Smart Buildings vs. Data Privacy Law

Michael Keil
Betreuer: Dr. Holger Kinkelin, Marcel von Maltitz
Seminar Innovative Internettechnologien und Mobilkommunikation WS 2014/2015
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: Michaelkeil8590@aol.com

KURZFASSUNG

Um die Energieeffizienz von Gebäuden und Stromnetzen zu verbessern, wird eine große Menge an unterschiedlichen Daten, z.B. Energieverbräuche und Präsenz-Daten, gesammelt. Da diese Daten in manchen Situationen benutzt werden können um Personen eindeutig zu identifizieren, und aus ihnen andere Informationen wie Verhaltensmuster abzuleiten, treten Datenschutzgesetze in Kraft um vor Missbrauch persönlicher Daten zu schützen. Inwieweit Datenschutzgesetze auf das Sammeln von Daten in intelligenten Gebäuden zutreffen, welche Auswirkungen diese haben und welche Anforderungen erfüllt werden müssen um in keinen Konflikt mit den Datenschutzgesetzen zu geraten wird in dieser Ausarbeitung dargelegt.

Schlüsselworte

Datenschutz, Intelligente Gebäude, Smart Building

1. EINLEITUNG

Heutzutage legen viele Menschen immer größeren Wert auf die Erzeugung von erneuerbarer Energie. Um die erzeugte Energie so gut wie möglich nutzen zu können, ist es sehr wichtig neue Technologien und Systeme zu entwickeln und zu installieren die eine optimale Verteilung ermöglichen. Zusätzlich muss hierfür der Energieverbrauch gemessen werden und neue, bessere Technologien zum Speichern gewonnener Energie müssen erforscht werden, um den überschüssigen Strom, der zum Beispiel Nachts erzeugt wird, nicht zu verschwenden. Aus diesen Beweggründen sind viele Staaten dazu übergegangen Pläne für intelligente Stromnetze, sogenannte „Smart Grids“, zu entwickeln. Die Bundesnetzagentur spricht von einem „Smart Grid“ wenn ein konventionelles Elektrizitätsnetz mit Kommunikations-, Mess-, Steuer-, Regel-, und Automatisierungstechnik sowie IT-Komponenten aufgerüstet wird um den Netzzustand in „Echtzeit“ zu erfassen und Möglichkeiten zur Steuerung und Regelung des Netzes bestehen, um die Netzkapazität optimal nutzen zu können. [1] Während über die Datenschutzprobleme, die mit dem Erfassen von Energiedaten in „Smart Grids“ entstehen, in vielen Ländern diskutiert wurde, ist diese Problematik, in intelligenten Gebäuden, sogenannten Smart Buildings, bisher nur wenig beachtet worden. Auch ist diese Problematik bei intelligenten Gebäuden wesentlich schwerer zu erfassen, als bei der Erfassung des Energieverbrauches in intelligenten Stromnetzen. Während es bei Smart Grids offensichtlich ist, dass die Daten die in Haushalten erfasst werden geschützt werden müssen, da auch Haushalte erfasst werden in denen einzelne Personen oder Familien leben, ist die Problematik bei intelligenten Gebäuden weniger gut zu erkennen. Intelligente Gebäude zielen darauf ab Energieeffizienz, Komfort und Sicherheit im gesamten Gebäude zu gewährleisten, die Datenerfassung bezieht sich deshalb hauptsächlich auf Sensor- und Energiedaten welche in den meisten Fällen gesetzlich nicht geschützt werden müssen, jedoch gibt es auch Ausnahmen in denen die erfassten Daten unter den gesetzlichen Schutz fallen und ein gesetzeskonformer Umgang gewährleistet sein muss. Deshalb beschäftigt sich diese Arbeit damit, die Problematik des Datenschutzes in intelligenten Gebäuden darzulegen und aufzuzeigen welche Datenschutzgesetze eingehalten werden müssen und ob vorhandene Strategien zur Entwicklung datenschutzkonformer Software angewendet werden können, um die Vorgaben die hinsichtlich Datensicherheit und Datenschutz bestehen, erfüllen zu können.

In Kapitel 2 wird hierfür der Begriff „Smart Building“ definiert und es wird dargelegt welche Daten in diesen Gebäuden gesammelt werden. Kapitel 3 befasst sich dann mit den bestehenden Datenschutzgesetzen und der Fragestellung warum diese auf die gesammelten Daten intelligenter Gebäude Anwendung finden. In Kapitel 4 werden Hoepmanns Strategien dargelegt und es wird in Kapitel 5 untersucht ob diese auf die Problemstellung anwendbar sind.

2. SMART BUILDING GRUNDLAGEN

Der Auf- und Ausbau von „Smart Buildings“ ist ein wichtiges Thema, das auch in Zukunft noch weiterhin betrachtet werden wird.

2.1 Definition

Verschiedene Definition zum Begriff „Smart Building“ sind heutzutage vorhanden. der „Smart 2020“-Bericht liefert anhand von fünf Begriffen eine Definition zum Thema Informations- und Kommunikationstechnologien (ICT) in Gebäuden.

In diesem Bericht werden folgende fünf Worte verwendet um den Begriff „smart“ im Bezug auf Gebäude zu definieren.

Standardise: Der Umgang mit Informationen zum Energiekonsum und Emissionen in Systemen und Produkten der ICT soll standardisiert sein.

Monitor: Daten sollen in „Echtzeit“ überwacht und überprüft werden um die Energieeffizienz des Gebäudes zu erhöhen.

Account: Dem Konsumenten werden aufbereitete Daten, zu Themen wie Energieverbrauch und Emissionen, zur Verfügung gestellt um diesen in einer Verbesserung der Energieeffizienz einzubinden.

doi: 10.2313/NET-2015-03-1_11

Rethink: Durch die übermittelten Informationen soll der Konsument angestoßen werden sein Verhalten zu überdenken und bewusster mit Energie umzugehen.

Transform: Letztendlich soll der Konsument sein Energieverhalten verändern um die Energieeffizienz, an Stellen an denen eine Automatisierung nicht möglich ist, zu verbessern. [3][4]

Eine andere Definition liefert die Siemens AG. Diese ist der Meinung, dass nur Lösungen, welche die größte Synergie zwischen Energieeffizienz, Komfort und Sicherheit besitzen über längere Zeit bestehen bleiben werden. Lösungen die Gebäude in lebendige Organismen verwandeln, die vernetzt, intelligent, sensibel und anpassungsfähig sind. [5]

Intelligente Gebäude sind also Gebäude, die die Energieeffizienz verbessern, sich gegebenen Umständen anpassen, Wartungskosten reduzieren, indem nur notwendige Wartungen durchgeführt werden anstelle von Wartungen die nach einem vordefinierten Zeitplan stattfinden, und einen erhöhten Komfort liefern.

2.2 Erfassbare Daten

Um diese Ziele erreichen können werden in intelligenten Gebäuden eine Vielzahl von Daten gesammelt.

2.2.1 Temperatur

Temperatursensoren messen die vorherrschende Temperatur und leiten diese weiter zum Beispiel an eine Anzeigevorrichtung oder einen Datenspeicher. Ein Beispiel hierfür ist das Thermometer

2.2.2 Bewegungsdaten

Ein weiterer Sensor der heutzutage in den meisten größeren Gebäuden vorkommt ist der Bewegungssensor. Dieser erkennt die Bewegung eines Objektes oder Subjektes und kann dadurch Aktionen auslösen.

2.2.3 Stromverbrauch

Eine der wichtigsten Datenmessungen, um die Energieeffizienz zu erhöhen, ist das Aufzeichnen des Stromverbrauches. Je detaillierter man diesen misst und auswertet umso einfacher ist es eine Steigerung der Energieeffizienz zu erzielen.

2.2.4 Luftqualität und Luftfeuchtigkeit

Auch die Luft wird gemessen und analysiert. Neben der Qualität werden vor allem Rauchsensoren angebracht um auf eventuelle Gefahrensituationen reagieren zu können.

2.2.5 Statussensoren

Eine weitere Möglichkeit Ursachen für eventuelle unerwünschte Situationen zu finden ist das Messen von Statusinformationen. So wird zum Beispiel gemessen ob ein Fenster oder eine Tür geöffnet ist, in welchem Stock sich zurzeit der Aufzug befindet oder ob Leuchten angeschaltet sind oder nicht.

2.2.6 Kameraüberwachung

Um sicherheitsrelevante Bereiche abzudecken besteht auch die Möglichkeit Überwachungskameras anzubringen und somit optische Daten zu sammeln.

2.2.7 Sonstiges

Auch können weitere Sensoren angebracht sein um zu erkennen ob eine Glasscheibe intakt ist und wie hell es in einem Raum ist. Neben gebäudeinternen Daten werden auch gebäudeexterne Daten gesammelt zum Beispiel durch die Benutzung von Wetterstationen[6]

2.3 Datenverwendung

Diese Daten werden für unterschiedliche Aktionen verwendet. Um die Sicherheit von Personen im Gebäude und des Gebäudes selbst zu gewährleisten, werden in vielen Gebäuden sicherheitsrelevante Plätze Videoüberwacht um Bedrohungen rechtzeitig erkennen und beheben zu können. Neben Kameras dienen vor allem auch Glasbruchsensoren dazu ein unbefugtes Betreten von außerhalb zu erkennen, um somit Personen und Gegenstände im Gebäude zu schützen. Aber auch Gefahrensituationen innerhalb des intelligenten Gebäudes sollen mit Hilfe dieser Daten erkannt und gelöst werden. Beispiele dafür sind das Ausbrechen eines Feuers, oder das Auftreten gesundheitsgefährdender Gase in der Luft. Diese werden durch Rauchsensoren und Sensoren zur Überprüfung der Luftqualität erkannt und es können Gegenmaßnahmen eingeleitet werden, wie zum Beispiel die Räumung des Gebäudes und die Verständigung zuständiger Stellen.

Neben der Sicherheit ist der Komfort ein wichtiger Faktor intelligenter Gebäude. So helfen Temperatursensoren die Belüftungsanlagen zu steuern um eine angenehme Temperatur innerhalb des Gebäudes zu gewährleisten und Lichtsensoren steuern ein automatisches Herablassen des Sonnenschutzes um den Aufenthalt im Gebäude so komfortabel wie möglich zu gestalten.

Neben Komfort und Sicherheit spielt der Energieverbrauch eine wichtige Rolle. In dieses Thema fallen wie schon angesprochen das Thema Beleuchtung aber auch die Verwendung von Statussensoren hilft ein Gebäude effizienter zu machen. Ein schnelles Erkennen und mögliches automatisches Schließen eines offenen Fensters im Winter hilft dabei zum Beispiel. Um Gebäude jedoch noch Energieeffizienter gestalten zu können, zu hohen Energieverbrauch messen zu können und dazu beizutragen, dass nur der Strom verbraucht wird, der auch benötigt wird, ist es wichtig den Energieverbrauch von Geräten so genau wie möglich zu bestimmen.

Viele Sensoren helfen bei mehr als einem dieser Problem. So trägt der Bewegungssensor einerseits dazu bei den Stromverbauch des Gebäudes zu senken indem er die Lampensteuerung übernimmt, und Leuchten nur angehen wenn sie gebraucht werden, sondern erhöht auch gleichzeitig den Komfort innerhalb des Gebäudes, da das Betätigen von Lichtschaltern wegfällt.

Jedoch unterliegt das Sammeln und Verwenden von bestimmten Daten gesetzlichen Vorschriften. Dies führt dazu, dass ein gesetzeskonformes System entwickelt und eingesetzt werden muss um die Datensicherheit und den Datenschutz zu gewährleisten.

3. DATENERFASSUNG VS. DATENSCHUTZ

Während es einen internationalen Standard zum Thema Datenschutz gibt (ISO 29100 [7]) an dem man sich orientieren kann, ist es wichtig das Erfassen und Weiterverarbeiten von Daten so zu gestalten, dass es mit dem zutreffenden Gesetz kompatibel

doi: 10.2313/NET-2015-03-1_11

ist. In Deutschland gilt zum Beispiel das Bundesdatenschutzgesetz (BDSG) an das man sich halten muss. Im folgenden werden einige themenbetreffende Auszüge aus diesem Gesetz vorgestellt.

3.1 Bundesdatenschutzgesetz (BDSG)

Für intelligente Gebäude ist es sehr wichtig Daten so genau wie möglich zu sammeln um eine Optimierung der Energieeffizienz gewährleisten zu können. In manchen Fällen können jedoch Personen anhand eines Datensatzes identifiziert werden. Beispielsweise wenn der Energieverbrauch eines bestimmtes Computers gemessen wird, der nur von einer einzigen Person benutzt wird. Die so gesammelten Daten werden dann als personenbezogene Daten nach BDSG §3 bezeichnet.

Wodurch die komplette Datenerfassung den Paragraphen 9 des BDSG erfüllen muss. Wäre es möglich eine Zuordnung grundsätzlich zu verhindern, würde dem Bundesdatenschutzgesetz ebenfalls genüge getan.

(1) „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.

(2) Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“ [8]

Da Daten in intelligenten Gebäuden automatisiert gesammelt werden, muss die Datenerfassung konform zu den Anlagen des §9 sein. Diese besagen, dass

1. eine Zutrittskontrolle stattfinden muss, um zu gewährleisten, dass unbefugte Personen keinen Zutritt zu den Räumlichkeiten haben, in denen die gesammelten Daten verarbeitet werden. Ein Beispiel hierfür ist ein Firmenausweis, der nur Befugten das Betreten der Datenverarbeitungsanlagen gestattet.

2. Es muss eine Zugangskontrolle stattfinden, die nur Befugten die Benutzung gewährleistet. Es dürfen also nur befugte Personen den Computer benutzen auf dem die Daten gespeichert und verarbeitet werden. Ein Beispiel für diese Zugangskontrolle ist eine Passwort-Kontrolle, sodass niemand anderes Zugang zu den Daten hat.

3. Es muss weiterhin gewährleistet sein, dass Befugte auch nur Zugriff auf die Daten haben, für die sie eine Zugriffsberechtigung haben und die personenbezogenen Daten bei der Nutzung, Verarbeitung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können .

4. Personenbezogene Daten bei der elektronischen Übertragung, ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Außerdem muss überprüft und festgestellt werden können an wen diese Daten übertragen werden dürfen.

5. Es muss eine Eingabekontrolle stattfinden. Das heißt es muss nachvollziehbar sein wer die personenbezogenen Daten gesammelt, verändert oder entfernt hat.

6. personenbezogene Daten dürfen nur so verarbeitet werden wie der Auftrag es zulässt. Das heißt zum Beispiel wenn eine Zeitung Email-Adressen sammelt um Neuigkeiten an die jeweiligen Personen übermitteln zu können, darf die Email-Adresse auch nur dafür verwendet werden.

7. Es muss gewährleistet werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8. Außerdem muss das System die Möglichkeit zur Verfügung stellen das Daten, die für unterschiedliche Zwecke gesammelt wurden auch getrennt voneinander verarbeitet werden können.

Außerdem ist es für die Punkte zwei bis vier besonders wichtig, dass keine veralteten Verschlüsselungsverfahren verwendet werden, da dies ein Verstoß gegen Satz 2 darstellen würde. Sollte außerdem ein Arbeitsverhältnis vorliegen, sodass der Arbeitgeber die Daten des Arbeitnehmers sammelt oder verarbeitet tritt zusätzlich noch BDSG § 32 in Kraft der die Datenerhebung, -verarbeitung und -benutzung für Zwecke des Beschäftigungsverhältnisses regelt.[8]

3.2 Problem der Datenerfassung

Wie beschrieben gelten diese Datenschutzparagraphen nur für personenbezogene Daten, wäre es unter keinen Umständen oder nur mit einem unverhältnismäßigen großen Aufwand an Zeit, Kosten und Arbeitskraft möglich mit Hilfe der gesammelten Daten eine Person zu identifizieren, würde die Datenschutzgesetze nicht in Kraft treten. Außerdem würde die in BDSG §3a verlangte Anonymisierung wegfallen, die verlangt das personenbezogene Daten soweit wie möglich anonymisiert werden um eine Identifikation zu erschweren. [8]

Um eine genauere Erklärung aufzuzeigen, betrachten wir das Problem anhand der Energiemessung eines Computers (Abbildung 1). In der Abbildung sieht man das Starten des

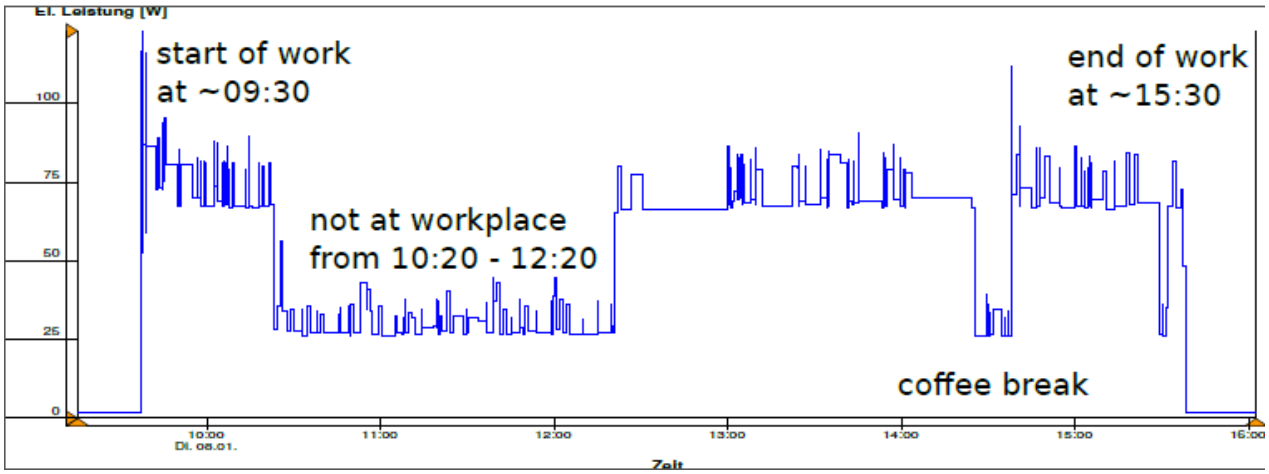

Abbildung 1. Energiemessung eines Computers[11]

doi: 10.2313/NET-2015-03-1_11

Computers um ungefähr 9.30 Uhr. Von ca. 10.20 Uhr bis 12.20 Uhr benötigt der Computer weniger Energie. Dies deutet darauf hin, dass der Computer zu dieser Zeit nicht benutzt wurde. Um 14.30 Uhr ist der Computer wieder nicht in Benutzung. Wenn man diese Daten jetzt mit der Energiemessung der Kaffeemaschine des Büros vergleicht, wäre es möglich Rückschlüsse führen zu können, ob der Benutzer zu dieser Zeit einen Kaffee getrunken hat. Auch wäre es möglich diese Zeit mit den Meldungen von Türen zu vergleichen um eine mögliche Route nachzubilden.

Neben Energiemessungen können aber auch andere Daten zu bestimmten Zeitpunkten oder in unterschiedlichen Kombinationen dazu benutzt werden um ein Individuum zu identifizieren. So können Bewegungsdaten von Bewegungsmeldern, oder Temperaturdaten des Büros dazu genutzt werden einen Bewegungsablauf zu bestimmen. Besonders einfach wäre dies bei Messungen in einem Büro, in dem nur eine Person arbeitet. Auch die Daten einer Zutrittskontrolle sollten auf keinem Fall in Verbindung mit anderen Daten genutzt werden dürfen. Selbst wenn die Daten der Zutrittskontrolle anonymisiert sind, sobald es möglich ist Festzustellen ob nur eine Person ein Gebäude betreten hat, stellt diese Information in Verbindung mit vielen anderen Daten eine Grundlage zu einer Identifizierung da. So können Sensordaten von Türen zum Beispiel dazu genutzt werden ein Bewegungsprofil zu erstellen. Dieses Profil kann mit Informationen darüber welche Türen geöffnet wurden zu einer Identifizierung führen.

Aber auch sensible Temperatur- und Luftqualitätssensoren könnten in kleinen Räumen Schwankungen aufweisen, die es gestatten könnten, den Aufenthalt einer Person in diesem Raum zu bestimmen. Diese Information könnte dann wiederum in Kombination mit anderen Daten wie zum Beispiel einer automatischen Lampensteuerung auf den Gängen dazu benutzt werden Bewegungsprofile anzulegen, welche wie beschrieben zu einer Identifizierung führen könnte.

In solchen Fällen sind diese Daten dann personenbezogene Daten und müssen, um sie nutzen zu können, entweder anonymisiert oder geschützt werden und den Anlagen des §9 des BDSG entsprechen. Sollte eine Anonymisierung nicht möglich sein dürfen die geschützten personenbezogene Daten nur nach Einwilligung der jeweiligen Person benutzt werden. Außerdem hat die jeweilige Person nach Charta der Grundrechte der europäischen Union das Recht zu erfahren welche Daten gesammelt wurden [8][9].

Nachdem das Problem der Datensammlung von „Smart Buildings“ erkannt wurde, stellt sich die Frage ob es möglich ist bestehenden Softwareentwicklungsstrategien zu folgen um eine datenschutzkonforme Erfassung und Verarbeitung für intelligente Gebäude zu entwickeln.

4. DATENSCHUTZSTRATEGIEN VON HOEPMANN

Neben der ISO 29100 gibt es auch verschiedene weitere Strategien an denen man sich orientieren kann um den Datenschutz einzuhalten. Darunter fallen auch die von Hoepmann vorgestellten Strategien, die als Unterstützung dienen sollen um datenschutzkonforme Software zu entwickeln. Diese orientieren sich an den europäischen Gesetzen und Richtlinien und erhöhen, bei einer Umsetzung dieser Strategien, die Wahrscheinlichkeit das die entwickelte Software gesetzeskonform in Europa ist.

4.1 Beschreibung und Erklärung der Datenschutzstrategien

Hoepmann entwickelte folgende acht Strategien um Datenschutzprobleme auszuschließen. Die Strategien sind Minimieren (Minimise), Verbergen (Hide), Trennen (Separate), Aggregieren (Aggregate), Informieren (Inform), Kontrollieren (Control), Durchsetzen (Enforce) und Demonstrieren (Demonstrate)

4.1.1 Minimieren

Unter „Minimieren“ versteht Hoepmann, dass

„die Menge der personenbezogener Daten die verarbeitet wird auf die geringste mögliche Menge begrenzt ist.“[10]

Das heißt, dass man, wenn möglich, keine personenbezogenen Daten sammelt und verarbeitet. Sollte es jedoch nicht möglich sein ohne diese Daten, dass gewünschte Ergebnis zu erzielen soll die Menge der persönlichen Daten so gering wie möglich gehalten werden.

4.1.2 Verbergen

Die zweite Strategie ist das „Verbergen“.

„Jede Art von persönlichen Daten, und ihre Beziehungen zueinander, sollen von jeglicher Betrachtungsmöglichkeit aus verborgen werden.“ [10]

Der Hintergedanke dieser Entscheidung ist, dass es nicht möglich ist die persönlichen Daten zu missbrauchen, wenn man keine Einsicht in diese hat. In welchem Ausmaße diese Strategie umgesetzt werden sollte ist jedoch situationsabhängig. Nehmen wir an ein Arbeitgeber braucht einige persönliche Daten eines Angestellten um diesem Angestellten in einer Angelegenheit zu helfen. Wenn der Arbeitgeber das Einverständnis des Angestellten hat, seine Daten für diesen Zweck zu benutzen, müssten in diesem Fall die persönlichen Daten nur vor Dritten verborgen werden.

4.1.3 Trennen

Bei der Strategie „Trennen“ geht es darum, dass persönliche Daten einzelner Personen getrennt voneinander und von verschiedenen Abteilungen bearbeitet werden. Dies soll verhindern, dass ein komplettes Profil einer Person angelegt werden kann, aufgrund der Tatsache, dass man nur einzelne Daten dieser Person besitzt. Auch die Speicherung persönlicher Daten sollte in verschiedenen, nicht verbundenen Plätzen stattfinden, um zu verhindern, dass Unbefugte die Möglichkeit besitzen diese Daten zusammenzufügen.

4.1.4 Aggregieren

Nachdem in der Strategie „Trennen“, die persönlichen Daten einzelner Personen getrennt wurden, soll in der Strategie „Aggregieren“ ein Zusammenfügen ähnlicher Daten stattfinden.

„Persönliche Daten sollen hier in größtmöglichen Gruppierungen und mit dem kleinstmöglichen Detailreichtum, in der die Daten noch nutzbar sind, verarbeitet werden.“ [10]

Hinter dieser Entscheidung steht die Idee, dass gruppierte Datensätze an Detailreichtum verlieren, da beispielsweise nur Durchschnittswerte der Daten verwendet werden, wodurch Spitzen eines einzelnen Datensatzes verloren gehen, und somit

von diesen Daten weniger auf einzelne Personen geschlossen werden kann. Jedoch kann man hier nicht nur auf die Größe der Gruppierungen achten, da der Datensatz nach dem Gruppieren immer noch eine sinnvolle Verarbeitung zulassen muss. Wenn man beispielsweise den Energieverbrauch von Computern mit dem Energieverbrauch von Leuchten gruppiert, könnte man aus dieser Gruppierung wahrscheinlich keine sinnvollen Daten mehr extrahieren.

4.1.5 Informieren

Während die ersten vier Strategien besonders darauf abzielen wie die Daten verarbeitet werden sollen, decken „Informieren“, „Kontrollieren“, „Durchsetzen“ und „Demonstrieren“ das Selbstbestimmungsrecht über die eigenen persönlichen Daten ab.

Die Strategie „Informieren“ ist dafür der erste Schritt. Personen müssen nach §33 BDSG informiert werden wenn ihre personenbezogenen Daten gespeichert oder verwendet werden.

Sie müssen informiert werden, welche Daten wie verwendet werden und welches Ziel hinter der Verwendung steht. Außerdem müssen sie auf Anfrage darüber informiert werden wie ihre persönlichen Daten geschützt werden und ob diese Daten mit Dritten geteilt werden. Auch muss Betroffenen auf Nachfrage mitgeteilt werden, welche Daten zum jeweiligen Zeitpunkt noch gespeichert sind.

4.1.6 Kontrollieren

Da wie gesagt jeder das Recht hat selbst über seine personenbezogenen Daten zu bestimmen, müssen auch Möglichkeiten zur Verfügung gestellt werden, dass Betroffene eigene Daten betrachten, aktualisieren und wenn erwünscht auch löschen können. Diese Strategie steht im besonders engen Zusammenhang mit der „Informieren“-Strategie, da es weder sinnvoll ist Betroffene über alles zu informieren wenn sie jedoch keinerlei Möglichkeit besitzen diese Daten zu kontrollieren. Aber auch jegliche Möglichkeit der Kontrolle ist nicht sinnvoll, wenn Betroffene in nicht ausreichender Weise über die Verwendung ihrer persönlichen Daten informiert werden.

4.1.7 Durchsetzen

Durchsetzen bezeichnet die Strategie, dass

„Datenschutzstrategien, die die rechtlichen Anforderungen erfüllen, bestehen und durchgesetzt werden sollen.“[10]

Diese Strategie ist sehr wichtig um eine gesetzeskonforme Software zu entwickeln. Besonders wichtig ist, dass jeder Punkt der Strategie umgesetzt wird. Es darf beispielsweise nicht vorkommen, dass man eine Methodik entwickelt hat die eine rechtliche korrekte Ausführung zulässt, diese jedoch nicht umsetzt. Auch müssen verwendete Techniken und Maschinen auf dem aktuellen Wissensstand sein um Verstöße gegen das Datenschutzgesetz abzufangen. Ein Beispiel hierfür ist das Verwenden von aktuellen Verschlüsselungsverfahren anstelle von alten Verfahren, welche möglicherweise günstiger in der Verwendung sind jedoch nicht mehr als sicher angesehen werden.

4.1.8 Demonstrieren

Die letzte der acht Strategien, ist die Strategie des „Demonstrierens“. Diese verlangt, dass man demonstrieren kann, dass die entwickelte Software allen Datenschutzvorgaben gerecht wird. Datenschutzbeauftragten soll es mit der Umsetzung dieser Strategie möglich sein, eine effektive Implementierung der Gesetze zu zeigen und bei Problemen die Reichweite der möglichen Datenschutzprobleme zu identifizieren.

4.2 Initiale Anwendungsgebiete

Ursprünglich entwickelte Hoepmann seine Strategien als Design Strategien die Softwareentwickler unterstützen sollten, datenschutzkonforme Software zu entwickeln. Jedoch ergibt sich durch die Aufgliederung der Strategien und die Umsetzung der in Europa vorherrschenden Datenschutzgesetze die Möglichkeit diese Strategien auch zum Evaluieren bereits existierender Software Design Patterns und Software zu benutzen.

Abbildung 2 zeigt eine Tabelle, die zeigt, welche Strategien auf bestehende gesetzliche Richtlinien angewendet werden können. So wird zum Beispiel eine gesetzliche geforderte Minimierung der verwendeten personenbezogenen Daten in den Strategien „Minimieren“, „Verbergen“ und „Aggregieren“ großflächig abgedeckt, während eine Benachrichtigung von Betroffenen bei einer Verletzung des Datenschutzgesetzes, also wenn zum Beispiel Unbefugte sich Zugang zu diesen Daten geschaffen haben, in der Strategie „Informieren“ abgedeckt ist.

	Aufgabenbegrenzung	Datenminimierung	Datenqualität	Transparenz	Selbstbestimmung der Betroffenen	Adäquater Schutz	Benachrichtigung bei Verletzung des Datenschutzes	Nachweisbare Einhaltung der Datenschutzgesetze
Minimieren	o	x						
Verbergen		x				o		
Trennen	o					o		
Aggregieren	o	x						
Informieren				x			x	
Kontrollieren			o	x	x			
Durchsetzen	x		x		x	x		o
Demonstrieren				o				x

Legende:
"x": große Abdeckung
"o": geringfügige Abdeckung

Abbildung 2. Abbildung der Strategien auf gesetzliche Prinzipien

5. ANWENDBARKEIT VON HOEPMANNS STRATEGIEN AUF DAS BESTEHENDE DATENSCHUTZPROBLEM

Nachdem Hoepmanns Strategien dargelegt wurden, stellt sich die Frage ob sich diese Strategien, die eine sinnvolle Unterstützung zur Entwicklung von datenschutzkonformer Software darstellen, auf das Datenschutzproblem, das sich bei der Datensammlung in intelligenten Gebäuden ergibt, anwenden lassen.

doi: 10.2313/NET-2015-03-1_11

5.1 Strategieanwendung

Da sich bei Anwendbarkeit und Einhaltung aller acht Strategien ein System ergibt, dass den Datenschutzgesetzen in Europa entspricht, wäre es wünschenswert wenn diese Strategien nicht nur auf Softwaresysteme Anwendung finden würden. Deshalb wird hier die Anwendbarkeit jeder einzelnen Strategie auf das vorliegende Problem überprüft, um mit Hilfe dieser Strategien ein gesetzeskonformes System für dieses Problem entwickeln zu können.

5.1.1 Minimieren

Die „Minimieren"-Strategie verlangt, dass die Erhebung personenbezogener Daten so weit wie möglich minimiert wird. Da in intelligenten Gebäuden nicht gezielt personenbezogene Daten gesammelt werden, sondern die gesammelten Daten personenbezogene Daten sind, da man in Einzelfällen diese Daten bestimmten Personen zuordnen kann, ist eine Minimierung im Grunde schon umgesetzt. Eine weitere Minimierung wäre es nur wenn man das Sammeln von Datensätzen die einer Person zugeordnet werden können unterbindet, was jedoch nicht umsetzbar ist weil sich diese Situation verändern. Zum Beispiel an einer Kaffemaschine in einem Büro holen sich normalerweise viele Leute einen Kaffee, wodurch dieser Datensatz alleine keine Zuordnung zu einer einzelnen Person zulässt. Während der Urlaubszeit arbeitet jetzt nur eine Person in diesem Büro, wodurch eine Zuordnung möglich ist und das verarbeitende System jetzt das Bundesdatenschutzgesetz erfüllen muss. Eine Minimierung auf die Benutzung keiner personenbezogenen Daten ist also nicht möglich. Inwiefern eine Umsetzung der „Minimieren"-Strategie umsetzbar ist, ist jedoch auch abhängig vom Ziel der Datennutzung. Wenn dieses Ziel trotz Minimierung des Datensatzes erfüllbar ist, kann und sollte eine Reduzierung des Datensatzes vorgenommen werden. Da in Smart Buildings jedoch eine Vielzahl unterschiedlicher Daten gesammelt werden, besteht in den meisten Fällen die Möglichkeit den erfassten Datensatz weiter zu reduzieren. Auch sollte mit dem Hinzufügen und Entfernen von Diensten die Größe des Datensatzes jedes mal neu bestimmt werden, um einen minimalen Datensatz zu gewährleisten.

5.1.2 Verbergen

Da in intelligenten Gebäude eine automatisierte Sammlung stattfindet, wäre es möglich die Strategie „Verbergen" soweit umzusetzen, dass niemand Zugriff auf personenbezogene Daten hat, sondern eine automatische Verarbeitungssoftware die Daten soweit anonymisiert, dass kein Rückschluss auf eine Person mehr möglich ist. Somit hätten weitere Bearbeiter nur Zugriff auf eine Datensammlung, die keine personenbezogene Daten mehr enthält. Sollte es jedoch nicht möglich sein bestimme personenbezogenen Daten zu anonymisieren oder zu gruppieren, sollte ein Whitelistingansatz eingeführt werden, sodass nur einzelne Personen Zugriff zu bestimmten Datensätzen haben. Auch sollte hier die Strategie „Trennen" umgesetzt werden, damit einzelne Personen nicht Zugriff zu verschiedenen Datensätzen haben, was die Wahrscheinlichkeit einer Zuordnung zu einer Person erhöht. Es wäre also am sichersten wenn für jeden Datensatz der nicht automatisiert verarbeitet werden kann, nur eine einzige Person Zugriff zu diesen Daten erhält, die keine Genehmigung hat andere Datensätze einzusehen und zu bearbeiten.

5.1.3 Trennen

Da in Smart Buildings eine Vielzahl an verschiedenen Diensten installiert ist und angeboten wird, werden für deren Umsetzung auch eine riesige Menge Daten erfasst. Diese Daten sollten aufgrund der „Trennen"-Strategie separiert gespeichert und behandelt werden. Da einige Mehrwertdienste zur Umsetzung jedoch mehr als einen Datensatz benötigen, könnte hier wiederum ein Whitelistingansatz realisiert werden, sodass nur bestimmte Mehrwertdienste Zugriff auf mehrere Datensätze erhalten und dann auch nur auf die Datensätze die zur Erfüllung des Dienstes benötigt werden. Auch kann überlegt werden, ob man sich für jeden Mehrwertdienst einzeln die Einwilligung zur Verwendung der Nutzerdaten beschafft. Auf diese Weise kann jeder Nutzer selbst entscheiden welche Daten von welchen Diensten verwendet werden dürfen, wodurch der Nutzer die Kontrolle über die Trennung seiner Daten erhält.

5.1.4 Aggregieren

Auch ist es in Smart Buildings möglich Daten auf unterschiedliche Art und Weisen zu aggregieren. Die erste Möglichkeit ist eine räumliche Aggregation. Hier können zum Beispiel Daten aus Abteilung oder Geschossen zusammengefasst werden, um die Informationstiefe zu verschleiern. Es wäre möglich den Stromverbrauch aller Computer einer Abteilung zu aggregieren, so werden Benutzungsdaten einzelner Computer verschleiert, jedoch ist es weiterhin möglich den Stromverbrauch während unterschiedlicher Tageszeiten zu erfassen.

Neben einer räumlichen Aggregation kann auch eine zeitliche Aggregation stattfinden. Man gruppiert Datensätze also über einen ganzen Tag oder ganze Wochen. Auf diese Weise kann kein Benutzungsschema erstellt werden, was zu einer Zuordnung von Personen führen könnte, jedoch ist es beispielswiese weiterhin möglich den Stromverbrauch der Kaffeemaschine zu erfassen. Wenn man jetzt weiterhin erfasst wie viele Kaffee ausgegeben wurden und wie oft die Kaffemaschine sich selbst gereinigt hat, kann über längere Zeit trotz Aggregation festgestellt werden in welchen Phasen die Kaffemaschine wie viel Strom benötigt und ob die Anschaffung einer anderen Kaffeemaschine Einsparungen mit sich bringen könnte oder nicht.

5.1.5 Informieren

Eine Umsetzung der Strategie „Informieren" ist jedoch nur schwer möglich da man hierfür alle Datensätze, die eine Identifizierung zulassen, erkennen müsste und man sich auch mit der jeweiligen Zuordnung sicher sein müsste, um eine Weitergabe an Dritte ausschließen zu können. Die Information weiterzugeben welche Daten in einem intelligenten Gebäude gesammelt werden ist jedoch einfach zu erzielen, dies könnte mithilfe von öffentlicher Displays bewerkstelligt werden. Auch könnten Informationen auf einzelne Räume beschränkt werden. So könnte zum Beispiel in einem intelligenten Besprechungszimmer nur angezeigt werden, welche Daten in diesem Zimmer gesammelt werden. Auf diese Weise wären Benutzer darüber informiert welche Daten auf welche Weise erfasst werden.

5.1.6 Kontrollieren

Wie auch bei der Strategie „Informieren" ist das Anwenden von „Kontrollieren" für bestimmte Daten nur schwer erzielbar, da erst eine eindeutige Identifizierung dieser Datensätze stattfinden müsste um den betroffenen Personen die Möglichkeit zu geben diese Daten zu kontrollieren. Jedoch bietet das öffentliche

Informieren darüber welche Daten gesammelt werden dem Benutzer die Möglichkeit sich in vielen Fällen bewusst dagegen zu entscheiden. Würden Benutzer eines Besprechungszimmer darüber informiert werden welche Daten in diesem Besprechungszimmer erfasst werden, könnten Benutzer, die damit nicht einverstanden sind, das Besprechungszimmer verlassen oder die Besprechung könnte an einen anderen Ort verlegt werden. Auch könnte man diese Informationen vorab weiterleiten, sodass ein passender Ort gefunden werden kann.

5.1.7 Durchsetzen

Nachdem ein Lösungsansatz gefunden wurde um den Datenschutz in intelligenten Gebäuden einzuhalten, ist es möglich eine Methodik zu entwickeln den Datenschutz einzuhalten und es besteht auch die Möglichkeit diese Methodik durchzusetzen. Beispielsweise könnten man Beauftragte anstellen, die in regelmäßigen Abständen überprüfen ob nicht genehmigte Sensoren angebracht wurden beziehungsweise ob alle genehmigten Sensoren noch funktionsfähig sind. Damit kann ausgeschlossen werden, dass nicht genehmigte Daten von neuen Sensoren erfasst wurden. Außerdem stellt man so sicher, dass Benutzer korrekt informiert werden, welche Daten erfasst werden. Sollte ein Sensor defekt sein und man würde den Nutzer informieren, dass diese Daten gesammelt werden, würde man dem Nutzer ohne das Erfassen dieser Daten die Kontrolle entziehen. Auch könnten diese Beauftragten überprüfen ob Zutritts- und Zugangskontrollen richtig umgesetzt wurden und die Datenverarbeitungsanlagen gesetzeskonform gehandhabt werden.

5.1.8 Demonstrieren

Auch das „Demonstrieren“ könnte zu Problemen führen, da Lösungsansätze zur Einhaltung der Datenschutzgesetze in intelligenten Gebäuden mit hoher Wahrscheinlichkeit nicht verständlich für jeden sein werden und somit eine Demonstration und Erklärung schwer möglich wird. Außerdem müssten Umsetzungen, die ein anschauliches und verständliches Erklären ermöglichen, bei jeder kleinen Änderung des Systems aktualisiert werden und es müsste erneut erfasst werden ob diese neue Umsetzung allgemein verständlich ist. Auch ist in den meisten Fällen die Reichweite von Problemen schwer abzuschätzen, da selbst ein kleines Problem riesige Auswirkungen haben kann.

Im Allgemeinen lässt sich sagen, dass eine Abdeckung aller acht Strategien zwar umsetzbar ist, es jedoch noch einige Probleme zu überwinden gibt um dies zu erzielen.

5.2 Abdeckung vorhandener Problemlösungsansätze

An der Technischen Universität München wurde ein Ansatz für ein Energiemanagementsystem (EMS) entwickelt, das die Datenschutzgesetze, welche bei der Sammlung von Energiedaten Anwendung finden, einhalten soll. Dieses EMS deckt zurzeit einen Großteil von Hoepmanns Strategien ab. An Punkten wie „Informieren“, und „Demonstrieren“ muss in Zukunft jedoch noch gearbeitet werden. [11]

6. ZUSAMMENFASSUNG

Zusammenfassend ist zu sagen, dass das Thema Datenschutz in der heutigen Zeit ein sehr wichtiges und schwer umzusetzendes Thema darstellt. Auch wenn die Einführung von „Smart Grids“ und der Ausbau und Bau von „Smart Buildings“ für die Zukunft meiner Meinung nach der einzig richtige Weg ist, um eine energieeffizienteres Netzwerk aufzubauen. Es müssen jedoch noch einige Probleme überwunden werden. Ganz besonders das Informieren von Personen, deren Daten gesammelt wurden, stellt zur Zeit noch ein Problem da. Ein gute Möglichkeit auf den laufenden zu bleiben was das Thema Datenschutz bei „Smart Grids“ und „Smart Buildings“ betrifft, ist den „Smart Grid“ Aufbau in Großbritannien zu verfolgen, wo zur Zeit Vorschläge zu diesem Thema eingeholt werden.[2]

7. REFERENCES

[1] Bundesnetzagentur, Eckpunktepapier - "Smart Grid" und "Smart Market", Dezember 2011, Online verfügbar unter http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/NetzentwicklungundSmartGrid/SmartGrid_SmartMarket/smartgrid_smartmarket-node.html, Letzter Aufruf am 2014/12/17

[2] Department of Energy & Climate Change, Smart Grid Vision and Routemap, February 2014

[3] The Climate Group. Smart Report 2020. Enabling the low carbon economy in the information age, 2008 Online verfügbar unter http://www.smart2020.org.

[4] Dominik Blunshy, Smart Buildings Einsatz von ICT in Gebäuden zur Steigerung der Energieeffizienz., 2010

[5] Siemens, Smart buildings - the future of building technology, 2010, Video online verfügbar unter https://www.youtube.com/watch?v=gCuPx9shWT0

[6] Sean Barker, Aditya Mishra, David Irwin, Emmanuel Cecchet, and Prashant Shenoy, Jeannie Albrecht, Smart*: An Open Data Set and Tools for Enabling Research in Sustainable Homes, SustKDD 2012

[7] ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27.

[8] Gola/Schomerus BDSG, Bundesdatenschutzgesetz 10. Auflage 2010

[9] Charta der Grundrechte der europäischen Union, (2010/C 83/02)

[10] Jaap-Henk Hoepman. Privacy design strategies, 2012. Online verfügbar unter http://arxiv.org/abs/1210.6621; Letzter Aufruf am 2014/12/18.

[11] Holger Kinkelin, Marcel von Maltitz, Benedikt Peter, Cornelia Kappler, Heiko Niedermayer, Georg Carle. Privacy Preserving Energy Management, 2014, Online verfügbar unter http://idem-project.de/downloads.php; Letzter Aufruf am 2014/12/18