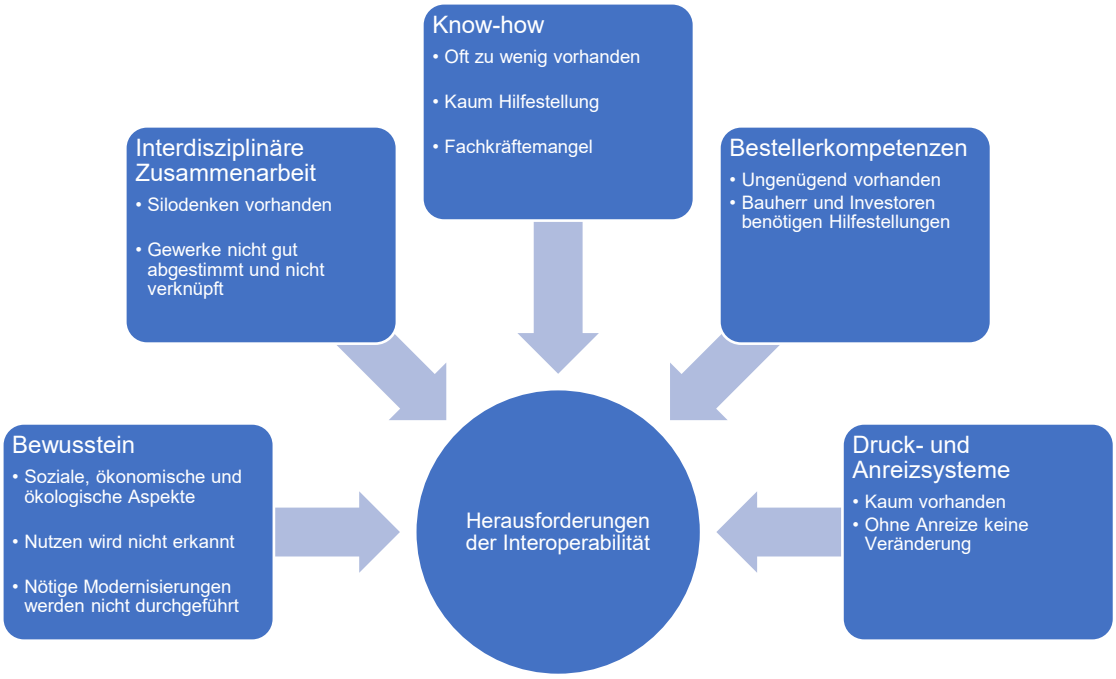


Abbildung 6: In Befragungen und Diskussionen sind einige Herausforderungen zum Thema Interoperabilität identifiziert worden.

a) Organisatorische und semantischen Ebene

Die Gebäudebranche ist noch sehr stark disziplinen- und gewerkeorientiert organisiert und strukturiert. Eine interdisziplinäre Zusammenarbeit findet in allen Phasen vielfach nicht oder nur wenig statt. Planer, Integratoren, Betreiber etc. denken primär an ihre Gewerke, was dazu führt, dass die einzelnen Gewerke nicht gut aufeinander abgestimmt oder gar nicht miteinander vernetzt sind.

Die isolierte Betrachtung der Gewerke hat auch zur Folge, dass die Kommunikation der Fachleute der verschiedenen Branchen erschwert wird. Dadurch wird die Integration der Gewerke zu einem Gesamtsystem wenig gefördert.

Neben der interdisziplinären Zusammenarbeit fehlt oft auch das entsprechend geforderte technische Know-how, um die Gebäude gewerkeübergreifend betreiben zu können. Dies weil Planende auf bewährte Konzepte setzen und so ihren Aufwand und ihr Risiko minimieren können. Neue Technologien kommen so wenig zur Anwendung. Investierende und auch Bauherren fördern dieses Vorgehen dadurch, dass sie auf eine kostengünstige Planung und Ausführung achten und weniger auf tiefe Betriebskosten. Daher fehlen Anreize, an diesem Umstand etwas zu ändern.

b) Syntaktische und strukturelle Ebene

Insbesondere auf der syntaktischen Ebene der Interoperabilität empfinden die Teilnehmenden an der Befragung sowie der Workshops die fehlende Harmonisierung von Standards als Hemmnis, weil dadurch die Komplexität für die Integration steigt. Allerdings besteht seitens der Herstellenden von Komponenten und Systemen wenig Anreiz, eine Harmonisierung zu erreichen. Einerseits sind verschiedene Standards bereits seit langem im Einsatz, ein Umstieg würde einen hohen Aufwand nach sich ziehen. Andererseits begründen verschiedene Anforderungen die Verwendung von verschiedenen Standards.

Alle Ebenen der Interoperabilität betrifft der Fachkräftemangel, welcher von den Befragten und in den Workshops genannt wird. Dabei fehlt es insbesondere an spezifischem Wissen zu digitalen Technologien.

3.2 «IST-Zustand» Cybersicherheit

Sicherheitslücken in Geräten und Systemen führen mit der zunehmenden Digitalisierung zu einer zunehmenden Gefahr von Cyberangriffen. Diese Sicherheitslücken können durch Fehler in der Programmierung, Schadsoftware oder durch einen gezielten Angriff auf das Softwareprogramm entstehen. Alle Geräte oder Techniken, welche mit dem Internet verbunden sind, sind potenziell dieser Gefahr ausgesetzt. Dies gilt auch für alle Geräte in Gebäuden, die mit Software gesteuert werden. Nicht nur die Manipulation solcher Geräte muss berücksichtigt werden, sondern auch der Schutz der damit entstehenden Daten. Wie die Situation von verschiedenen Anspruchsgruppen wahrgenommen wird, zeigt dieses Kapitel.

3.2.1 Befragung

Die im Rahmen des Projekts durchgeführte Befragung hat im Zusammenhang mit der Cybersicherheit ergeben, dass 40% der Befragten die erfassten Daten der Gebäudeautomation in der Cloud speichern (Abbildung 7). Dabei stufen 85% der Befragten den Stellenwert für die Cybersicherheit als wichtig oder sehr wichtig ein. 75% der Befragten schätzen auch die Wichtigkeit für Mieter*innen als mittel bis hoch ein. Ein Bewusstsein für das Thema ist also vorhanden. Für 65% der Befragten gibt es Unterschiede an die Anforderungen an die Cybersicherheit für private resp. kommerzielle Gebäude. Im Wesentlichen seien die Anforderungen an die Cybersicherheit im kommerziellen Bereich höher, auch weil eine Cyberattacke auf kommerzielle Gebäude als wahrscheinlicher erachtet wird als auf private Gebäude.

Trotz des hohen Bewusstseins für das Thema Cybersicherheit sehen die Befragten verschiedene Herausforderungen bei der Umsetzung von Massnahmen zur Erlangung einer genügenden Maturität der Cybersicherheit. Für 40% steht fehlendes Know-how im Vordergrund, gefolgt von fehlender Sensibilisierung der verschiedenen Anspruchsgruppen auf die Gefahren von Cyberangriffen (25% der Befragten). Fast 20% der Befragten nennen fehlende Standards als Herausforderung, weil von Standards eine Hilfestellung erwartet wird. Zudem stellen die Kosten für Anschaffung, Betrieb und Unterhalt von Systemen zum Schutz vor Cyberangriffen ein oft genanntes Hindernis dar, wobei den Befragten die konkrete Ausgestaltung solcher Massnahmen nicht immer klar ist. Weiter werden nicht geregelte Zuständigkeiten und Verantwortlichkeiten als hinderlich für die Cybersicherheit erwähnt. Weitere Herausforderungen liegen in den unterschiedlichen Systemen, auch alte Systeme (Legacy Systeme), welche miteinander vernetzt werden müssen und dadurch neue Angriffsflächen erzeugen können. Von den Befragten werden fehlender Regulationsdruck und die fehlende Überprüfbarkeit der Leistungen von Anbietern im Bereich Cybersicherheit als weitere Schwierigkeiten genannt.

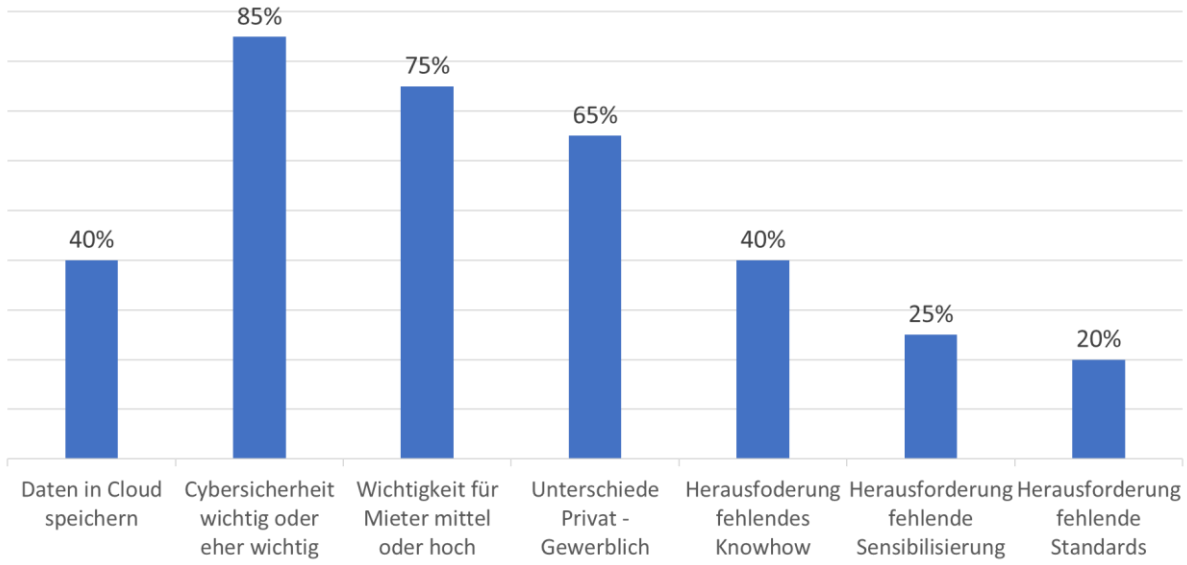


Abbildung 7: Die Ergebnisse der Befragung zum Thema Cybersicherheit

3.2.2 Standards zur Sicherheit im IoT

Die Komponenten der Gebäudetechnik und -automation sind zunehmend vernetzt und können deshalb als Teil des Internet of Things (IoT) betrachtet werden. Deshalb sind Normen, Standards und Richtlinien für IoT auch für Gebäude von Relevanz. Für den Bericht «Sicherheitsstandards für IoT-Geräte (Lit. 7)» hat die HSLU eine Übersicht von relevanten Normen, Standards, Richtlinien und Leitfäden (nachfolgend Standards genannt) zusammengestellt.

Im Bericht wird festgehalten, dass es wenige Standards spezifisch für das IoT gibt. Allerdings existieren bereits viele Standards zu unterschiedlichen Themengebieten der Cybersicherheit. Bisher konnte sich keiner der Standards richtig etablieren. Das führt dazu, dass Hersteller von IoT-Geräten aber auch Betreiber von IoT-Systemen nicht wissen, an welchen Dokumenten sie sich orientieren sollen.

Die Autoren des Berichts stellen jedoch fest, dass viele Standards für die allgemeine Cybersicherheit allgemein gültige und bewährte Verfahren beschreiben. Die Standards können grundsätzlich in managementorientierte Standards und produktspezifische Standards aufgeteilt werden. Die managementorientierten Standards beschreiben Verfahren auf organisatorischer Ebene, welche sicherstellen, dass die für Cybersicherheit relevanten Fragestellungen bei der Planung, Inbetriebnahme und dem Betrieb von IT-Systemen beantwortet werden müssen. Produktspezifische Standards beschreiben konkret Anforderungen zu Cybersicherheit in den entsprechenden Produkten und sind für die Hersteller der Produkte relevant. Berücksichtigt man die Besonderheiten des IoT, können diese Standards durchaus auf IoT-Systeme und somit auf die Gebäudeautomation angewendet werden.

Im Rahmen des Projekts KiG sind eine Reihe von Standards auf die Relevanz für die Gebäudeautomation analysiert und nach verschiedenen Kriterien klassiert worden. Die Kriterien sind i) die Anspruchsgruppe, ii) Gebäudeart, iii) managementorientierte oder produktspezifische Standards, sowie iv) Anwendungsgebiet.

Diese Analyse zeigt, dass bereits viele Standards verfügbar sind, welche im Bereich Cybersicherheit für Gebäude anwendbar sind. Die Analyse zeigt zudem, dass die Schwierigkeit vor allem darin besteht, die für einen bestimmten Kontext relevanten Standards zu identifizieren.

Mit dem NIST Cybersecurity Framework (CSF, Lit. 18) steht ein Rahmen zur Verfügung, welcher bei der Umsetzung von Massnahmen zur Cybersicherheit Hilfestellungen anbietet. Das CSF listet Richtlinien zur Minderung von Cybersicherheitsrisiken in Unternehmen auf. Diese Richtlinien basieren auf bestehenden Standards, Richtlinien und Praktiken. Das CSF gliedert diese Richtlinien in die fünf Phasen Identify, Protect, Detect, Respond und Revocer. Das Framework selber gibt keine konkreten Anleitungen, sondern beschreibt mit Hilfe der Richtlinien, wie Risiken identifiziert und wie die Systeme geschützt werden sollen. Die weiteren Punkte sind die Detektion von Angriffen und die anschliessende Antwort darauf. Für die letzte Phase beschreibt das Framework die Wiederherstellung der Systeme.

Das CSF ist sehr generisch gehalten und kann in den verschiedensten Branchen zur Anwendung kommen. Der Rahmen ist derart flexibel gehalten, dass auch nur Teile daraus angewendet werden können. Das CSF lässt sich somit an die unterschiedlichsten Bedürfnisse anpassen und kann auch in der Planung und dem Betrieb von Gebäuden angewendet werden.

3.2.3 Resultate aus Workshops

Die Herausforderungen im Zusammenhang der Cybersicherheit sind in Workshops weiter analysiert worden. Die Teilnehmenden in den Workshops waren so gewählt, dass die verschiedenen Anspruchsgruppen vertreten waren. Es hat sich gezeigt, dass für die meisten Anspruchsgruppen eine der grössten Herausforderungen darin besteht, dass der Aufwand zur Gewährung der Cybersicherheit sehr hoch scheint. Dies ist darauf zurückzuführen, dass zu wenig Know-how vorhanden ist und deshalb nicht klar ist, was an Massnahmen tatsächlich notwendig ist. Ein guter Schutz wird so mit einem hohen Aufwand für die Schutzsysteme sowie deren Unterhalt gleichgesetzt. Dieser Wahrnehmung des hohen Aufwands könnte nach Meinung der Teilnehmenden entgegnet werden, wenn es eine einfache Übersicht gäbe, an der man sich je nach eigener Ausgangslage und Anwendungsfall orientieren könnte. Ohne Orientierungshilfe ist es schwierig geeignete Massnahmen zu identifizieren und einzuleiten. Diese Herausforderungen decken sich somit mit den in der Befragung gewonnenen Erkenntnissen.

In den Workshops wurde festgestellt, dass Technologien, Herangehensweisen, Verschlüsselungsmethoden, Datenschnittstellen usw. vorhanden sind, um Cybersicherheitsrisiken zu mindern. Auch, dass für viele Anwendungsfälle, z.B. die Inbetriebnahme von mit dem Internet verbundenen Geräten, bereits Lösungsansätze vorhanden sind und diese in Richtlinien, Leitfäden oder Normen beschrieben sind. So enthält die Webseite des National Center for Cyber Security beispielsweise für Privatpersonen viele Informationen zu verschiedenen Anwendungsfällen (Lit. 17). Allerdings empfinden es die Teilnehmenden in den Workshops als schwierig, sich in der Vielfalt solcher Hilfestellungen zurechtzufinden.

Die Befragung wie auch die Diskussionen in den Workshops zeigen, dass sich die Anspruchsgruppen durchaus bewusst sind, dass Cybersicherheit ein wichtiges Thema ist. Trotzdem erscheint auch im Rahmen der Workshops das Argument der fehlenden Sensibilisierung. Dies hat nach Meinung der Teilnehmenden in den Workshops damit zu tun, dass die Menschen das Thema Cybersicherheit, u.a.

durch die erhöhte Medienpräsenz, zunehmend wahrnehmen, sich allerdings im Umgang mit verbundenen Geräten nicht immer optimal verhalten. Sie geben Daten preis, ohne genau zu wissen, was mit diesen Daten passiert (Phishing), sie wählen einfach zu merkende Passwörter oder sie schalten Sicherheitselemente zugunsten einer vereinfachten Bedienung gleich ganz ab. Gleichzeitig wurde aber auch ein Misstrauen gegenüber intransparenten Datenprozessen festgestellt. Es wird befürchtet, dass Daten in falsche Hände gelangen und/oder verfälscht werden können. Diese Befürchtung wird bestärkt, weil Cyberangriffe oft spät bemerkt werden und man im Nachhinein nicht mehr nachvollziehen kann, was mit den Daten passiert ist. Es entsteht so ein Widerspruch, dass die Menschen einerseits misstrauisch sind und Ängste entwickelt haben, wenn es um den Austausch von Daten geht. Und andererseits gehen sie zu sorglos mit verbundenen Geräten um und vergrössern so die Angriffsfläche für Cyberangriffe.

Eine weitere Herausforderung stellen die unterschiedlichen Lebenszyklen dar, mit denen man im Gebäudebereich konfrontiert ist. So liegen die Lebenszyklen der Gebäude im Bereich von einigen Jahrzehnten und bei der Gebäudetechnik bei etwa 15 Jahren. Bei IT-Komponenten jedoch liegen die Lebenszyklen im Bereich weniger Jahre. Dementsprechend häufig müssen Komponenten ausgewechselt werden, um die Cybersicherheit gewährleisten zu können. Dabei ist das Hauptproblem die Kompatibilität mit den älteren Systemteilen, welche wegen der technologischen Entwicklung u.U. nicht mehr gewährleistet werden, kann. Das kann dazu führe, dass das Gesamtsystem nicht mehr funktioniert (z.B. inkompatible Kommunikation) oder dass die Sicherheit nicht mehr gewährleistet werden kann. Softwareupdates müssen regelmässig erfolgen, so dass allfällige Sicherheitslücken geschlossen werden können. Dies stellt eine weitere Hürde dar, sofern die Updates manuell vorgenommen werden müssen.

Gerade die unterschiedlichen Lebenszyklen erfordern klare Verantwortlichkeiten darüber, wer wann welche Aufgaben zur Erhaltung der Cybersicherheit übernimmt. Nach Meinung der Teilnehmenden der Workshops ist diese Verantwortlichkeit oft nicht klar zugeordnet. Erschwerend kommen Geräte hinzu, welche von Nutzenden der Gebäude selbst mitgebracht werden. Typischerweise sind das Smartphones, mit welchen Informationen über das Gebäude oder die Wohnung abgefragt oder Einstellungen vorgenommen werden können. Weitere Geräte sind Sprachassistenten, Unterhaltungselektronik und weitere Gadgets. Je nach Konfiguration der Systeme im Gebäude können auch solche Geräte eine Schwachstelle darstellen, welche für Cyberangriffe genutzt werden können.

In den Workshops wurde zudem festgestellt, dass insbesondere bei den Anspruchsgruppen, welche Dienste rund um die Planung, Bau und Nutzung von Gebäuden anbieten, Fachkräfte mit Kenntnissen im Bereich Cybersicherheit fehlen. Das Argument des fehlenden Know-hows bezieht sich somit nicht nur auf die Nutzer*innen von Gebäuden, welche sich wegen unvollständigem Wissen unvorteilhaft verhalten. Es wird festgehalten, dass Know-how zur Cybersicherheit insbesondere in IT-nahen Berufen vorhanden ist, dieses jedoch in anderen für den Gebäudesektor relevanten Berufen fehlt.

3.2.4 Fazit

Die wichtigsten identifizierten Herausforderungen, für die Gewährung von Cybersicherheit im Gebäudebereich sind in Abbildung 8 zusammengefasst. Das Thema Cybersicherheit ist für eine Mehrheit ein wichtiges Thema und man ist sich bewusst, dass durch die Vernetzung Risiken entstehen und Cybersicherheit ein wichtiges Thema ist. Im Alltag spiegelt sich dieses Bewusstsein aber nicht im Verhalten wider. Der Umgang mit Daten und den eigenen Geräten ist oft unsorgfältig. Dennoch bestehen Misstrauen und Ängste in Bezug auf die Weitergabe von Daten.

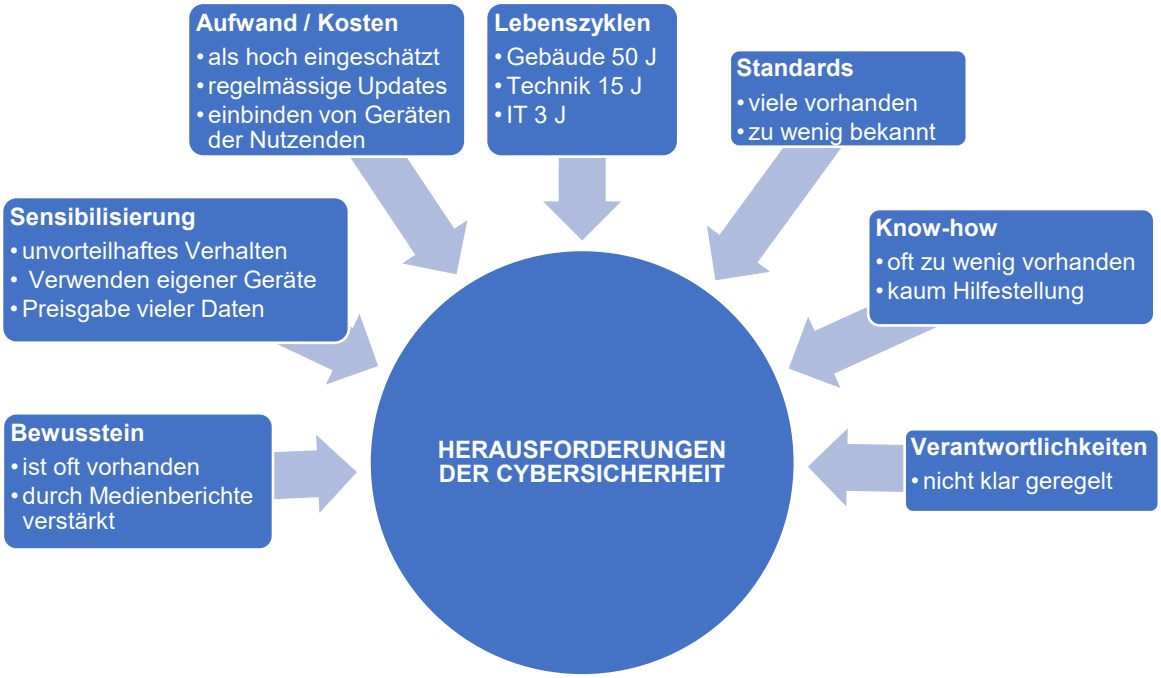


Abbildung 8: In Befragungen und Diskussionen sind einige Herausforderungen zum Thema Cybersicherheit identifiziert worden.

Es gibt Lösungsansätze, Technologien, Standards, Normen und Richtlinien, welche die Umsetzung von Massnahmen zur Gewährung der Cybersicherheit aufzeigen und ermöglichen (beispielsweise das NIST Cybersecurity Framework). Allerdings erschwert die Vielfalt der existierenden Dokumente den Durchblick und somit die Wahl der relevanten Standards, Lösungsansätze und Technologien. Zudem sind insbesondere Standards, Normen und Richtlinien oft zu wenig bekannt. Erschwert wird die Umsetzung von Massnahmen auch durch die unterschiedlichen Lebenszyklen der Technik in Gebäuden, was dazu führt, dass insbesondere IT-Komponenten oft ausgetauscht werden müssen und so durch möglicherweise entstehende Inkompatibilitäten zu Funktions- und Sicherheitseinschränkungen führen können. Ohne klar benennen zu können, welche Massnahmen wie umgesetzt werden müssen, werden Aufwand und Kosten zur Umsetzung von Massnahmen für die Cybersicherheit durch viele Personen in den Anspruchsgruppen als hoch wahrgenommen.

Den Anspruchsgruppen fehlen vor allem klar geregelte Verantwortlichkeiten und Hilfestellungen, um diese Herausforderungen anzugehen.

3.3 «IST-Zustand» Datenschutz

Datenschutz ist in Bezug auf die Digitalisierung ein wichtiges Thema. Welche Daten erfasst, gespeichert, weitergeleitet und verarbeitet werden, muss im Vorfeld definiert und auf die Einhaltung des Datenschutzes überprüft werden. Die von IoT-Geräten erfassten und analysierten Daten können Informationen über Verhaltensweisen von Individuen offenbaren. So können durch Temperatur- und Luftfeuchtigkeitsänderungen die An- und Abwesenheiten von Personen in Räumen nachgewiesen werden. Solche Datenauswertungen sind in Bezug auf Schutz der Privatsphäre nicht unbedenklich. Dieses Kapitel beleuchtet, wie das Thema Datenschutz insgesamt wahrgenommen wird.

3.3.1 Befragung

Die Befragung hat ergeben, dass 40% der Befragten Gebäudedaten in der Cloud und 60% lokal speichern (Abbildung 9). Insgesamt werten 70% der Befragten die Daten auch aus. Ein Drittel hat eine hohe Bereitschaft, die Daten Dritten für weitere Auswertungen zur Verfügung zu stellen, sofern sich daraus ein Vorteil ergibt. 85% denken, dass sich gegenüber heute aus den Daten durch weitere Auswertungen noch weitere Erkenntnisse gewinnen lassen können. 40% der Befragten würden die weiteren Auswertungen an Dritte auslagern. 75% aller Befragten denken, dass sie selbst mit den Datenschutzbestimmungen gut oder eher gut vertraut sind und diese auch einhalten. Bei der Umsetzung von Datenschutzmassnahmen erkennen 40% der Befragten fehlendes Know-how als Herausforderung. Für 30% ist eine fehlende Sensibilisierung das Problem, und 20% ordnen dem Thema Datenschutz keine Priorität zu.

In Bezug auf die Nutzung von Daten geben 55% der Befragten an, dass für Mitarbeitende in Büros ein Internetzugriff auf Informationen über das Gebäude, den Komfort oder die Funktionalität unwichtig oder eher unwichtig ist. Hingegen geben 60% der Befragten an, dass es für Mieter*innen von Wohnungen wichtig oder eher wichtig ist, via Internetzugriff auf Informationen über das Gebäude, den Komfort oder die Funktionalität zu erhalten. Für die Hälfte der Befragten ist der Bedarf an einer Sprachsteuerung im Gebäude tief.

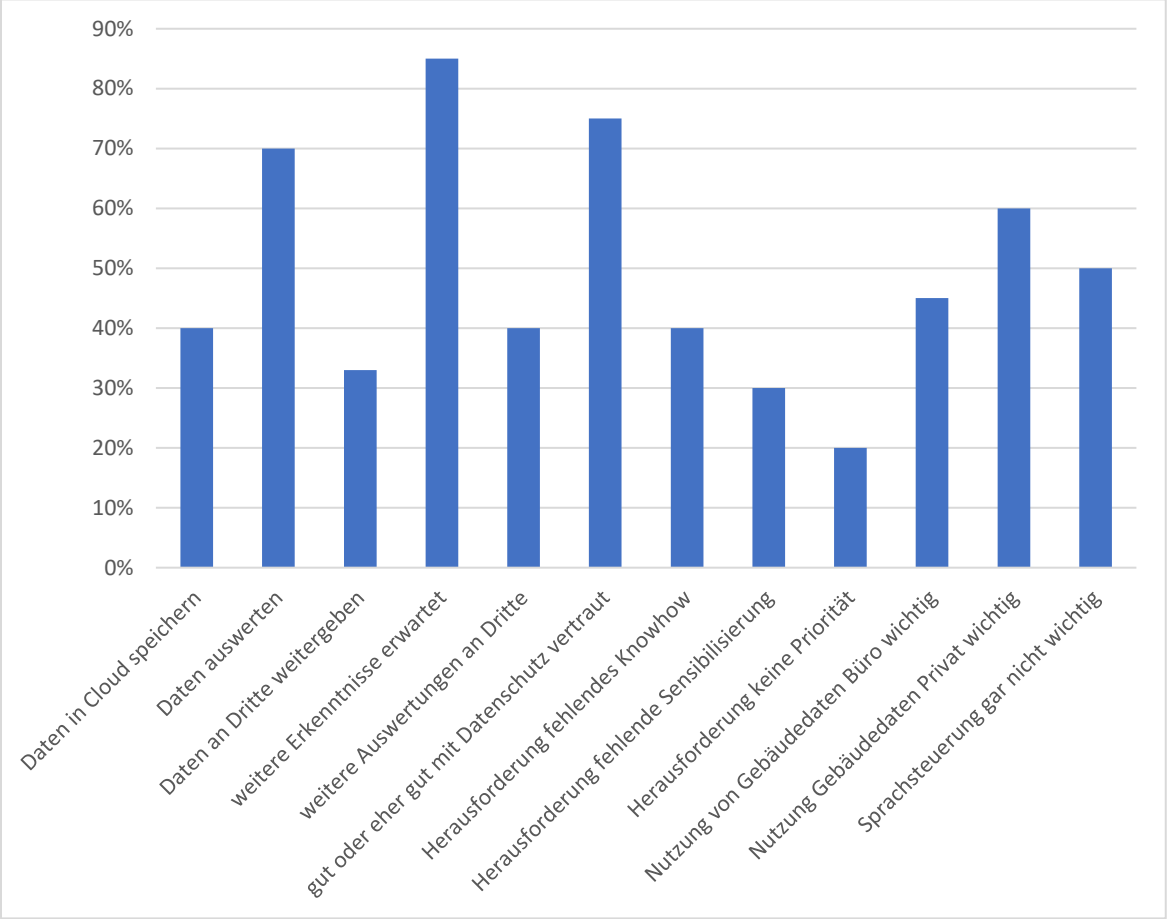


Abbildung 9: Die Ergebnisse der Befragung zum Thema Datenschutz

3.3.2 Standards und Gesetzgebung

Die im vorhergehenden Kapitel genannte Studie «Sicherheitsstandards für IoT-Geräte» umfasste auch Standards, welche in Bezug auf den Datenschutz relevant sind. Auch für den Datenschutz gilt, dass bereits viele Standards verfügbar sind. Die Schwierigkeit besteht wiederum darin, die für einen bestimmten Kontext relevanten Standards zu identifizieren.

Der Datenschutz ist zusätzlich durch die Gesetzgebung reguliert. Das aktuell in der Schweiz geltende Datenschutzgesetz datiert von 1992 und befindet sich derzeit in der Revision. Es ist geplant, das Gesetz per 1. September 2023 in Kraft zu setzen. Das neue Datenschutzgesetz berücksichtigt dabei die seit der letzten Revision einhergegangenen Veränderungen im Umgang mit Daten. Im Fokus stehen dabei Daten, welche durch die vermehrte Nutzung von Online-Diensten oder vernetzten Geräten entstehen. Im revidierten Gesetz werden die Rechte der Dateneigentümer verbessert, sie sollen die Hoheit über ihre eigenen Daten behalten. Die Anforderungen an die Datenbearbeiter steigen durch deren Eigenverantwortung in Bezug auf die Informationspflicht bei der Beschaffung von Personendaten sowie die Meldepflicht bei einem Verlust von Personendaten. Diese Massnahmen haben zum Ziel, mehr Transparenz zu schaffen. Der Schutz der persönlichen Daten soll durch die zur Verfügung stehende Technik weiter erhöht werden.

3.3.3 Resultate aus Workshops

In den Diskussionen in den Workshops wird der Digitalisierung von Planung, Bau und Betrieb der Gebäude ein hoher Stellenwert beigemessen. Der Datenschutz wird als natürliche Konsequenz davon und als notwendig wahrgenommen. Welche Daten gesammelt werden und was mit ihnen geschieht, muss im Vorfeld definiert und auf die Einhaltung des Datenschutzes überprüft werden. Der Datenschutz

muss in allen Phasen von datenbearbeitenden Prozessen berücksichtigt werden, also bei der Erfassung, Speicherung, Weiterleitung und Auswertung von Daten. Gegenstand des Datenschutzes sind die personenbezogenen Daten. Es müssen aber auch Daten berücksichtigt werden, aus denen auf eine Person zurückgeschlossen werden kann, auch wenn dies mit einem gewissen Aufwand verbunden ist.

Das Bewusstsein für das Thema Datenschutz ist vorhanden, u.a. auch durch Medienmeldungen, welche über Datenmissbrauch berichten. Die fehlende Sensibilisierung äussert sich in einem teilweise sorglosen Umgang mit Daten. Die Teilnehmenden des Workshops vermuten ein fehlendes Bewusstsein darüber, wie die Informationen aus der Datenanalyse verwendet werden können (z.B. kann aus der Analyse des Stromverbrauchs erkannt werden, welche Geräte in einem Haushalt vorhanden sind). Ausserdem ein fehlendes Bewusstsein darüber, dass die Analyse von Daten detaillierte Informationen über die Verhaltensweisen einzelner Personen liefern kann (z.B. kann die Analyse des Stromverbrauchs aufzeigen, wann die Kaffeemaschine benutzt wird).

Der sorglose Umgang mit Daten äussert sich oft darin, dass sehr persönliches preisgegeben wird, meist im Zusammenhang mit sozialen Medien. Das kann darauf hindeuten, dass man bei einem wahrgenommenen Nutzen auch bereit ist, Daten preiszugeben. Und dass der Nutzen durch die sozialen Medien als höher empfunden wird als in anderen Bereichen wie z.B. der Heimautomation. Im Zusammenhang mit dem Datenschutz kann der sorglose Umgang zu Missbrauch der persönlichen Daten führen. Im Zusammenhang mit der Cybersicherheit ist die Konsequenz des sorglosen Umgangs, dass Systeme leichter angegriffen werden können

Im Umgang mit Daten resp. daraus abgeleiteten Informationen müssen verschiedene rechtliche Aspekte berücksichtigt werden (Abbildung 10). So ist das Urheberrecht, also wem die Daten gehören, ein fundamentaler Baustein. Denn der Dateneigentümer muss letztlich seine Einwilligung geben, dass Daten überhaupt erhoben, gespeichert, weitergeleitet und weiterverarbeitet werden dürfen. Dies trifft auch auf Daten zu, welche in Gebäuden entstehen. Besonders bei personenbezogenen Daten muss dem Datenschutz eine hohe Wichtigkeit zuteilwerden. Wegen der hohen Schutzwürdigkeit von personenbezogenen Daten gelten die rechtlichen Vorgaben der Datenschutzgesetzgebung.

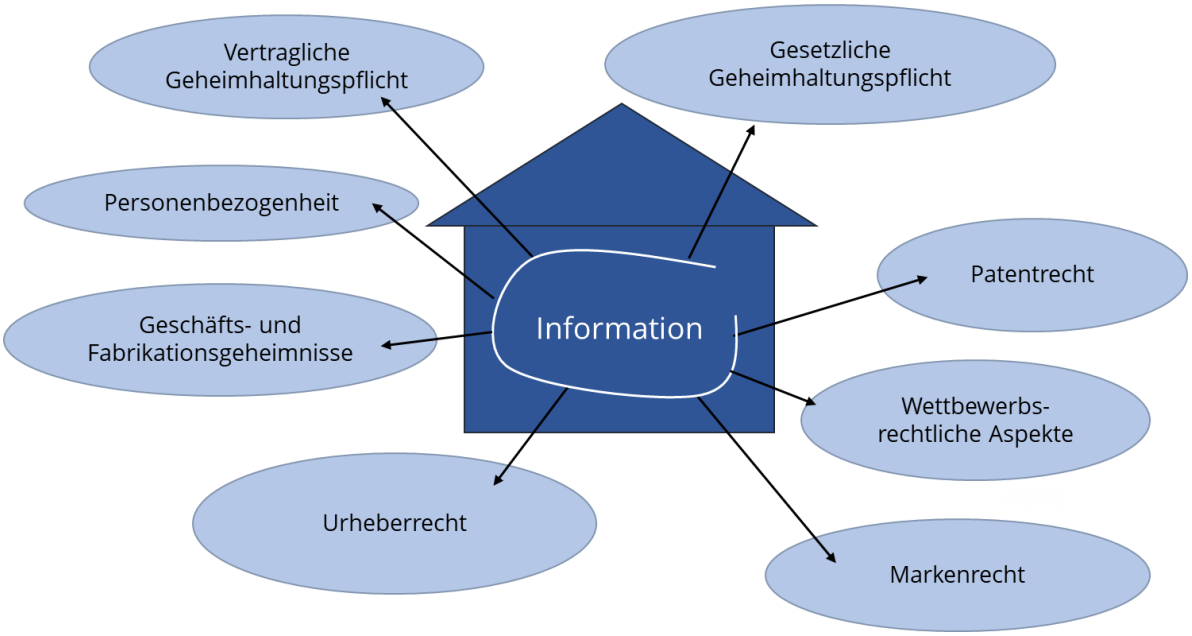


Abbildung 10: Im Umgang mit Daten und daraus gewonnenen Informationen sind einige rechtliche Aspekte zu berücksichtigen (Quelle: Ursula Sury, HSLU, Lit. 11)

Einig ist man sich in den Diskussionen, dass Daten für einen effizienten Betrieb von Gebäuden erfasst und verarbeitet werden müssen, auch personenbezogene Daten. Nicht in allen Anspruchsgruppen herrscht jedoch Klarheit darüber, welche Daten öffentlich oder welche nur beschränkt verfügbar sein sollen, oder welche Daten nicht genutzt werden dürfen. Auch ist nicht allen klar, wem die Daten gehören, wer dafür verantwortlich ist und wer die Daten einsehen, kopieren oder ändern darf.

Weitere Herausforderungen bestehen, ähnlich wie beim Thema Cybersicherheit, in einer Vielzahl an Lösungsansätzen, Standards, Normen und Richtlinien auch zum Thema Datenschutz. Für die

Anspruchsgruppen ist es anspruchsvoll, hier die relevanten Informationen zu finden. Auch die Kosten resp. der Aufwand, um Massnahmen zur Erreichung des gesetzlich geforderten Datenschutzes umzusetzen, werden als hoch bewertet. Diese Wahrnehmung entsteht, analog wie beim Thema Cybersicherheit, durch fehlendes Know-how und einer erwarteten hohen Komplexität der Massnahmen wie z.B. Einbau von zusätzlichen Systemen oder zusätzlicher Software und deren Unterhalt. Auch Prozesse, welche zur Einhaltung des Datenschutzes nötig werden könnten, werden als zusätzlicher Aufwand empfunden.

3.3.4 Fazit

Die wichtigsten identifizierten Herausforderungen, für die Gewährung des Datenschutzes im Gebäudebereich sind in Abbildung 11 zusammengefasst. Das Thema Datenschutz wird als wichtiges Thema wahrgenommen und wird grösstenteils auch korrekt umgesetzt. Trotzdem ist eine fehlende Sensibilisierung für den richtigen Umgang mit Daten im Alltag vorhanden.

Abbildung 11: In Befragungen und Diskussionen sind einige Herausforderungen zum Thema Cybersicherheit identifiziert worden.

Beim Datenschutz sind neben Standards, Normen und Richtlinien die Gesetzgebung zu berücksichtigen. Ein Ergebnis der Befragung ist, dass die Existenz des Datenschutzgesetzes bekannt ist, teilweise auch der Inhalt. Die Befragung und die Diskussionen in den Workshops haben ergeben, dass nicht allen Befragten klar ist, wie der Datenschutz umzusetzen ist. Unklar ist insbesondere, wie sich die Dateneigentümerschaft, die Datennutzung und die Gewährung des Zugriffs auf die Daten darauf auswirken, wie der Datenschutz bei Gebäudesystemen gewährleistet wird und welche Massnahmen umzusetzen sind. Wiederum sind viele relevante Standards bzgl. des Datenschutzes verfügbar, allerdings fehlt ein einfacher und niederschwelliger Zugang, welcher das Auffinden von relevanten Dokumenten erleichtern würde. Das Datenschutzgesetz ist aktuell in der Revision und stärkt die Rechte der Dateneigentümer. Das Gesetz regelt die Informations- und Meldepflicht bei der Beschaffung und dem Verlust von Daten. Die Inkraftsetzung ist per 1. September 2023 geplant.

Fehlendes Know-how führt dazu, dass die zur Erreichung des Datenschutzes erforderlichen Massnahmen nicht genau bekannt sind. Dadurch entsteht der Eindruck, dass der Aufwand und die Kosten für die Umsetzung der Massnahmen hoch seien.

3.4 «SOLL-Zustand» Interoperabilität

Das Bedürfnis nach über alle Gewerke hinweg integrierte Systeme wächst. Aus den Befragungen und den Diskussionen in den Workshops geht hervor, dass diese Integration als Mittel gesehen wird, um Ressourcen (insbesondere Energie) effizienter zu nutzen. Um dies zu erreichen, muss die Konnektivität

auf allen Ebenen der Interoperabilität verbessert oder ermöglicht werden. Auf der syntaktischen und strukturellen Ebene sollen die Schnittstellen zwischen den Systemen und den Gewerken technisch vereinheitlicht werden und auf standardisierten Funktionsbeschrieben und Anwendungsfällen basieren. Dies hat auch Auswirkungen auf die organisatorische und semantische Ebene, denn schon in der Planungsphase soll die Frage gestellt und beantwortet werden, wie eine gewerkeübergreifende Kommunikation gewährleistet werden kann. Und das so, dass die verbauten Systeme ohne grossen Integrationsaufwand im Zusammenspiel funktionieren und zu einem späteren Zeitpunkt während des Betriebs einfach erweitert, werden können. Auch der Ersatz von Komponenten muss bereits in der Planungsphase beachtet werden. Denn auch die Instandstellung trägt zu den Betriebskosten bei und diese sollten minimiert werden.

Neben den technischen Schnittstellen, sollten auch die Prozesse der Zusammenarbeit der verschiedenen Stakeholder verbessert werden. So soll in der Planungsphase die Planung der Gebäudeautomation nicht isoliert von Heizung, Lüftung, Beleuchtung oder Beschattung durchgeführt werden. Erst eine integrierte Herangehensweise ermöglicht die erforderliche Integration der verschiedenen Gewerke zu einem Gesamtsystem, welches Kosteneinsparungen durch weniger Ressourcenverbrauch ermöglicht. Zudem können Synergieeffekte genutzt werden, wenn beispielsweise auch die Verlegung von Leitungen und Rohren integral geplant werden. Eine weitere Dimension ergibt die Berücksichtigung der Lebenszyklen in die Planung. Nur wenn die Betriebskosten bereits bei der Planung Eingang finden, können diese auch reduziert werden.

Bereits in der Planungsphase müssen klar messbare Ziele formuliert werden, welche die Gebäude während der Betriebsphase z.B. in Bezug auf Energieverbrauch, Eigenverbrauch oder Autarkie erreichen müssen. Damit hängt auch zusammen, dass in der Planung bestimmt werden muss, welche Daten in welcher Form aufgezeichnet und ausgewertet werden müssen. Zudem muss die Verantwortlichkeit für Datenerfassung und Datenauswertung definiert werden. Die Planung soll bereits aufzeigen, wir auf die Datenauswertungen reagiert werden soll. Wer also beispielsweise Anpassungen am System vornimmt, wenn die Zielwerte nicht erreicht werden.

Die Planung, also auch die Festlegung der Ziele, muss die Bedürfnisse aller an der Nutzung der Gebäude Beteiligten (Mieter, Vermieter, Eigentümer, Verwaltung, Facility Management, usw.) berücksichtigen. Diese sind ins Zentrum der Überlegungen zu stellen (Nutzerzentrierung). Nur so kann gewährleistet werden, dass die Ziele auf den Nutzen ausgerichtet sind, welcher von den an der Nutzung Beteiligten erwartet wird.

Allerdings sind die Interessen dieser Anspruchsgruppen nicht immer deckungsgleich. So haben Mieter*innen z.B. den Anspruch auf möglichst viel Komfort, die Betreibenden legen Wert auf möglichst tiefe Kosten. Solche potenziellen Konflikte müssen frühzeitig, optimalerweise bereits in der Planungsphase, erkannt werden, um dann möglichst früh Kompromisse finden zu können.

Unterstützend können Standards, Normen und Richtlinien wirken. Auch Allianzen oder Initiativen können die interdisziplinäre Zusammenarbeit über die Phasen des Lebenszyklus von Gebäuden fördern. Dazu müssen die relevanten Standards, Normen oder Richtlinien, aber auch Allianzen oder Initiativen bekannt sein. Hier können Leitfäden helfen, welche für verschiedene Anwendungsfälle im Zusammenhang mit der Planung, der Erstellung und dem Betrieb von Gebäuden konkrete Hinweise geben. Leitfäden sollen neben Verweisen zu Standards, Normen, Richtlinien, Allianzen oder Initiativen auch Handlungsanweisungen enthalten. Die Leitfäden werden laufend aktualisiert, so dass sie neuste technologische Entwicklungen berücksichtigen können.

Der Soll-Zustand zielt also darauf ab, dass die interdisziplinäre Zusammenarbeit verbessert und ausgebaut wird. Dazu sind Fachkräfte erforderlich, welche die Kompetenzen für die Interdisziplinarität mitbringen und die Zusammenarbeit über Branchengrenzen hinweg umsetzen können. Es liegt allerdings auch an den Bestellenden, entsprechende Leistungen einzufordern (Abbildung 12). Dies sind die wesentlichen Handlungsfelder für den Soll-Zustand.

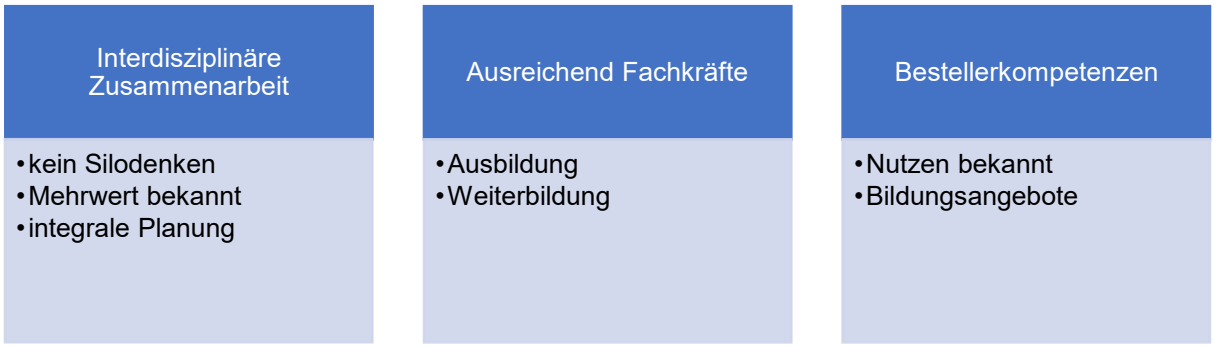


Abbildung 12: Die Handlungsfelder Interdisziplinäre Zusammenarbeit, ausreichend Fachkräfte, Bestellerkompetenz für den Soll-Zustand

3.4.1 Interdisziplinäre Zusammenarbeit

Eine der Hauptanforderungen bezüglich der Konnektivität im Gebäude ist die bisher isoliert verwendeten oder nicht erhobenen Daten miteinander zu verknüpfen. So wird beispielsweise in der Planung schon länger auf die Verwendung räumlicher Daten durch digitale Modelle wie CAD zurückgegriffen. Neu sollen jedoch auch noch die digitalen Modelle verschiedener Gewerke sowie die Verknüpfung von digitalen Modellen mit physischen Geräten oder Infrastrukturen erfolgen. Ein intelligentes Gebäude soll die Daten der verschiedenen Gewerke zentral verfügbar und nutzbar machen. Dies bedeutet, dass eine Vernetzung der einzelnen Systeme gegeben sein muss. Auch der Zugang zu den aktuellen Daten soll zentral erfolgen inkl. der Möglichkeit direkt Einfluss auf diese Daten nehmen zu können. Die Prozesse im Unterhalt und der Bewirtschaftung sollen hoch automatisiert sein, damit sich die Gebäude vorausschauend und selbständig an neue Situationen anpassen. Die Gebäude sollen ebenfalls direkt und selbständig vom Benutzerverhalten lernen und entsprechend agieren können. So soll die Energieeffizienz von Gebäuden verbessert werden, wobei der Komfort mindestens gehalten, optimalerweise sogar gesteigert werden soll.

Durch eine integrale Planung (s. 3.1.3) könnte eine bessere und transparentere Planung gewährleistet werden, welche während der Planungsphase bereits Entscheidungsgrundlagen für den Gebäudebetrieb ermöglicht. Eine derartige Planung wäre zukunftsgerichteter und unterstützt die gewerkeübergreifende Vernetzung von Technologien. Simulationen und Prognosen für die Bewirtschaftung der Gebäude in der Planungsphase verbessern die Planungsergebnisse dahingehend, dass der Betrieb effizienter wird. Und sie führen zusätzlich zu weniger Fehlfunktionen im späteren Betrieb und sich daraus ergebenden Mehrkosten.

Der Entscheid, welche Informationen verwendet werden, soll daher schon in der Planungsphase geschehen. Dabei spielt vor allem die semantische und syntaktische Ebene der Interoperabilität eine wichtige Rolle, d.h. die Beschreibung der Informationen wie beispielsweise Wertebereiche von Parametern und oder deren Bedeutung während der Nutzung. Nur so können daraus später die entsprechenden Informationen abgeleitet und eine systemübergreifende Funktionalität sichergestellt werden. Dies entspricht der strukturellen Ebene der Interoperabilität. Auf der organisatorischen Ebene dann sind die digitalen Technologien von allen Beteiligten gemeinsam zu adressieren. In der Umsetzung sollte das Ziel sein, die Komplexität so stark mit möglich zu reduzieren. Eine durchgehende Datenaufnahme und –analyse führt zu einem kosteneffizienteren Betrieb und verbessert die Energieeffizienz der Gebäude. Common Data Modelle vereinfachen die Kommunikation zwischen den Gewerken und sollen daher zur Anwendung kommen. Weiter soll die Anzahl der Standards eher reduziert als immer weiter erhöht werden. Weniger Standards führen auch zu geringeren Abstimmungs- und Integrationsaufwände. Da die Anzahl Standards kaum aus diesem Projekt heraus beeinflusst werden kann, soll die Problematik über Leitfäden angegangen werden, welche für die Planenden die relevanten Standards so aufbereiten, dass sie einfach zugänglich und umsetzbar sind.

3.4.2 Ausreichend Fachkräfte und Bestellerkompetenz

Die Bestellerkompetenz in der Bestellung und Planung benötigt vermehrt Aufmerksamkeit und soll langfristig verbessert werden. Durch neue digitale Technologien und der Zunahme der Datenmenge auch im Gebäude, muss die Digitalisierungskompetenz in den Fachbereichen erhöht und die Mitarbeitenden sollten zukunftsgerichtet entwickelt werden. Aktuelle Berufe werden sich weiterentwickeln oder wegfallen und neue Berufe werden entstehen. Erfolgt keine gezielte Mitarbeiterentwicklung muss notwendiges Know-how von extern eingekauft werden. Allerdings herrscht auf dem Arbeitsmarkt bereits jetzt ein Mangel an spezialisierten Fachkräften für diese Thematiken.

3.5 «SOLL-Zustand» Cybersicherheit und Datenschutz

Da die Themen Cybersicherheit und Datenschutz viele gemeinsame Herausforderungen besitzen, wird der Soll-Zustand für beide gemeinsam abgehandelt. Der Soll-Zustand wurde gemeinsam mit den Teilnehmenden der Workshops erarbeitet. Als relevante Handlungsfelder haben die Teilnehmenden das sichere Verhalten aller beteiligten Anspruchsgruppen, ausreichend Fachkräfte sowie sichere Produkte und Systeme identifiziert (Abbildung 13).

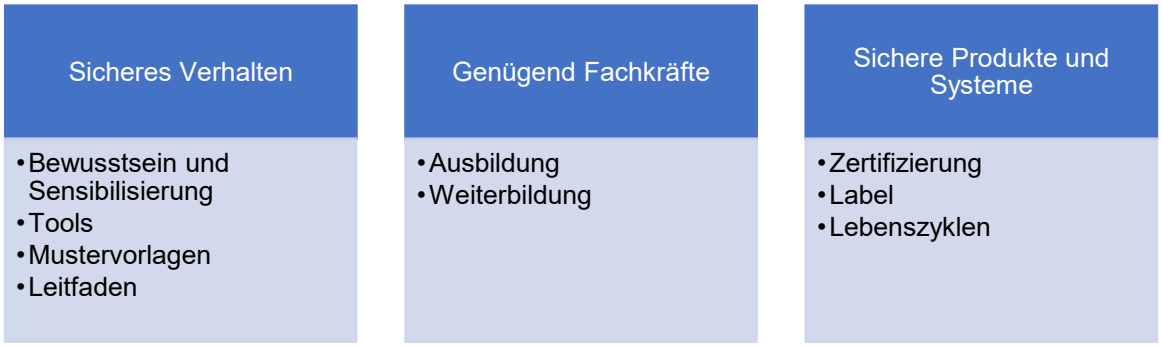


Abbildung 13: Die Handlungsfelder Sicheres Verhalten, genügend Fachkräfte und sichere Produkte für den Soll-Zustand

3.5.1 Sicheres Verhalten aller Beteiligten

Um die Cybersicherheit zu gewährleisten, müssen sich alle an Planung, Bau, Betrieb und Nutzung von Gebäuden beteiligten Anspruchsgruppen entsprechend verhalten. Dies setzt voraus, dass sie sich den Risiken bewusst und auch genügend sensibilisiert sind, die erforderlichen Sicherheitsstandards einzuhalten. Sicherheitsstandards beziehen sich auf die Nutzung von starken Sicherheitselementen wie Passwörter, Verschlüsselung und die Verwendung von sicheren Produkten. Je nachdem aus welcher Anspruchsgruppe die Personen kommen, sind auch Kenntnisse über relevante Standards, Normen und Richtlinien erforderlich.

a) Sensibilisierung

Diese Personen darüber zu informieren, dass solche Standards, Normen und Richtlinien vorhanden sind, muss wegen der Vielfalt der Anspruchsgruppen auf verschiedenen Kanälen erfolgen. So können Planer*innen, Betreiber*innen und Hersteller*innen über Fachmedien oder auch über die Aus- und Weiterbildung erreicht werden. Wohingegen Besitzer*innen oder Mieter*innen eher über Massenmedien und Soziale Medien aber auch über Aus- und Weiterbildung anzusprechen sind. Dazu müssen entsprechende Beiträge zum Thema Informationssicherheit und Datenschutz[3] produziert und publiziert werden. Die Beiträge sollen zielgruppengerechte Inhalte aufweisen und auf den für die Zielgruppe geeigneten Kanälen veröffentlicht werden. Die Beiträge sollen Fachleute eher über Fachmedien sowie Aus- und Weiterbildung mit Informationen zu Massnahmen, Standards und Richtlinien erreichen, Besitzer*innen und Mieter*innen über Massen- und soziale Medien. Für Fachleute könnten die Beiträge eher auf Massnahmen und Standards ausgerichtet sein, während für Besitzer*innen und Mieter*innen eher die Sensibilisierung und Verhaltensregeln im Fokus stehen. Eine mögliche Zuordnung zeigt Abbildung 14.

[3] Stellvertretend für Cybersicherheit und Datenschutz

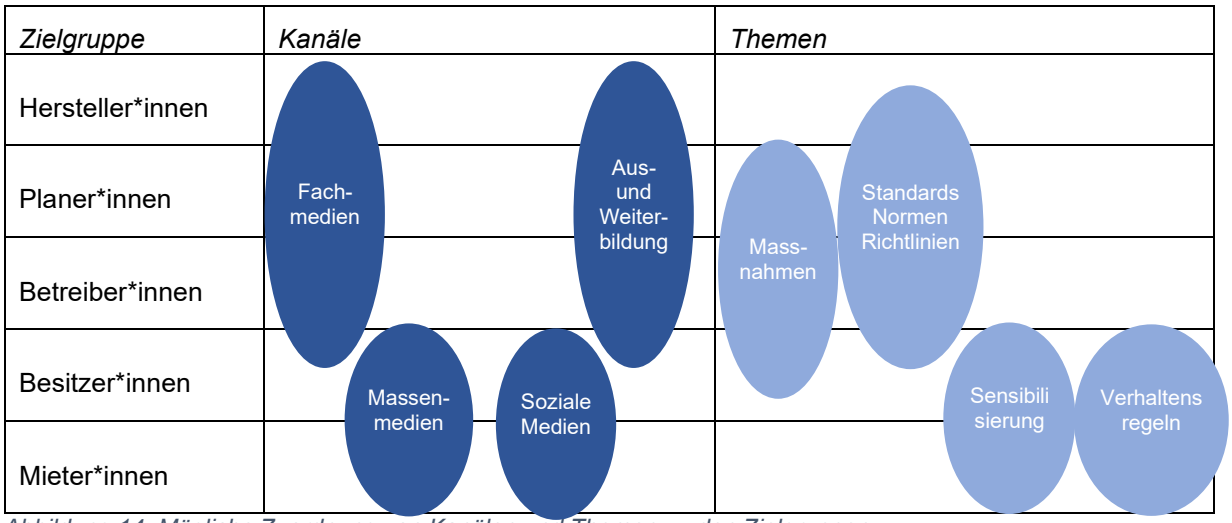


Abbildung 14: Mögliche Zuordnung von Kanälen und Themen zu den Zielgruppen

b) Unterstützung durch digitales Tool

Ein sicheres Verhalten aller Personen soll mit Hilfestellungen unterstützt werden. Für konkrete Fragestellungen im spezifischen Kontext der Anspruchsgruppe, sollen die Personen auf ihre Bedürfnisse zugeschnittene Informationen bekommen, welche sie bei der Definition oder Umsetzung von Massnahmen zur Cybersicherheit und zum Datenschutz unterstützen. Die Hilfestellungen ermöglichen einen effizienten Umgang mit den Herausforderungen der Cybersicherheit und des Datenschutzes und leiten die Beteiligten an.

Eine solche Hilfestellung stellt ein digitales Tool dar, welches Standards, Normen und Richtlinien, aber auch Checklisten oder Mustervorlagen auf eine Problemstellung zugeschnitten zur Verfügung stellt. Durch eine geschickte Benutzerführung soll es den Nutzenden möglichst einfach gemacht werden, die relevanten Informationen zu finden. Das Tool soll sich nicht auf die genannten Dokumente beschränken, sondern auch Hinweise auf aktuelle Risikosituationen geben und aufzeigen, wie man sich gegen diese Risiken schützen kann.

Um den Kontext zu erfassen, in welchem Informationen gesucht werden, können Nutzende Angaben zu Anspruchsgruppen, Art der gesuchten Information, Gebäudeart und Anwendung erfassen. Als Anspruchsgruppen sind Entwickler*innen und Hersteller*innen von Produkten und Dienstleistungen, Integratoren*innen, Betreiber*innen und Verwalter*innen von Gebäuden, Eigentümer*innen, Mieter*innen, IT-Experten*innen in den Organisationen sowie Behörden zu berücksichtigen. Die Art der gesuchten Information zielt auf managementorientierte oder technische Informationen ab. Ein weiteres Kriterium ist die Gebäudeart: öffentliche Gebäude, öffentliche Infrastrukturen, kritischen Infrastrukturen, Schulgebäude, Industriegebäude, Büro- und Verwaltungsgebäude und medizinische Einrichtungen. Auch die Anwendung entscheidet darüber, welche Information relevant ist. Unterschieden werden können Informationen zur Sicherheit, Netzwerkarchitektur, zu Updates, Anlagen und Maschinen, Smart Home sowie Industrielle Kontrollsysteme, aber auch allgemeine Tipps (Abbildung 15).

- Anspruchsgruppe
- Art der Information
- Art des Gebäudes
- Anwendung

Abbildung 15: Kriterien, nach denen Standards, Normen und Richtlinien zu Cybersicherheit und Datenschutz klassiert werden können

Ergänzend zu Standards, Normen und Richtlinien, sollen auch Mustervorlagen verfügbar sein. Insbesondere für Immobilienbetreibende oder Verwaltungen stellt eine Cyber-Hausordnung, welche das Thema Cybersicherheit abdeckt, ein wichtiges Instrument dar. Damit können sie den Wohnungseigentümern*innen oder Mieter*innen Hilfestellungen anbieten, welche den Einsatz von mit dem Internet verbundenen Geräten regelt. Dies betrifft vor allem gemeinsam genutzte Infrastruktur. Die Cyber-Hausordnung enthält Hinweise zum Verhalten und zur Technik in Bezug auf Cybersicherheit.

Eine Mustervorlage soll eine Hilfestellung beim Erstellen von Cyber-Hausordnungen bieten, indem Massnahmen oder Verhaltensregeln vorgeschlagen werden. Die Cyber-Hausordnung soll nicht statisch sein, sondern basierend auf den spezifischen Bedürfnissen und auf die spezifische Situation passend erstellt werden.

c) Leitfaden

Ein Leitfaden ermöglicht durch Vermittlung von Know-how und Anleitungen die Sicherheit im Umgang mit Daten zu erhöhen. Ein Leitfaden soll für spezifische Problemstellungen verschiedener Anspruchsgruppen konkrete Empfehlungen und Handlungsanweisungen geben. In Kapitel 6.2 ist detaillierter beschrieben, welche Inhalte ein Leitfaden enthalten soll.

3.5.2 Ausreichend Fachkräfte

Um ausreichend Fachkräfte im Bereich der Planung, dem Bau und dem Betrieb von Gebäuden aufzubauen, welche über Fachwissen zu Cybersicherheit und Datenschutz verfügen, ist bei der Aus- und Weiterbildung anzusetzen. Ausbildungskonzepte definieren die Anforderungen an die Curriculi der Studiengänge und Lehrgänge in verschiedenen Branchen rund ums Gebäude. Die Anforderungen berücksichtigen die relevanten Themen zu Cybersicherheit und Datenschutz, welche in die bestehenden Angebote zu integrieren (z.B. Immobilienbetreiber*innen mit IT-Kenntnissen / Integratoren*innen / Gebäudeinformatiker*innen). Je nach Bedarf sollen Aus- und Weiterbildungsangebote ausgebaut und klare Job-Profile definiert werden. Zudem definiert das Ausbildungskonzept die Kompetenzen, welche die Lernenden und Studierenden erlangen sollen (Abbildung 16).

Aus- und Weiterbildung stellt eine weitere, wichtige Form der Sensibilisierung dar. Über diesen Weg ist es einfach möglich, sehr gezielt die Herausforderungen aus Cybersicherheit und Datenschutz dem Zielpublikum näherzubringen. Insbesondere erfahren die Lernenden und Studierenden auf diesem Weg branchenspezifisch, welche Herausforderungen wie anzugehen sind.

Während es in der Weiterbildung bereits einige Angebote gibt, sollen Cybersicherheit und Datenschutz verstärkt in der Ausbildung thematisiert werden. Dazu sind Aktivitäten zu starten, um die Verantwortlichen von Studiengängen oder Ausbildungslehrgängen im Aufbau von entsprechenden Ausbildungseinheiten zu unterstützen.

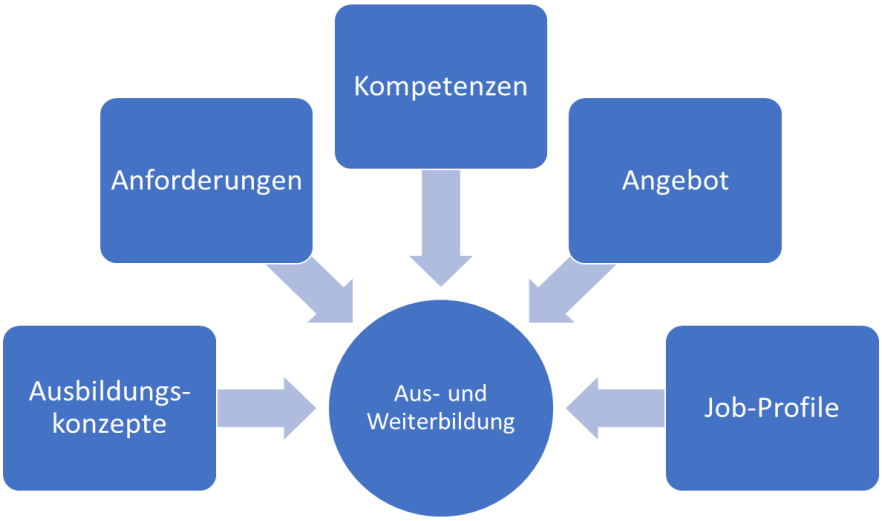


Abbildung 16: Die Aus- und Weiterbildung in allen Branchen rund ums Gebäude müssen die Themen Cybersicherheit und Datenschutz aufnehmen

3.5.3 Sichere Produkte und Systeme

Ein weiteres Element zur Gewährleistung von Cybersicherheit und Datenschutz sind sichere Produkte, Systeme und Dienstleistungen (im Folgenden Produkte genannt). Die Verantwortung dafür liegt bei den Herstellenden. Labels können den Kund*innen sichtbar machen, welche Produkte sicher sind. Solche Labels können eine Aussage darüber machen, dass die für das jeweilige Produkt erforderlichen Standards, Normen und Richtlinien eingehalten werden, ohne dass die Kund*innen diese im Detail kennen müssen.

Als Produkt im Sinne eines Labels kann auch ein Gebäude gelten. Es ist deshalb die Vergabe eines Labels für Gebäude und somit eine Zertifizierung für Gebäude zu prüfen. Um die Zertifizierung zu erlangen, stehen Vorgaben und Checklisten für eine Auditierung zur Verfügung, welche die Cybersicherheit und den Datenschutz abdecken.

Ein wichtiger Punkt, welcher die Zertifizierung berücksichtigen soll, sind die unterschiedlichen Lebenszyklen der im Gebäude enthaltenen Komponenten und die daraus möglicherweise entstehenden Sicherheitsprobleme. Diese können entschärft werden, wenn einerseits veraltete Komponenten durch kompatible, sichere Komponenten ersetzt werden und andererseits das gesamte System nach dem Austausch rezertifiziert wird. Die Rezertifizierung soll integrierter Bestandteil der Vorgaben für die Zertifizierung von Gebäuden sein.

Um die Zertifizierung von Gebäuden hinsichtlich Cybersicherheit und Datenschutz zu erleichtern, soll auf zertifizierte resp. mit einem Label versehene Produkte zurückgegriffen werden können (Abbildung 17). Ein solches Label würde den Produkten attestieren, dass sie sicher sind und die entsprechenden Vorgaben aus den Standards und Normen erfüllen. Wünschenswert ist ein international gültiges Label, z.B. analog zur CE-Kennzeichnung von Produkten. Ein solches würde sicherstellen, dass die für das jeweilige Produkt gültigen Gesetze, Standards und Normen eingehalten sind.

Abbildung 17: Mit Zertifizierungen und Kennzeichnungen sollen Produkte und Systeme als sicher hinsichtlich Cybersicherheit und Datenschutz erkannt werden können.

4 Beschreibung und Resultate aus der GAP-Analyse

In der Gap-Analyse wird der Ist- mit dem Soll-Zustand aus Kapitel 3 verglichen. Daraus wird abgeleitet, wo die wichtigsten Lücken zwischen der gewünschten Situation und der aktuellen Lage sind und entsprechend ein Handlungsbedarf besteht. Die sich aus der GAP-Analyse abzuleitende Massnahmen werden anschliessend im Kapitel 5 beschrieben.

4.1 Interoperabilität

Im Bereich Interoperabilität haben wir den Soll-Zustand in den drei Themen *Interdisziplinäre Zusammenarbeit*, *Ausreichend Fachkräfte* und *Bestellerkompetenz* beschrieben. In diesen Themen sind jeweils einige Lücken festzustellen und deshalb Massnahmen notwendig.

4.1.1 Interdisziplinäre Zusammenarbeit

Die interdisziplinäre Zusammenarbeit beinhaltet viele Themen und muss kontinuierlich überprüft und angepasst werden damit alle betroffenen Bereiche optimal ineinandergreifen und somit einen Mehrwert generieren. Damit die Dekarbonisierung vorangetrieben werden kann, müssen vorhandene und kommende Technologien richtig eingesetzt und genutzt werden. Beim Einsatz der Technologien ist auch wichtig, dass versucht wird, die Komplexität so stark wie mögliche zu reduzieren und nicht zu erhöhen, da sonst die Akzeptanz fehlt und entsprechend kommende Technologien nicht eingesetzt werden. Um gezielte Optimierungen vorzunehmen, bedarf es einer klaren Vorgehensweise. Durch Sensibilisierung kann das Bewusstsein auf dieser Ebene gestärkt und Strategien angepasst werden.

Aus der Ist- und Soll-Analyse geht hervor, dass eine gesamtheitliche Denkweise bei vielen Beteiligten immer noch fehlt. Ein Gebäude wird nicht über seinen kompletten Lebenszyklus hinweg beurteilt und betrachtet. Vorhandenes Wissen muss geteilt werden, um so gemeinsam einen Mehrwert für die Nutzenden zu schaffen. Das vorhandene Silodenken mit einer starken Fokussierung auf die Vermarktung der eigenen Kompetenzen, Produkte und Dienstleistungen muss zugunsten einer vernetzten Denkweise aufgebrochen werden. Dies müssen die verschiedenen Gewerke im Gebäude ebenso berücksichtigen wie die Phasen Planung, Erstellung, Nutzung bis hin zum Rückbau. Es gibt noch kaum oder zu wenig regulatorischen Druck oder Anreizsysteme, welche einen positiven Effekt auf die Nachhaltigkeit und der Immobilen Branche haben könnten. Anreizsysteme wie beispielsweise das Gebäudeprogramm basieren auf Freiwilligkeit, können jedoch einen Ansatz darstellen, um diese Thematik anzugehen.

4.1.2 Ausreichend Fachkräfte und Bestellerkompetenz

Die interdisziplinäre Zusammenarbeit muss aus mehreren Gründen gestärkt werden. Einerseits soll eine gewerkeübergreifende Zusammenarbeit den Endnutzen steigern und den Energieverbrauch reduzieren als auch den Werterhalt eines Gebäudes sichern. Dies wiederum sichert die Rendite von Gebäudeinvestoren. Fehlende Bestellerkompetenz auf Seiten der Bestellenden und fehlendes Know-how bei wichtigen Stakeholdern, wie beispielsweise Investoren oder Mitarbeitenden, sollen gezielt durch Aus- und Weiterbildungsangebote verbessert werden. Die Aus- und Weiterbildung in allen Branchen rund um das Gebäude berücksichtigt die Themen Interoperabilität noch zu wenig, welche den Lernenden und Studierenden die Kompetenzen vermitteln, mit den Herausforderungen der Interoperabilität umzugehen. Hinderlich zur Erreichung des Soll-Zustands können die Bedenken der hohen oder zunehmenden Komplexität wirken, welche einerseits durch die Interdisziplinarität über die Gewerke und Phasen entstehen kann (organisatorische Ebene der Interoperabilität). Andererseits sorgt auf den anderen Ebenen der Interoperabilität die Vielzahl an Standards oder Protokollen, welche bei der Integration der Teilsysteme zum Gesamtsystem zum Einsatz kommen, für Überforderung. Diese Aspekte werden bei der Aus- und Weiterbildung noch zu wenig berücksichtigt

4.2 Cybersicherheit und Datenschutz

Der Soll-Zustand im Bereich Cybersicherheit und Datenschutz umfasst die Handlungsfelder *Sicheres Verhalten*, *Ausreichend Fachkräfte* und *Sichere Produkte und Systeme*. In diesen Feldern sind jeweils einige Lücken festzustellen und deshalb Massnahmen notwendig.

4.2.1 Sicheres Verhalten

Dieser Abschnitt beschreibt die Lücken zum Thema *Sicheres Verhalten*. Zur Sprache kommt das problematische Verhalten vieler Nutzenden, der Umstand, dass Standards zu wenig bekannt sind und

dass fehlendes Know-how und hoher Aufwand zur Umsetzung von Massnahmen als Herausforderung gesehen werden (Abbildung 18).

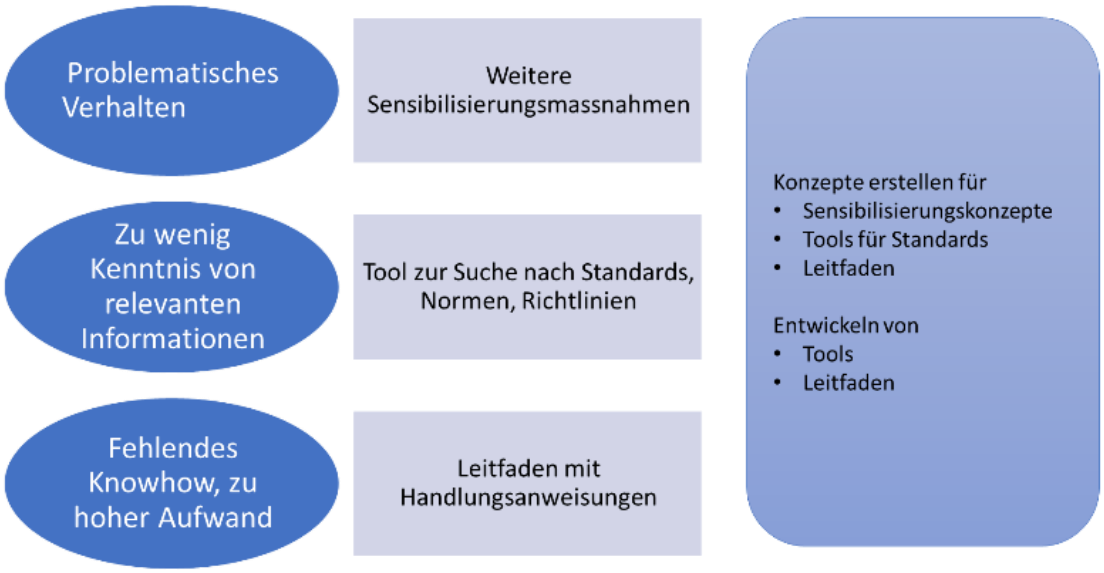


Abbildung 18: Um die Lücken zum Sicheren Verhalten zu schliessen, sind Konzepte für Sensibilisierungsmassnahmen, Tools und Leitfäden zu erstellen. Die Sensibilisierungsmassnahmen, Tools und Leitfäden sind auch zu entwickeln und umzusetzen.

In Bezug auf das sichere Verhalten kann festgestellt werden, dass die Personen der Anspruchsgruppen rund um Erstellung, Bau, Betrieb und Nutzung von Gebäuden sich der Probleme im Bereich Cybersicherheit und Datenschutz durchaus bewusst sind. Trotzdem verhalten sie sich zumindest teilweise problematisch: sie missachten einfache Verhaltensregeln für den sicheren Betrieb von verbundenen Geräten und gehen mit Daten wenig sorgsam um. Das kann zu unsicheren, d.h. leicht angreifbaren Systemen sowie Datenmissbrauch führen. Mit zielgruppengerechten Sensibilisierungsmassnahmen soll dieser Problematik begegnet werden. Die Sensibilisierungsmassnahmen sollen nicht nur die Probleme adressieren und die Risiken durch Cyberangriffe oder Datenmissbrauch aufzeigen, sondern auch Verhaltensregeln aufzeigen, wie die Risiken reduziert werden können. Zudem soll auch der Nutzen für die jeweilige Zielgruppe aufgezeigt werden, wenn das Verhalten dem Risiko entsprechend angepasst wird. Solche Sensibilisierungsmassnahmen, welche zusätzlich auf die Wichtigkeit der Themen Cybersicherheit und Datenschutz hinweisen sollen, bestehen noch zu wenig oder sind zu wenig auf die Zielgruppen ausgerichtet (z.B. Medienberichte über erfolgte Cyberangriffe). Um effektive Sensibilisierungsmassnahmen zu erstellen, sind entsprechende Konzepte zu entwickeln. Die Konzepte müssen zwingend die Zielgruppe definieren und Formate beschreiben, welche auf die Zielgruppen ausgerichtet sind.

Im Bereich der Standards, Normen und Richtlinien ist das Ziel, ein Tool zur Selektion der relevanten Dokumente bereitzustellen. Mit diesem Tool sollen die Vertreter*innen aus den Anspruchsgruppen die für ihre Problemstellung und ihren Kontext relevanten Dokumente aufgelistet bekommen. Dadurch kann man sich im Kontext der eigenen Problemstellung schnell einen Überblick verschaffen und sich auf die Dokumente fokussieren, welche wichtig sind. Der Kontext umfasst u.a. die Rolle (z.B. Planer*in, Betreiber*in, Nutzer*in), die Art des Gebäudes oder die Art der Geräte, die zum Einsatz kommen sollen. Für das Tool besteht bereits ein Prototyp und ein erster Entwurf von Anwendungsfällen und Anforderungen. Um das Tool fertigzustellen, müssen weitere Anforderungen und Anwendungsfälle aufgenommen und in den Prototyp integriert werden. Zusätzlich fehlt aktuell noch ein Konzept für die Inbetriebnahme, den Betrieb und den Unterhalt.

Um dem fehlenden Know-how oder dem befürchteten hohen Aufwand zur Umsetzung von Massnahmen zur Minderung von Cybersicherheitsrisiken resp. Gewährung des Datenschutzes zu begegnen, sollen Leitfäden mit Handlungsanweisungen zur Verfügung stehen. Bereits existierende Leitfäden sind zu wenig oder nicht bekannt (analog zu den Standards, Normen und Richtlinien), für viele spezifische Problemstellungen im Umfeld von Gebäuden fehlen. Die Leitfäden müssen erstellt werden, wobei vorgängig definiert werden muss, für welche Problemstellungen dies zu erfolgen hat. So sind die zu berücksichtigenden Prozesse zu definieren, und für welche Personen resp. Personengruppen der Leitfaden relevant ist.

4.2.2 Ausreichend Fachkräfte

Es stehen zu wenige Fachkräfte mit Kenntnissen zu Cybersicherheit und Datenschutz zur Verfügung (Abbildung 19). Dies betrifft vor allem Branchen, welche aus der Vergangenheit wenig oder nichts mit Themen der IT zu tun hatten. Erst mit dem Aufkommen vernetzter Systeme ist z.B. auch eine Gebäudeplanerin oder ein Immobilienbetreiber mit Fragen konfrontiert, welche in IT-nahen Branchen längst üblich sind. Die Aus- und Weiterbildung in allen Branchen rund um das Gebäude sollen deshalb die Themen Cybersicherheit und Datenschutz zusätzlich umfassen und den Lernenden und Studierenden die Kompetenzen vermitteln, mit den Herausforderungen aus Cybersicherheit und Datenschutz umzugehen.

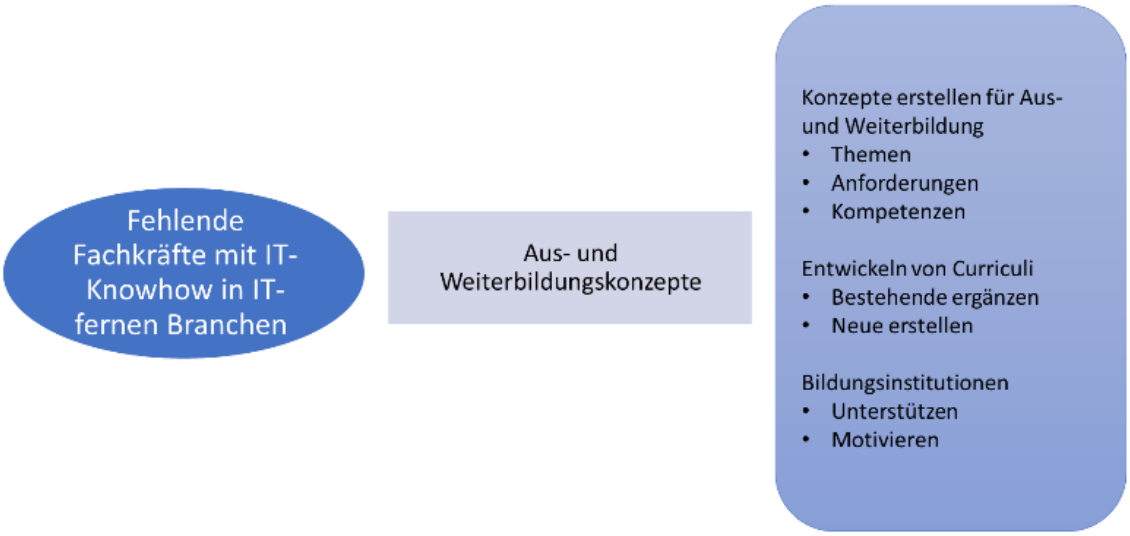


Abbildung 19: Um dem Problem der fehlenden Fachkräfte entgegenzuwirken, sind Konzepte und Curriculi für die Aus- und Weiterbildung zu erstellen. Bildungsinstitutionen sind zu motivieren und zu unterstützen.

Dazu fehlen vielfach noch Konzepte, welche die zu vermittelnde Themen identifizieren. Die Konzepte für Lehr- und Studiengänge sollen Anforderungen an die Ausbildung definieren und die Kompetenzen beschreiben, welche Absolvierende erlangen sollen. Auf Basis der Konzepte können die Bildungsinstitutionen die Curriculi der Lehr- und Studiengänge ergänzen oder neue erstellen. Ziel soll sein, dass das Angebot der Bildungsinstitutionen um das Thema Cybersicherheit und Datenschutz erweitert wird. Neben den Konzepten sind Massnahmen zu planen, welche die Verantwortlichen der Bildungsinstitutionen motivieren und fachlich unterstützen, das Angebot entsprechend zu erweitern.

Während die Themen Cybersicherheit und Datenschutz in IT-nahen Branchen längst im Bildungsangebot enthalten sind, fehlt die Sensibilisierung und der Kompetenzaufbau in IT-fernen Branchen. Mittels Aus- und Weiterbildung in IT-fernen Branchen können eine Sensibilisierung für das Thema erreicht und die Kompetenzen bei Absolvent*innen aufgebaut werden. entsprechen.

4.2.3 Sichere Produkte und Systeme

In den Diskussionen in den Workshops ist festgestellt worden, dass es für die meisten Personen nur schwer möglich ist, zu erkennen, welche Produkte oder Systeme hinsichtlich Cybersicherheit und Datenschutz sicher sind. So kann kaum jemand beurteilen, ob ein smartes Gerät wie ein Sprachassistent sicher ist. Noch schwieriger wird es bei Systemen, wie z.B. der gesamten in einem Gebäude integrierten Haustechnik (Abbildung 20).

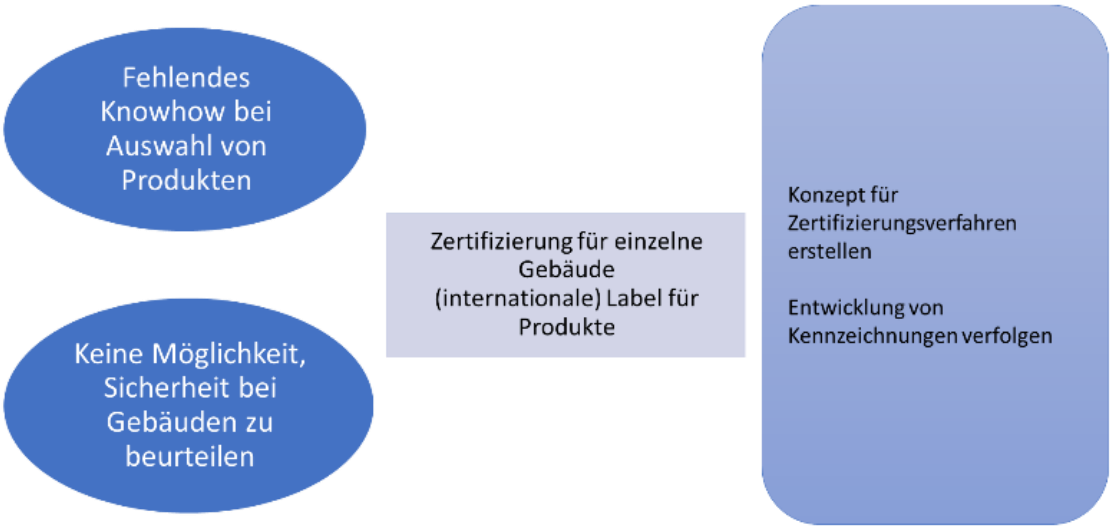


Abbildung 20: Um sichere Produkte und Systeme besser erkenntlich zu machen, soll ein Zertifizierungsverfahren für Gebäude entwickelt werden. Produkte sollen mit einer Kennzeichnung versehen werden, welche die Einhaltung der gültigen Vorschriften gewährleistet.

Wünschenswert wäre deshalb eine Zertifizierung für einzelne Gebäude, welche die Erfüllung der jeweils gültigen Standards garantiert. Dabei ist es für die Nutzenden der Gebäude nicht notwendig, die einzelnen Standards, Normen oder Richtlinien zu kennen, welche erfüllt sein müssen. Der Umstand, dass eine Zertifizierung vorliegt, zeigt, dass die Erstellende der Gebäude oder die Herstellende der technischen Systeme die relevanten Standards kennen und umgesetzt haben. Eine solche Zertifizierung ist vergleichbar mit z.B. der FSC-Zertifizierung, bei der sich der Käufer von Holz sicher sein kann, dass das Holz aus nachhaltigem Anbau stammt. Für die Zertifizierung von Gebäuden ist der erste Schritt die Entwicklung eines Konzepts für ein Zertifizierungsverfahren.

Ein nicht zu unterschätzendes Thema sind Geräte, welche die Nutzenden von Gebäuden selbst mitbringen und ins System des Gebäudes einbinden. Für diesen Fall, wie auch für Systemintegratoren*innen wäre eine Kennzeichnung hilfreich, welche die Einhaltung der für das jeweilige Produkt relevanten Standards garantiert. Solche Kennzeichnungen sind z.B. für die Einhaltung der elektrischen Sicherheit bekannt. Im europäischen Raum ist dies die CE-Kennzeichnung. Für Cybersicherheit und Datenschutz fehlt eine solche Kennzeichnung noch. Um eine solche Kennzeichnung für Produkte zu erreichen, sind Aktivitäten auf internationaler und politischer Ebene notwendig. Wir empfehlen deshalb, die Entwicklungen zu beobachten und sobald sie verfügbar sind, in die Leitfäden aufzunehmen.

5 Ableitung der empfohlenen Massnahmen

5.1 Interoperabilität

Den an Planung, Erstellung und Betrieb Beteiligten (Planer*innen, Integratoren*innen, Hersteller*innen, Betreiber*innen) ist durchaus bewusst, dass durch bessere Abstimmung der einzelnen Gebäudesysteme aufeinander Energie effizienter eingesetzt und Kosten eingespart werden können. Digitale Technologien helfen bereits während der Planung (z.B. BIM), aber auch im Betrieb durch die Vernetzung der Systeme, diese Ziele zu erreichen. Hemmnisse, welche die Ausschöpfung des Potenzials bremsen sind a) im Bereich der interdisziplinären Zusammenarbeit das immer noch vielfach vorherrschende Silodenken der involvierten Parteien, b) die Aus- und Weiterbildung und der Bestellerkompetenz, welche die Aspekte der Interdisziplinarität und der vernetzten Systeme zu wenig berücksichtigen und c) die grosse Anzahl an Standards, Protokollen und Schnittstellen, welche zu einer hohen Komplexität führen.

5.1.1 Interdisziplinäre Zusammenarbeit stärken

Durch den Einsatz von digitalen Technologien im Gebäude können Kosten und Energie in der Betriebsphase eingespart werden. Je besser die Geräte miteinander kommunizieren und interoperabel sind, umso höher ist das entsprechende Einsparpotential. Damit dies erreicht werden kann, sind die Ziele für den Betrieb der Gebäude bereits in der Planung zu berücksichtigen. Zu Beginn eines Bauprojektes sind die späteren Nutzenden und Betreibenden nicht immer bekannt. Werden die Ziele für die Funktionalitäten der Gebäudetechnik nicht entsprechend offen definiert, kann dies zu einem späteren Zeitpunkt zu Mehraufwänden führen, welche durch umfangreiche Anpassungen am System notwendig werden können. Zukünftig sollte für die integrale Planung ein iteratives Vorgehen angestrebt werden, damit die Auswirkungen von potenziellen Anforderungen aufgenommen und umfassend beurteilt werden können. Ein iteratives Vorgehen ermöglicht es allen Beteiligten, situationsgerecht zu arbeiten und fundiert zu entscheiden. Die Abwägung der Chancen und Risiken spielt dabei ebenso eine zentrale Rolle wie das Ausbalancieren der Anforderungen in Bezug auf die Nachhaltigkeit. Damit ist die Beurteilung aus ökonomischen, ökologischen und sozialen Aspekten zu verstehen, welche durch die beteiligten Interessensgruppen erstellt werden muss.

Ein Ansatz wie die interdisziplinäre Zusammenarbeit gestärkt werden kann, ist das High Performance Building. Vorgängig zur Swissbau 2022 wurde während einem Jahr in interdisziplinären Partnerteams bei drei realen Bauprojekten dieser Ansatz angewendet und die Resultate im Rahmen der Swissbau vorgestellt (Lit. 22).

Die Funktionsweise Anforderungen an ein High Performance Building können nicht linear gestellt werden. Es muss ein iteratives Vorgehen gewählt werden, damit durch die relevanten Beteiligungen beurteilt werden kann, was konkret realisiert werden kann und welchen Nutzen in der Bewirtschaftung zu erwarten ist. Abbildung 21 zeigt ein mögliches Vorgehen.

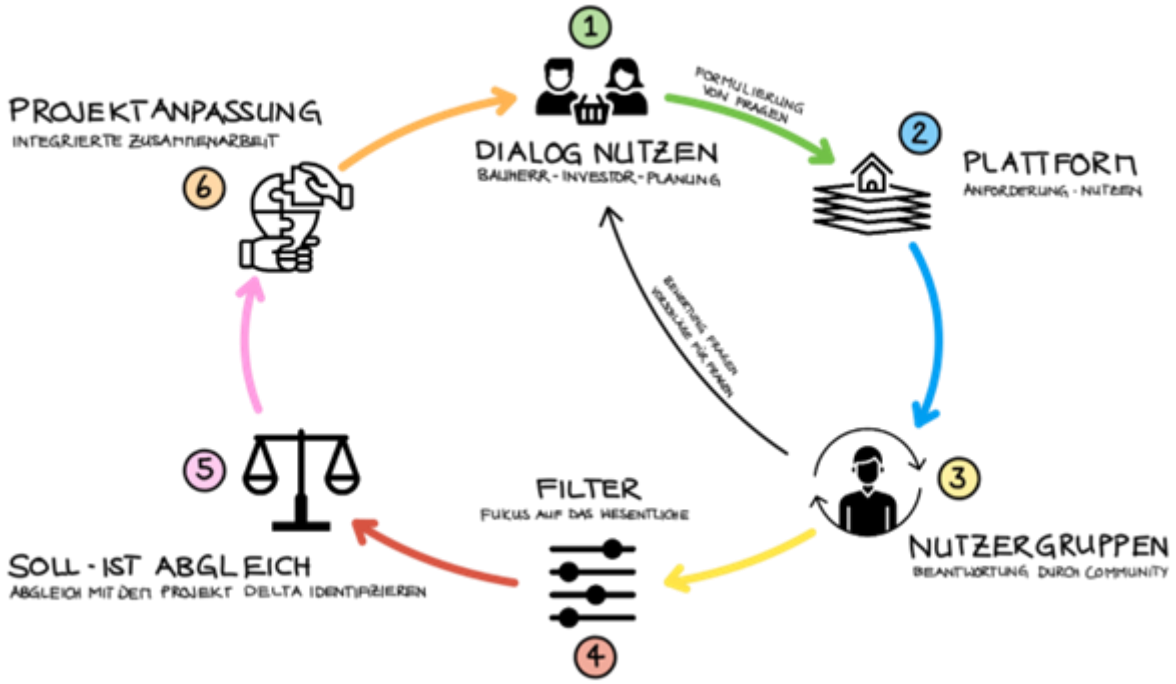


Abbildung 21: Systemabbildung des Prototyps im High Performance Building[4]

1. Die Formulierung von Anforderungen ist generell nicht einfach, wird jedoch zur Problematik, wenn die Stakeholder der Betriebsphase nicht oder nur vage bekannt sind. Nutzende und das Facility Management (FM) auf der operativen Ebene sind wichtig, damit ein Betrieb optimiert werden kann. Die hier bekannten Stakeholder sind meist der Auftraggeber (Investor oder Projektentwickler und später die Planenden). Sie formulieren typische Nutzungen und deren Anforderungen als Fragestellungen (Thesen).
2. Die Fragestellungen der Planer werden auf einer Plattform visuell im 3D-Modell wie auch als Fragen formuliert und der kompetenten Nutzer-Community zur Beantwortung bereitgestellt. Dabei werden die Anforderungen wie auch der Nutzen ins Zentrum gestellt, damit die jeweiligen Stakeholder ein möglichst optimiertes Bauwerk erhalten.
3. Die Stakeholder beantworten die Fragestellungen nach ihrem besten Wissen und nach ihren Bedürfnissen. Dabei sollen möglichst viele, verschiedene Perspektiven eingeholt und verglichen werden können. Zugleich können die Fragestellungen bewertet und ergänzt werden.
4. Über verschiedene Filter können die Anforderungen auf den jeweiligen Projektstand eingestellt werden.
5. Durch einen Soll-/Ist-Vergleich werden die Anforderungen im Projekt mit den Anforderungen der Stakeholder-Community verglichen und die Unterschiede aufgezeigt.
6. Mittels gleichzeitiger, integrierter Zusammenarbeit definieren Bauherr*innen (Projektentwicklung und ggf. Investor*in) und Planung die erforderlichen Anpassungen und optimieren das Projekt gemeinsam für die weiteren Projektphasen.
   Dieser Schritt kann mehrmals und in unterschiedlichen Zusammensetzungen stattfinden.
   Zudem kann je nach Stand, noch einmal mit Fragestellungen gestartet werden.

Um die Zusammenarbeit zwischen allen Beteiligten zu verstärken, muss das Wissen zu den Modellen und Werkzeugen, wie z.B. das High Performance Building, verstärkt in der Aus- und Weiterbildung integriert werden.

5.1.2 Aus- und Weiterbildung im Bereich Digitalisierung im Gebäude intensivieren

Bei der Umfrage, wie auch bei den Workshops hat sich gezeigt, dass vielfach das entsprechend geforderte technische Know-how fehlt, auch bei Planern*innen und Beratern*innen, welche nicht auf dem neusten Stand sind, um die Gebäude mit digitalen Technologien energieeffizienter betreiben zu können. Dies wurde nicht nur in diesem Projekt festgestellt, sondern auch im Bericht *Bildungsoffensive*

[4] Anforderungsplattform High Performance Building, Swissbau Innovation Lab 2022: Fokusgruppe IPD

Gebäude entsprechend dokumentiert. Die Autoren des Berichts Bildungsoffensive Gebäude (Lit. 9) kommen zum gleichen Schluss wie dieser Bericht, dass es zum Erreichen der Energie- und Klimaziele gut ausgebildete Fachleute benötigt, die sich laufend weitere Kompetenzen aneignen, diese Fachleute derzeit aber fehlen.

Daher ist es wichtig, dass die Aus- und Weiterbildung verstärkt in Richtung Interoperabilität auf allen Ebenen weiterentwickelt wird und die Fachkräfte entsprechende Kompetenzen erwerben können.

Der Bericht *Bildungsoffensive Gebäude* sieht diesbezüglich vier Handlungsbereiche:

1. Stärken der formalen Bildung
2. Befähigen bestehender Fachkräfte für gegenwärtige und künftige Herausforderungen über nicht-formale Bildung
3. Steigern der Attraktivität und Verbessern des Images
4. Stärken der branchenübergreifenden Zusammenarbeit

Massnahmen bezüglich der Thematik ausreichende Fachkräfte wird als wichtig angesehen:

Das Wissen über die aktuellen und zukünftigen digitalen Gebäudetechnologien und ihre Potentiale, in Bezug auf die Wirtschaftlichkeit aber auch in Bezug auf die Erreichung der Energie- und Klimaziele, müssen in den bestehenden Aus- und Weiterbildungen integriert und laufend weiterentwickelt werden. Dies nicht nur in den technischen Ausbildungen (z. B. Gebäudetechniker*innen, Planer*innen etc.), sondern vermehrt auch in den Ausbildungen mit einem wirtschaftlichen Bezug (z. B. Immobilienentwickler*innen, Immobilienbewirtschafter*innen etc.). Das erhöhte Wissen über die Potenziale von Gebäudetechnologien bei Personen mit wirtschaftlichem Bezug hilft Abhängigkeiten zum/r Planer*in zu reduzieren und die Bestellerkompetenz aufzubauen.

Die Bildungsoffensive Gebäude empfiehlt im Handlungsbereich „Stärken der branchenübergreifenden Zusammenarbeit“ einen regelmässigen Austausch unter den Verantwortlichen der Aus- und Weiterbildung der Gebäudebranche aufzubauen.

5.1.3 Bestellerkompetenz erhöhen und ein Smart Readiness Indikator einführen

Damit die Gebäude nachhaltiger betrieben werden, ist es wichtig, dass Gebäudebesitzer*innen, wie auch Gebäudebewirtschafter*innen ein Bewusstsein über die Energie- und Kosteneinsparungsmöglichkeiten entwickeln, die durch digitale Gebäudetechnologien möglich ist. Dieses Bewusstsein kann über Weiterbildungen und Informationsveranstaltung vermittelt werden, in welchen der Mehrwert und Nutzen anhand von konkreten Fallbeispielen aufgezeigt wird.

Es gibt eine Vielzahl an Gebäudeautomationslösungen und gerade im Energiebereich gibt es mehr und mehr Anbieter, die Energiemanagementsysteme bereitstellen, um die Energieproduktion im Gebäude mit Verbrauchern und Speichern zu integrieren und einen optimierten Betrieb sicher zu stellen. Diese Systeme integrieren eine Vielzahl an Betriebsmitteln und nutzen dazu viele technische Standards. Die Auswahl ist gross und Bestellende sehen zunehmend die Herausforderung, sich in diesem komplexen Markt zu bewegen und die richtige Wahl für ihre Bedürfnisse zu treffen. Ein „Vendor-Lock-In“ droht, wenn die Interoperabilität nicht gegeben ist. Mehr Markttransparenz und ein regelmäßig aktualisierter Überblick kann die Bestellenden in ihrer Wahl unterstützen und das Verständnis für die Lösungen sowie deren Nutzen stärken. Dabei sollte der Überblick möglichst einfach sein und auf einfach verständliche Indikatoren setzen. Er sollte insbesondere die Interoperabilität der Systeme thematisieren aber auch technische Aspekte der Informationssicherheit und des Datenschutzes aufgreifen.

Ein Ansatz ist der „Smart Readiness Indicator“ (SRI. Lit. 24), welcher durch die Europäische Kommission definiert wurde. Der SRI soll die Digitalisierung von Gebäuden, neue Funktionalitäten, die Automatisierung und die Überwachung technischer Anlagen im Gebäude zur Verbesserung der Energieeffizienz unterstützen.
Der SRI misst und weist die Intelligenzfähigkeit des Gebäudes bezüglich der eingesetzten Informations- und Kommunikationstechnologie, des Gebäudebetriebs, der Energieeffizienz und des Wohlbefindens der Gebäudenutzer aus (Abbildung 22).

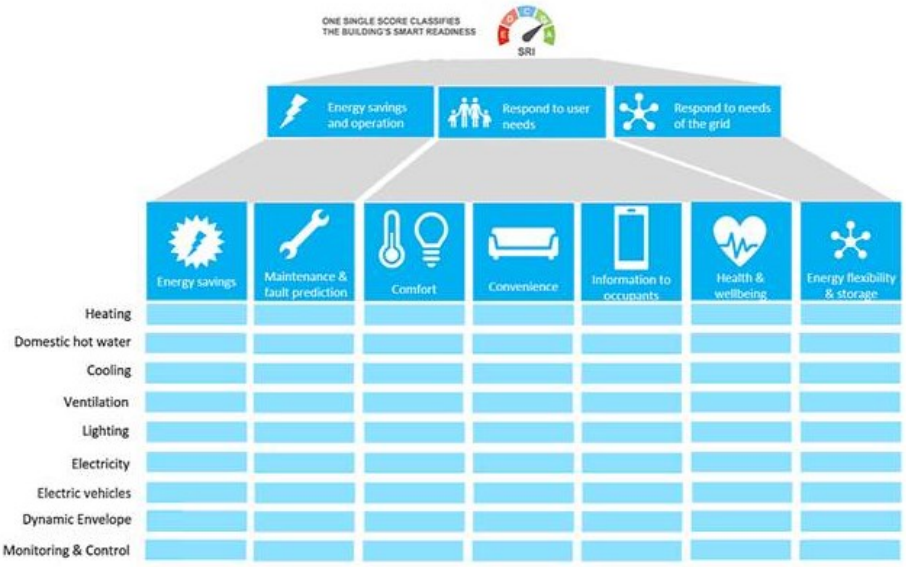


Abbildung 22: SRI-Struktur besteht aus 9 Bereiche, 7 Auswirkungskriterien, 3 SRI-Schlüsselfunktionen und die einer Gesamtbewertung. (Quelle: Final report on the technical support to the development of a smart readiness indicator for buildings, Lit. 3)

Ziel des SRI ist das Bewusstsein und das Vertrauen in die digitale Gebäudetechnologie zu stärken. In der Umfrage dieses Projekts hat sich gezeigt, dass der SRI bei mehr als 75% der Umfrageteilnehmer unbekannt ist. Die Autoren dieses Berichts sind aber der Ansicht, dass der SRI die Komplexität der Digitalisierung im Gebäude verständlicher macht und die Zusammenarbeit zwischen Gebäudeinvestoren*innen, Gebäudebesitzer*innen, Gebäudebewirtschafter*innen, Planer*innen und Integratoren*innen unterstützt. Durch einfach verständliche Kategorien kann auf transparenter Art und Weise gemeinsam entschieden werden welche Funktionalitäten in ein Gebäude eingebaut werden und deren Einfluss auf Kosten, Energieeffizienz und Wert des Gebäudes.

Um diesen Ansatz für Bestellende besser zugänglich zu machen, sollen für die wichtigsten Anwendungsfälle Leitfäden bereitgestellt werden. Diese Leitfäden fassen das Know-how für den Anwendungsfall zusammen und bilden für die Bestellenden eine Basis für deren Entscheidungen. Die Leitfäden sollen die relevanten Informationen aus den Werkzeugen, aber auch aus Normen und Standards bedarfsgerecht bereitstellen.

5.1.4 Standards, Protokolle und Schnittstellen harmonisieren und Integrationsaufwand reduzieren

Zwischenzeitlich gibt es diverse Initiativen, welche sich der «Reduzierung» der Anzahl Standards, Protokolle und Schnittstellen annehmen.

Eine Initiative, welche breit abgestützt ist, nicht nur auf Herstellerseite, sondern auch auf Seite der Gebäudebesitzer*innen und Gebäudebetreiber*innen ist die *International Building Performance & Data Initiative* (IBPDI, Lit. 12). Das Ziel von IBPDI, ist einen gemeinsamen Datenstandard für die Immobilien zu definieren, dies auf Basis eines gemeinsamen Datenmodells.

Einige der projektteilnehmenden Firmen unterstützen diese Initiative, welche dazu beiträgt, die Komplexität des Zusammenspiels der unterschiedlichen digitalen Technologien im Gebäude zu reduzieren. Ob sich dieses Initiative breit durchsetzen kann, wird die Zeit zeigen.

Eine weitere Initiative, welche versucht, den Integrationsaufwand unter den Geräten im Gebäude mittels standardisierter Kommunikationsschnittstelle zu verringern, ist das SmartGridReady Label. Geräte mit diesem Label ermöglichen die Kommunikation untereinander, indem eine standardisierte, sichere Kommunikation eingesetzt wird (Lit. 19).

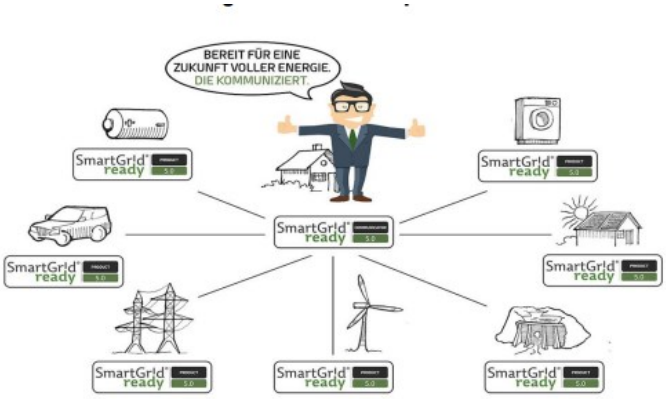


Abbildung 23: Vision Quelle: SmartGridready (Lit. 21)

Im «Mittelpunkt» von SmartGridready ist der Customer Energy Manager, welcher zwischen den Geräten im Gebäude (PV-Anlage, Wärmepumpenanlage, Gebäudeautomation etc.) vermittelt (Abbildung 23). Der Customer Energy Manager kann diese Vermittlungsrolle nicht nur innerhalb des Gebäudes, sondern auch gegen aussen z. B. zum Energieversorger übernehmen. (Abbildung 24)

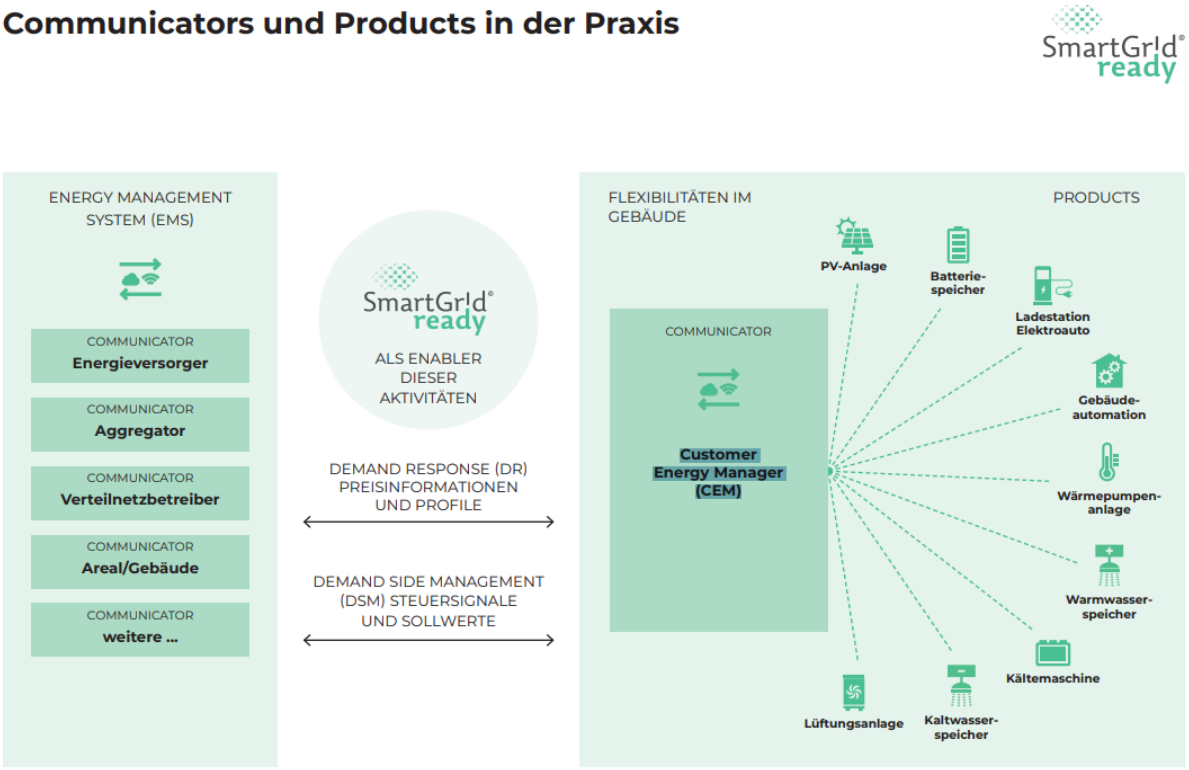


Abbildung 24: Funktionsweise Quelle: SmartGridready (Lit. 20)

Es gibt zwischenzeitlich diverse Initiativen, welche sich dem Thema Reduzierung der Integrationsaufwände durch Vereinfachung der Interoperabilität angenommen haben. Das ist wichtig und auch nötig. Welche dieser Initiativen sich langfristig durchsetzen, ist aktuell noch schwierig abzuschätzen. Von Vorteil wäre, wenn sich die verschiedenen Initiativen untereinander absprechen und auch abgleichen.

Als Massnahme sollen deshalb die Verantwortlichen der Initiativen kontaktiert und motiviert werden, den Austausch in einer unabhängigen Organisation zu pflegen. Eine solche Organisation könnte eine Interessengemeinschaft (IG) sein, welche allenfalls noch zu gründen wäre. Die IG würde den Rahmen bieten, dass Informationen aus den einzelnen Initiativen gegenseitig vorgestellt werden können. Ziel müsste sein, grösstmögliche Synergien zu erreichen. So soll erreicht werden, dass eine breit abgestützte Initiative auch erfolgreich umgesetzt werden kann.

5.2 Cybersicherheit und Datenschutz

5.2.1 Sensibilisierung der Bestellenden, Planenden und im Betrieb

Wie sich aus den Umfragen ergeben hat, besteht bei den Beteiligten durchaus Bewusstsein für die Herausforderungen der Cybersicherheit und des Datenschutzes. Allerdings sind sie sich eher unsicher, wie sie die Herausforderungen angehen sollen. Die Komplexität heutiger Gebäudetechnik mit vielen daran beteiligten Komponenten, sowie zusätzliche Schnittstellen mit privaten Geräten fördert die Unsicherheit. Hier zeigt sich mind. teilweise fehlendes Know-how und die Hürde der hohen Komplexität, um wirkungsvolle Massnahmen zur Erhöhung der Cybersicherheit umzusetzen. Dem soll mit Sensibilisierungsmassnahmen entgegengewirkt werden. Die Sensibilisierung soll dazu dienen aufzuzeigen, dass die Gefahren nicht nur zu erkennen sind, sondern dass auch aktiv Massnahmen getroffen werde müssen. Sensibilisierungskampagnen müssen verschiedene Anspruchsgruppen mit unterschiedlichen Bedürfnissen ansprechen können. Dementsprechend müssen in einem Konzept für eine Sensibilisierungskampagne mehrere Wege beschrieben werden.

Für alle Optionen einer Sensibilisierungskampagne gilt, dass diese aufzeigen müssen, welche Mehrwerte durch Einhalten der auszuarbeitenden Verhaltensregeln und Massnahmen entstehen. Ausserdem soll auch die Relevanz ein Thema sein und so aufzeigen, wie wichtig für die verschiedenen Beteiligten die Verhaltensregeln und Massnahmen sind.

Als mögliche Optionen einer Sensibilisierungskampagne stehen folgende Massnahmen zur Diskussion:

Informationskampagne: ähnlich wie es bereits für z.B. der Energieeffizienz umgesetzt wurde, soll auch für das Thema Cybersicherheit und Datenschutz ein Werbespot am Fernsehen, in sozialen Medien oder Werbung in Zeitungen, Zeitschriften, Fachzeitschriften, Plakaten usw. die Bevölkerung sensibilisieren. Ein Konzept für die Werbekampagnen wäre noch auszuarbeiten. Insbesondere die Botschaften und das Zielpublikum muss das Konzept klar definieren.

Aus- und Weiterbildung: Information über Aus- und Weiterbildung stellt aus Sicht des Projektteams eine sehr wichtige Form der Sensibilisierung dar. Über diesen Weg ist es einfach möglich, sehr gezielt die Herausforderungen aus Cybersicherheit und Datenschutz dem Zielpublikum näherzubringen. Insbesondere erfahren die Lernenden und Studierenden auf diesem Weg branchenspezifisch, welche Herausforderungen wie anzugehen sind. Die Entwicklung eines konkreten Aus- und Weiterbildungskonzept wäre im Anschluss an dieses Projekt anzugehen. Ein Konzept müsste insbesondere enthalten, welche Anforderungen in den Curriculi enthalten sein und welche Kompetenzen die Lernenden und Studierenden erlangen sollen.

„Roadshows“: Beteiligte können auch über Anlässe an verschiedenen Orten wie z.B. Ausstellungen, Kongressen oder öffentlichen Anlässen sensibilisiert werden. Ein Beispiel, welches bereits umgesetzt ist, kann im iHomeLab Visitor Center der Hochschule Luzern in Horw besichtig werden. Mit verschiedenen Geschichten führen die Guides die Besucher*innen an die Themen Datenerfassung, -weiterleitung und -verarbeitung heran. So lernen und erfahren die Besucher*innen, welche Vorteile daraus entstehen. Aber auch deren Nachteile und die Gefahren bezogen auf Cybersicherheit und Datenschutz werden dort thematisiert. Die Besucher*innen erhalten Denkanstösse zum Umgang mit Daten und wie man sich vor Missbrauch schützen kann. Ein Konzept für solche Roadshows wäre noch auszuarbeiten. Dieses soll die wichtigen, auf das jeweilige Zielpublikum ausgerichtete Botschaften definieren. Das Konzept soll ermuntern, das Thema Cybersicherheit und Datenschutz an Anlässen aufzugreifen und den Organisatoren Hilfestellungen für die Umsetzung geben.

5.2.2 Toolunterstützung zur Anwendung von Standards, Normen und Richtlinien

Wie in 4.2.1 beschrieben, soll ein Tool spezifisch für eine Problemstellung die relevanten Standards, Normen und Richtlinien auflisten. Ein solches Tool besteht als Prototyp und muss weiterentwickelt werden. Im Prototyp ist eine erste Klassierung der Standards, Normen und Richtlinien vorgenommen worden. Die Klassierung muss noch weiterentwickelt und verbessert werden. Als Datengrundlage sind im Moment etwa 80 Standards, Normen und Richtlinien im Tool enthalten. Diese muss weiter ergänzt und bereinigt werden.

Die wichtigsten Anwendungsfälle des Tools sind (Abbildung 25):

Suche von relevanten Standards: Dies ist der Hauptanwendungsfall. Wie im Soll-Zustand beschrieben sollen die Nutzenden die für ihre Situation und Problemstellung relevanten Standards aufgelistet bekommen.

Kommentieren von Suchresultaten: Den Nutzenden soll die Möglichkeit gegeben werden, die Suchresultate zu kommentieren. Das soll ermöglichen, die Qualität des Tools laufend zu verbessern.

Vorschlagen neuer Standards: Sobald ein neuer Standard erscheint, sollen die Nutzenden vorschlagen können, diesen ins Tool zu integrieren.

Standards zum Löschen vorschlagen: Standards, welche nicht mehr relevant sind, sollen aus dem Datenbestand gelöscht werden können.

Editieren von Einträgen: Der Datenbestand soll laufend aktualisiert werden können. So u.a. auch die Klassierung von einzelnen Standards.

Weitere Anwendungsfälle wären noch zu definieren.

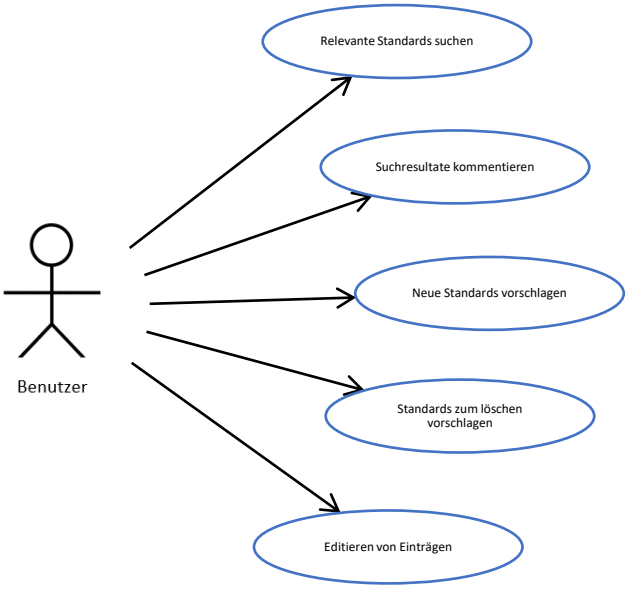


Abbildung 25: Anwendungsfälle für das Tool zur Suche nach Standards, Normen und Richtlinien

Um die Pflege des Datenbestandes zu gewährleisten, ist noch eine Stelle zu bestimmen. Diese zeichnet dafür verantwortlich, vorgeschlagene Änderungen und neu einzutragende Standards zu prüfen und die Daten zu erfassen. Ausserdem ist noch ein Konzept für die Inbetriebnahme, den Betrieb und den Unterhalt in technischer und finanzieller Hinsicht auszuarbeiten.

Für das Tool soll die internationale Zusammenarbeit thematisiert werden, damit auch Know-how aus dem (europäischen) Ausland einfliessen kann.

5.2.3 Entwicklung Leitfaden für Anwendungsfälle im Gebäude

Beteiligte sollen in Fragen zur Cybersicherheit oder zum Datenschutz unterstützt werden, indem sie für ihre spezifischen Anwendungsfälle Leitfäden abfragen können. Diese Leitfäden sollen auf die wichtigsten Fragen Antworten geben, aber auch Hinweise darauf enthalten, wie und wo weitere Hilfestellungen erhalten werden, kann. Die Umsetzung von Cybersicherheit und Datenschutz sollen erleichtert werden, indem in den Leitfäden das Know-how bereits für die Anwendungsfälle aufbereitet ist und als Handlungsanweisungen zur Verfügung steht.

Die Inhalte für Leitfäden und Mustervorlagen sind noch zu erstellen. Dies umfasst auch, dass ein Werkzeug zur Verfügung steht, wo Experten diese Inhalte erfassen können. Zu entwickeln ist ein Detailkonzept für das Tool, so dass Nutzende Antworten auf ihre spezifischen Frage- und Problemstellungen erhalten. Das Konzept definiert die Kriterien, nach denen im Tool gesucht werden kann. Anhand der Kriterien kann der spezifische Leitfaden erstellt und vom Tool ausgegeben werden (Abbildung 26).

Für eine erste Version des Leitfadens sollen für die wichtigsten Problemstellungen (diese sind noch zu definieren) statische Dokumente zusammengestellt werden. So können in kurzer Zeit erste Hilfestellungen angeboten und z.B. auf Webseiten von Branchenverbänden veröffentlicht werden.

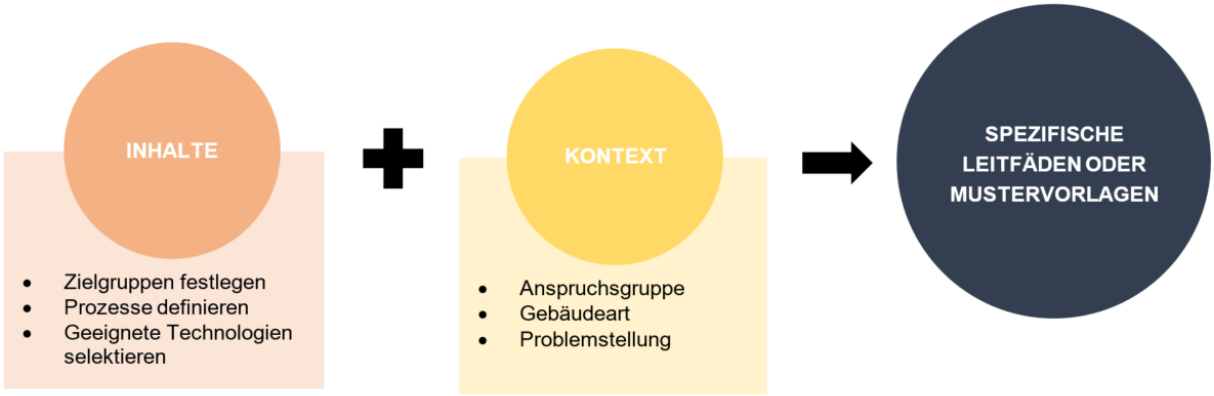


Abbildung 26: Aus den Inhalten werden kontextspezifische Leitfäden oder Mustervorlagen generiert.

5.2.4 Aus- und Weiterbildung stärken

Für die Aus- und Weiterbildung sind in einem ersten Schritt die detaillierten Themen im Bereich Cybersicherheit und Datenschutz zu definieren, welche in den Lehr- und Studiengängen aufgenommen werden sollen. Mögliche Themen sind Frameworks für Cybersicherheit, welche den Umgang mit Cybersicherheit und Datenschutz auf organisatorischer Ebene regeln. Oder auf der technischen Ebene, Verschlüsselungstechnologien und Kommunikationsprotokolle. Die Themen sollen auf das jeweilige Fachgebiet spezifisch angepasst sein. Dies gilt auch für die von den Lernenden und Studierenden zu erlangenden Kompetenzen (Abbildung 27).

In einem zweiten Schritt sind Curriculi für Lehrgänge zu entwerfen oder anzupassen, so dass Lernende und Studierende die definierten Kompetenzen erlangen können. Bildungsinstitutionen sollen Angebote für Aus- und Weiterbildung entwickeln, welche die Themen Cybersicherheit und Datenschutz zum Inhalt haben. In den IT-nahen Ausbildungen stehen bereits eine Vielzahl an Lehr- und Studiengängen zur Verfügung. In anderen Fachgebieten muss das Thema verstärkt berücksichtigt werden. Dazu sind mit Sensibilisierungsmassnahmen die Verantwortlichen für die Lehrgangsgestaltung zu motivieren, diese Themen zu berücksichtigen.

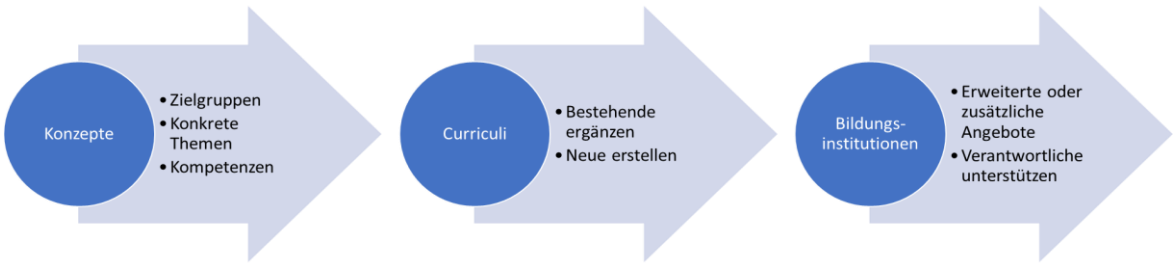


Abbildung 27: für die Aus- und Weiterbildung müssen Konzepte und Curriculi erstellt werden. Bildungsinstitutionen bieten zusätzliche Angebote an. Die Verantwortlichen müssen fachlich unterstützt werden.

5.2.5 Zertifizierung und Label einführen

Für die Zertifizierung von einzelnen Gebäuden ist ein entsprechendes Zertifizierungsverfahren zu entwickeln. Dies umfasst auch die Entwicklung von Anleitungen für Auditierungen sowie Checklisten, welche die Verantwortlichen bei der Vorbereitung zur Zertifizierung von Gebäuden unterstützen (Abbildung 28).

Da für die Etablierung von Kennzeichnungen Anstrengungen auf internationaler und politischer Ebene notwendig sind, sollen die Bestrebungen zu und die Entwicklungen von Kennzeichnungen beobachtet werden. Sind Kennzeichnungen verfügbar, sollen diese in die Erstellung von kontextspezifischen Leitfäden aufgenommen werden.

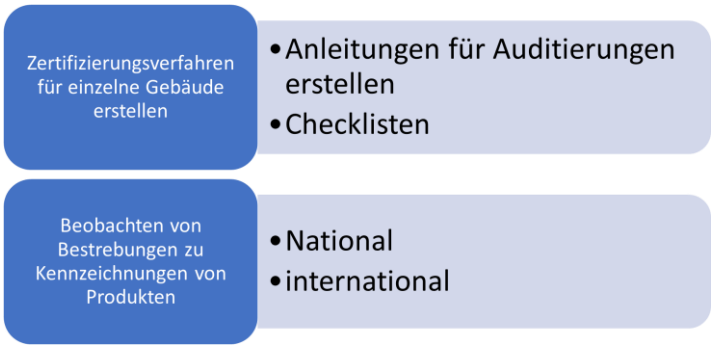


Abbildung 28: Für Gebäude ist ein Zertifizierungsverfahren zu erstellen, die Bestrebungen nach Kennzeichnungen sind zu beobachten.

6 Beschreibung des weiteren Vorgehens und des Leitfadens

6.1 Weiteres Vorgehen im Bereich Interoperabilität

Der Ansatz des Smart Readiness Indicator (SRI) ermöglicht es, den Grad der möglichen Gebäudeintelligenz von Gebäuden auszuweisen. Die Gebäudeintelligenz wird anhand des Digitalisierungsgrades der Bereiche Betrieb, Management und Monitoring, Interaktion der Bewohner, Netzdienlichkeit, Interoperabilität der Gebäudeautomation und technischer Gebäudeausstattung bestimmt (sinngemäss der sieben Auswirkungskriterien Abb. 22). Der Indikator liefert auf dieser Basis nützliche Informationen zur aktuellen Gebäudeintelligenz für Gebäudeinvestoren*innen, Gebäudebesitzer*innen und Gebäudebetreiber*innen. Mittels dieses Indikators kann einerseits die Bewertung des Objektes verbessert werden und der Umfang der Digitalisierung im Gebäude schon während der Planung an den Bedürfnissen in der Betriebsphase angepasst werden. Anderseits kann damit auch erarbeitet werden, was getan werden muss, um eine entsprechende avisierte Gebäudeintelligenz erreichen zu können.

Der SRI ist ein Instrument, welcher die Bestellerkompetenz von Gebäudeinvestoren*innen, Gebäudebesitzern*innen und Gebäudebetreibern*innen erhöhen und das gemeinsame Verständnis für die digitalen Technologien über die Gebäudebranche hinweg stärken kann.

Der SRI kann als Grundlage für die Vermittlung von Know-how und die Entwicklung von Anleitungen für die Erhöhung der Bestellerkompetenz dienen. Ein weiteres Ziel müsste sein den SRI mit Normen und Standards bedarfsgerecht zu erweitern und mittels eines dynamischen Prozesses permanent weiterzuentwickeln.

Mit der relativ einfachen Struktur aus neun Bereichen, sieben Auswirkungskriterien und drei Schlüsselfunktionen werden auch Personen mit wenig Fachkompetenz bezüglich der digitalen Technologien im Gebäude befähigt, ihre Anforderungen und die entsprechenden Auswirkungen beurteilen zu können.

Die HEA – Fachgemeinschaft hat im Jahr 2019 gemeinsam mit dem Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) eine Grundlagenstudie zum SRI publiziert, welche zum Schluss kommt, dass die Ausweisung des Grades der möglichen Gebäudeintelligenz von Gebäuden anhand des einfachen Ansatzes der SRI nicht nur Energieeffizienz und Komfort in Gebäuden erhöhen kann, sondern auch erhebliches Marktpotential eröffnet. Voraussetzung ist ein gemeinsamer Dialog zwischen allen an Planung, Bau und Betrieb Beteiligten, sowie auch den Nutzenden. Das Vorgehen dazu muss noch definiert werden.

Im Rahmen dieses Projektes hat sich gezeigt, dass die Akzeptanz eines solchen Indikators vorhanden ist. Als einer der nächsten Schritte sollte verifiziert werden, wie ein solcher Indikator in der Schweiz eingesetzt werden könnte resp. welche Informationen ergänzend in Anleitungen übernommen werden sollen und welche Anpassungen für den Schweizer Markt gefordert sind.

Im Rahmen der IG Konnektivität im Gebäude sollte überprüft werden, wie die Bestrebungen des High Performance Building unterstützt werden können, damit die interdisziplinäre Zusammenarbeit über die Stakeholder hinweg gestärkt werden kann.

Weiter soll die Marktransparenz im Bereich der Energiemanagementsysteme verbessert werden. Ein regelmässig aktualisierter und neutraler Marktüberblick, der einfache Indikatoren verwendet und die wichtigsten Produkte sowie deren Features umreist, wäre zu entwickeln und sicherzustellen. Der Marktüberblick wäre insbesondere für Nutzer und Bestellende wichtig und sollte entlang ihrer Bedürfnisse entwickelt werden. Erste Ansätze wurden bereits 2020 im Rahmen eines durch Energie Schweiz unterstützen Projektes entwickelt[5]. Diese wären aufzugreifen, weiterzuentwickeln und insbesondere in einfach nutzbarer Form, z.B. als Webapplikation verfügbar zu machen. Damit können Hemmnisse und Komplexität reduziert und die Verbreitung solche Systeme unterstützt werden.

Die Erkenntnisse aus den Bestrebungen zur Etablierung des *Smart Readiness Indicators* und des *High Performance Buildings* sollen anschliessend mit weiteren Handlungsanleitungen ergänzt werden, so dass für verschiedene Anwendungsfälle zum Thema Interoperabilität in Planung, Bau und Betrieb von Gebäuden Leitfäden erstellt werden können. Diese Leitfäden sollen zudem mit den relevanten Standards, Normen und Protokollen ergänzt werden, sofern diese nicht bereits aus den Initiativen hervorgehen.

6.2 Leitfaden für Cybersicherheit und Datenschutz

Ein Leitfaden ermöglicht durch Vermittlung von Know-how und Anleitungen die Sicherheit im Umgang mit Daten, also bzgl. Cybersicherheit und Datenschutz, zu erhöhen. Der Leitfaden soll in den drei Bereichen Prozesse, Menschen und Technologien Hilfestellungen und Massnahmen vorschlagen. Massnahmen sollen Prozesse sicherer machen. Zu berücksichtigen sind Prozesse in der Planungs- und Entstehungsphase (z.B. Ausschreibungen) aber auch im Betrieb (z.B. bei einem Mieterwechsel, oder wenn neue Geräte in ein bestehendes System eingebunden werden). Die Rolle der Menschen ist wesentlich. Letztlich hängt es vom Verhalten jedes Beteiligten, jeder Beteiligten ab, wie wirksam die umgesetzten Massnahmen sind. Die im Leitfaden vorgeschlagenen Technologien, wie beispielsweise Kommunikationsprotokolle oder Verschlüsselungsmethoden, sind so gewählt, dass Cybersicherheit und Datenschutz gewährleistet werden können. Der Leitfaden soll alle Beteiligten in deren Rolle unterstützen, die Cybersicherheit und Datenschutz bei Prozessen, im Verhalten und der Wahl von Technologien zu gewährleisten. Sei es als Bewohner*in, als Eigentümer*in, Bewirtschafter*in, Hersteller*in, Planer*in usw.

6.2.1 Konzept für Leitfaden

Der Leitfaden soll in Form eines Tools gestaltet werden kann, welches dann flexibel für unterschiedliche Rollen und Anwendungsfälle Verwendung finden kann. Der Leitfaden deckt die drei Bereiche Prozesse, Verhalten und Technologien angepasst auf die Anspruchsgruppe und den Anwendungsfall ab (Abbildung 29). Die Inhalte eines solchen Tools sind regelmässig zu aktualisieren und überprüfen.

Der toolgestützte Leitfaden liefert konkretere Empfehlungen zu Massnahmen zur Gewährung und Erhöhung von Cybersicherheit und Datenschutz. Die Empfehlungen sollen auf die technischen Herausforderungen eingehen und Lösungsansätze für die jeweilige Anspruchsgruppe präsentieren. So unterscheiden sich die Massnahmen für Gebäude in Betrieb von solchen der Planungs- und Bauphase. Im ersten Fall sind die Anspruchsgruppen Wohnungseigentümer, Mieter, Betreiber und Verwaltungen. In der Planungs- und Bauphase sind die Anspruchsgruppen Planer, Immobilienentwickler und Architekten. Der Leitfaden soll verschiedene Typen von Gebäuden berücksichtigen: residentielle oder kommerzielle Gebäude, kritische Infrastrukturen, industrielles Umfeld.

[5] Energiemanagementsysteme. Digitales Werkzeug der Energieversorgung. Eine Marktübersicht. (Lit. 25)

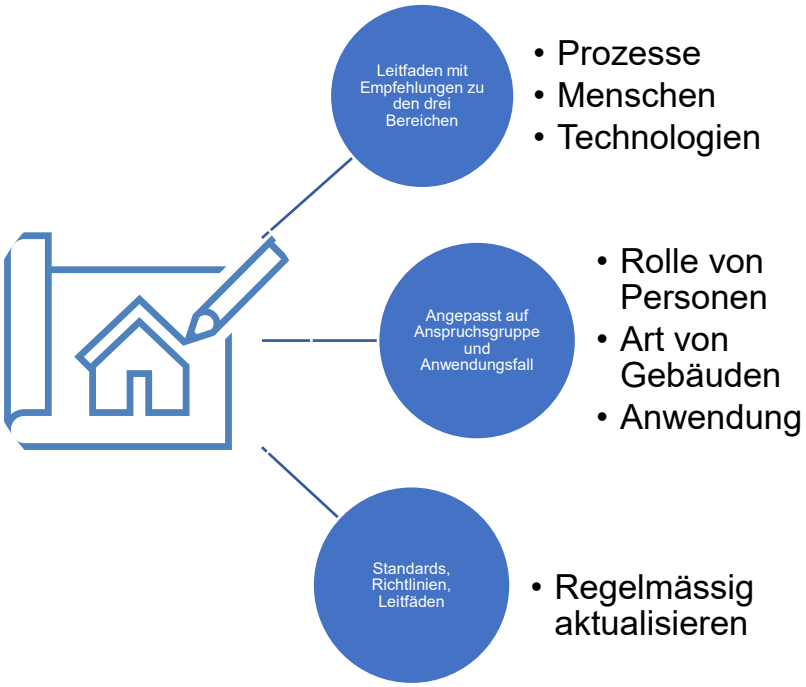


Abbildung 29: Mögliche Inhalte eines Leitfadens zur Unterstützung im Thema Cybersicherheit und Datenschutz

6.2.2 Inhalte des Leitfadens

Cybersicherheit

Der Leitfaden soll sich inhaltlich an das NIST Cybersecurity Framework (CSF) halten (Abbildung 30). Je nach Prozess und nach Anspruchsgruppe sind die fünf Phasen des CSF im Leitfaden mit entsprechenden Inhalten zu füllen. Nachfolgend ist für die fünf Phasen beschrieben, welche Aktivitäten diese beinhalten. Geplant ist, dass für verschiedene Prozesse und Anspruchsgruppen verschiedene Leitfäden zur Verfügung stehen. Nicht jeder Leitfaden muss alle fünf Phasen beschreiben, sondern soll die für die jeweilige Problemstellung wichtigen Phasen umfassen.

Abbildung 30: Das NIST Cybersecurity Framework ist in die fünf Phasen Identify, Protect, Detect, Respond und Recover gegliedert.

a) Phase Identify

In dieser Phase geht es darum, die im Gebäude enthaltenen Systeme und Geräte aber auch Personen und Daten zu identifizieren. Ebenso müssen die Ziele, die Anspruchsgruppen und Prozesse verstanden und priorisiert werden, um Rollen und Verantwortlichkeiten zu bestimmen. Diese Informationen stellen auch die Basis für die Risikoanalyse und das Risikomanagement dar. Der Leitfaden soll dazu mit konkreten Anleitungen spezifische Hilfestellung geben. Der Leitfaden kann bei gut abgrenzbaren Prozessen auch konkret die Risiken benennen.

b) Phase Protect

Die Risikoanalyse ist die Grundlage für Schutzmassnahmen. Dort wo ein bedeutendes Risiko besteht, ist der Zugang zu den Systemen auf autorisierte Personen zu beschränken. Der Leitfaden soll auf die Risiken sensibilisieren und die Beteiligten mit Anleitungen schulen, ihre jeweilige Verantwortung wahrzunehmen. Der Leitfaden gibt Hinweise, wie Daten sicher verwaltet werden können und wie die Verfügbarkeit von Informationen gewährleistet werden kann. Diese Phase regelt zudem, wie Wartung und Reparaturen auch hinsichtlich Cybersicherheit erfolgen sollen. Auch Technologien zum Schutz der Systeme von Cyberangriffen können hier festgelegt werden.

c) Phase Detect

Ein Leitfaden kann auch Angaben darüber enthalten, wie Anomalien im Datenverkehr, und somit potenzielle Cyberangriffe, festgesellt werden können. Er beschreibt, wie eine kontinuierliche Überwachung der Daten im Gebäude erfolgen kann, so dass aussergewöhnliche Ereignisse frühzeitig erkannt und verstanden werden.

d) Phase Respond

Für den Fall eines aussergewöhnlichen Ereignisses sind Abläufe und Verhaltensregeln zu definieren, wie in diesem Fall vorzugehen ist. Je nach Prozess ist die interne mit der externen Kommunikation zu koordinieren, z.B. um Hilfe von spezialisierten Unternehmen anzufordern. Ein Leitfaden kann auch die Analyse der Vorfälle beschreiben, um eine adäquate Kommunikation zu ermöglichen. Neben der Kommunikation sind auch Massnahmen zu beschreiben, welche den Schaden durch Cyberangriffe möglichst schnell und wirksam eingrenzen.

e) Phase Recover

Um die Systeme im Gebäude wieder zur Verfügung stellen zu können, sind Verfahren zu beschreiben, wie bei der Wiederherstellung der Systeme vorzugehen ist.

Datenschutz

In der Schweiz ist geplant, im September 2023 das überarbeitete Datenschutzgesetz in Kraft zu setzen. Der Leitfaden soll bei Empfehlungen und Anleitungen bereits diese neue Gesetzgebung und so die aktuellen Entwicklungen im Datenschutz berücksichtigen.

7 Anerkennung

Dem Projektteam war es ein grosses Anliegen, die Themen der Interdisziplinarität, integrale Planung, Cybersicherheit und Datenschutz im Zusammenhang mit Gebäuden so aufzubereiten, dass daraus weitere Massnahmen abgeleitet werden können. Die Projektleitung dankt insbesondere dem BFE, Energie Schweiz und den beteiligten Firmen, welche durch ihre Finanzierung dieses Projekt ermöglicht haben. Der Dank gilt auch den Vertretern der beteiligten Verbände und Institutionen, welche ihre Erfahrungen in das Projekt einfliessen liessen. Zudem den Vertretern von Empa, FHNW und HSLU, welche die Arbeitspakete und die Workshops geleitet und ausgewertet haben.

8 Grundlagen

Die Grundlagen dieses Projektes beruhen auf selbst durchgeführten Umfragen sowie intensiven Recherchen.

Um eine klare Übersicht zu gewährleisten, wurden separate Dateien mit allen verwendeten Unterlagen erstellt und nicht direkt in diesen Bericht integriert.

Alle verwendeten Unterlagen zum Thema Interoperabilität und Intelligentes Gebäudes finden Sie unter der Datei «Grundlagen_Abschlussbericht_KiG» im ersten Folder «1_Interoperabilität». Im Text werden die betroffenen Stellen mit dem Verweis «GA_F1» markiert.

Alle verwendeten Unterlagen zum Thema Cyber Security und Datenschutz finden Sie unter der Datei «Grundlagen_Abschlussbericht_KiG» im zweiten Folder «2_CyberS & Datenschutz». Im Text werden die betroffenen Stellen mit dem Verweis «GA_F2» markiert.

9 Literaturverzeichnis

1. **Baunormlexikon. DIN EN 15232-1; 2017:** https://www.baunormenlexikon.de/norm/din-en-15232-1/c9acce24-ab83-4d79-aaa9-aad121318fdb
2. **Bitcom. Klimaschutz und Energieeffizienz durch digitale Gebäudetechnologien; 2021:** https://www.bitkom.org/sites/main/files/2021-11/211111_st_klimaschutz-und-energieeffizienz.pdf
3. **Build Up. Final report on the technical support to the development of a smart readiness indicator for buildings; 2020:** https://www.buildup.eu/en/practices/publications/final-report-technical-support-development-smart-readiness-indicator
4. **Bundesamt für Energie. Gebäude; 2022:** https://www.bfe.admin.ch/bfe/de/home/effizienz/gebaeude.html
5. **Bundesamt für Energie. Gebäudepark 2050 – Vision des BFE; 2022:** https://www.bfe.admin.ch/bfe/de/home/effizienz/gebaeude.exturl.html/aHR0cHM6Ly9wdWJkYi5iZmUuYWRtaW4uY2gvZGUvcHVibGljYX/Rpb24vZG93bmxvYWQvODk4NQ==.html
6. **Bundesamt für Umwelt. Treibhausgasinventar der Schweiz; 2022:** https://www.bafu.admin.ch/bafu/de/home/themen/klima/zustand/daten/treibhausgasinventar.html
7. **Bundesrat. Sicherheitsstandards für Internet-of-Things Geräte (IoT); 2019:** https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/29042020-Bericht-IoT-d.pdf.download.pdf/29042020-Bericht-IoT-d.pdf
8. **Deloitte. 2020 commercial real estate outlook; 2020:** https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/realestate/lu-2020-commercial-real-estate-outlook.pdf
9. **EnergieSchweiz. Bildungsoffensive Gebäude | Gemeinsam bilden wir Energie- und Klimazukunft; 2021:** https://www.energieschweiz.ch/bildung/bildungsoffensive-gebaeude/
10. **HSLU. Markus Schmidiger & Christian Kraft | Was die Digitalisierung für Immobilieninvestoren bedeutet; 2018:** Was die Digitalisierung für Immobilieninvestoren bedeutet (1/3) - Immobilienblog Hochschule Luzern (hslu.ch)
11. **HSLU. Ursula Sury / Die Datenschutzerklärung; 2021:** https://www.youtube.com/watch?v=8Fd082HU5u0
12. **IBPDI. The global data model for real estate; 2022:** https://ibpdi.org/
13. **Integrale Planung. Nutzen der Intergralen Planung; 2016:** https://www.integrale-planung.net/nutzen-der-integralen-planung_1592?p=1
14. **Intergovernmental Panel on Climate Change. Special report | Climate Change and Land; 2022:** https://www.ipcc.ch/srccl/
15. **Kernenergie. Der Schweizer Strommix; 2022:** https://www.kernenergie.ch/de/schweizer-strommix-_content---1--1069.html
16. **Konferenz Kantonaler Energiefachstellen | Regionalkonferenz Innerschweiz. Energienachweis; 2014:** https://www.energie-zentralschweiz.ch/vollzug/energienachweise-muken-2014.html
17. **Nationales Zentrum für Cybersicherheit. Informationen für Private; 2022:** https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-private.html
18. **Nist. Cybersecurity Framework; 2020:** https://www.nist.gov/cyberframework
19. **SmartGridready. SmartGridready:** https://smartgridready.ch/
20. **SmartGridready. Wie funktioniert das Label:** https://smartgridready.ch/media/documents/Wie-funktioniert-das-Label_Akquisition.pdf

21. **SmartGridready. Kommunikation in der Praxis:** https://smartgridready.ch/media/documents/Kommunikation-in-der-Praxis.pdf
22. **Swiss Bau. Iroom Show | Sieben neue Ideen für das Gebäude der Zukunft; 2022:** https://www.swissbau.ch/de/veranstaltung/iroom-show-sieben-neue-ideen-fuer-das-gebaeude-der-zukunft-42
23. **Umwelt Bundesamt. Erneuerbare Energien in Zahlen; 2022:** https://www.umweltbundesamt.de/themen/klima-energie/erneuerbare-energien/erneuerbare-energien-in-zahlen#uberblick
24. **Vito. Deliverables of the prior technical support studies | Smart Readiness Indicator for Buildings; 2022:** https://smartreadinessindicator.eu/deliverables-prior-technical-support-studies.html
25. **Energie Zukunft Schweiz. Energiemanagementsysteme. Digitales Werkzeug der Energieversorgung. Eine Marktübersicht, 2020.** https://www.energieschweiz.ch/news/energiemanagementsysteme/

Abbildungsverzeichnis