Sicherheit und Datenschutz im Smart Metering

Martin Rost, Unabhängiges Landeszentrum für Datenschutz, Kiel

(Dieser Text enthält eine überarbeitete Fassung sowohl eines Vortrags als auch des daraus publizierten Beitrags für die Fachkonferenz „Sicherheit und Datenschutz bei Smart Energy“, die am 29. September 2011 in Berlin stattfand.)

Vorrede

Ich danke für die Einladung und auch für die warmen Worte bzgl. meiner doch zweifelsfrei schlechten Eigenschaft, in Vorträgen zu schnell zu sprechen, Herr Fox.

Vorweg: Sie reden hier vielfach von Sicherheit und Datenschutz…. Ich denke ich muss kurz sagen, was Datenschutz ist. Ich glaube, dass man noch viel tun muss, damit es überhaupt ein klares Verständnis von Datenschutz gibt, warum man Datenschutz bspw. nicht in Datensicherheit auflösen kann, dass die Herstellung von Datenschutz gegenüber Datensicherheit eine eigene Dimension ist. Hier haben die Datenschützer aber auch eine Bringeschuld einzulösen, diesen Unterschied zwischen Datensicherheit und Datenschutz klar zu markieren. Deshalb nun zum Einstieg die Bestimmung des Objektbereichs, dem Datenschutz sich widmet.

Was meint Datenschutz?

Datenschutz beobachtet die asymmetrische Machtbeziehung zwischen Organisationen und deren Personen. Im Außenverhältnis von Organisationen und Personen sind die Organisationen dabei in der Regel ungleich mächtiger, ihre Interessen durchzusetzen. Sie verfügen operativ über sehr viel mehr IT-Power, geben die Automatismen und Datenfelder vor und verfügen zur Gestaltung der Kommunikationen und zur Bearbeitung von Konfliktfällen spezielle Expertisen. Konkret gewendet meine ich damit die Verwaltung und den Bürger, das Unternehmen und den Kunde, die verschiedenen Praxen der Dienstleistungen mit akademischem Hintergrund und deren Patienten, Mandanten, Klienten, Individuen, Subjekten, Menschen, Personen. Diese generischen Rollenkonzepte vom Bürger, Kunden, Patienten… Individuum enthalten die Freiheitsversprechen moderner Gesellschaften für Menschen. Datenschutz beobachtet nun, wie diese Versprechen in der Praxis von Organisationen tatsächlich eingelöst werden. Der Umgang mit den Folgen aus diesen asymmetrischen Machtverhältnissen muss dabei auf beiden Seiten, auf der Seiten der Organisation und auf der Seite der Person, in seinen Auswirkungen jeweils gesondert betrachtet werden, wenn das gesellschaftliche „Versprechen“ besteht, dass diese Machtasymmetrie eben nicht einfach nur zu konstatieren ist, sondern die schwächere Person darauf vertrauen darf, dass eine Organisation ihre Prozesse beherrscht und sich auf Fairness

verpflichtet hat. Das lässt sich mit den Mitteln der Datensicherheit allein nicht lösen. Da muss man in die Verfahren selber hinein gehen. Um es scharf zu formulieren: Eine auf Datensicherheit zielende Betrachtung übernähme untergründig allein die Funktions- bzw. Sicherheitsinteressen der Organisationen.

Und im Innenverhältnis zwischen Organisationen und Personal haben wir den Mitarbeiterdatenschutz zu beachten. Hier kann wiederum durchaus eine einzelne Person, insbesondere als Mitarbeiter auf einer hohen Ebene der Entscheidungsgewalt, eine Organisation zerstören. Die größten Risiken gehen dabei sowohl vom Management als auch von der IT-Administration aus, die sozusagen die strukturell herausragenden Angreifer auf die operative Basis einer Organisation sind. Das ist aber eine andere Geschichte, die ich jetzt nicht weiter verfolgen möchte.

Unser Thema ist die Konditionierbarkeit der Beziehung und Interaktionen zwischen den IT-, Energie- und Access-Providern und deren Nutzern. Auch hier gibt es ein spezifisch zu betrachtendes, strukturell sehr tief greifendes asymmetrisches Machtverhältnis zwischen Organisationen und Personen. Denn man darf denke ich in Abwandlung eines Spruchs der Deutschen Bank sagen: Energie ist der Anfang von allem.

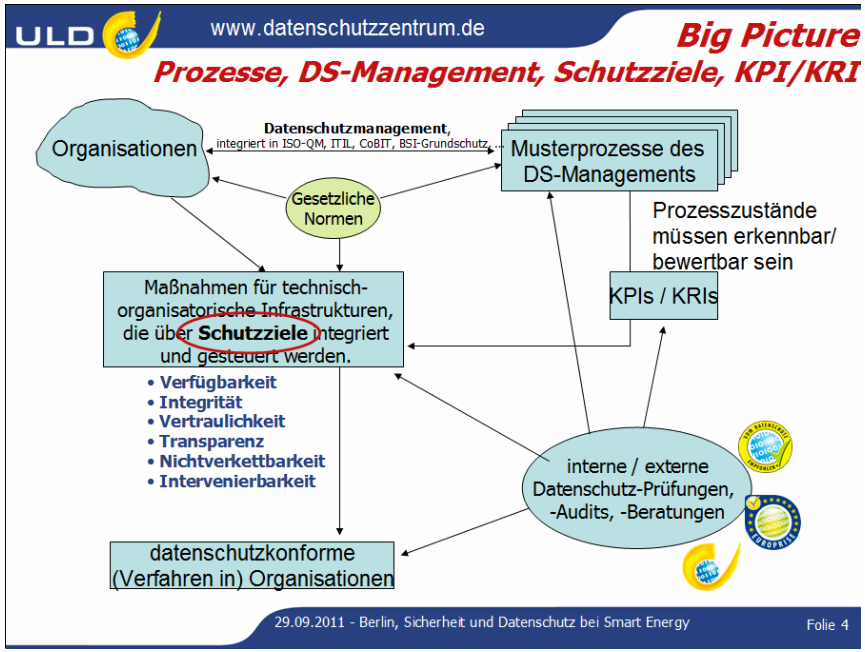
Datenschutz beobachtet die reale Ausgestaltung dieser asymmetrischen Machtverhältnisse zwischen Organisationen und Personen, zwischen Funktionen und Mechanismen der Datensicherheit und des Datenschutzes. Man hat es folglich mit einem Spannungsverhältnis zu tun. Um auch das so klar wie möglich auf den Punkt zu bringen: Aus der Sicht des Datenschutzes ist **jede Organisation ein Angreifer**. Grundsätzlich ist keine Organisation vertrauenswürdig, keine Verwaltung, kein Unternehmen, keine Praxis. Zumal Organisationen strukturell dazu gezwungen sind, bestimmten Funktionsimperativen einseitig zu folgen, wie dem nach der Aufrechterhaltung der gegebenen öffentlichen Ordnung und Sicherheit, der Optimierung der Kapitalverzinsung oder der absoluten Diskurshoheit in der Interpretation von Ausschnitten der Welt. Das sind alles strukturell eingebaute Monopolisierungstendenzen, die immer einzurechnen sind, die immer einer Nachregulation bedürfen. Und die sich an der Art des Zugriff auf Personen ablesen lassen. Aber davon hören Sie nur vergleichsweise wenig. Dagegen hören Sie sehr viel, so auch bei Gelegenheiten wie heute, den Risiken, die von betrügerischen Kunden und Mitarbeitern, externen Hackern und dem bereits angelaufenen Cyberkrieg ausgehen. Letzteres ist eine ganz andere Perspektive. Aus dieser Perspektive sind

es Personen, die nicht vertrauenswürdig sind. Vor Hackern Schutz zu gewähren ist nun diejenige der Datensicherheitsperspektive. Die Datensicherheit hat dafür zu sorgen, dass die Integrität der Prozesse von Organisationen gesichert ist, ebenso wie deren Verfügbarkeit und die Vertraulichkeit des wesentlichen Kerns des Produktionsprozesses einer Organisation. Gesellschaftlich ist die Umsetzung dieser Anforderungen unerläßlich. Datensicherheit ist wiederum die Basis dafür, dass Organisationen in einer Gesellschaft beherrschbar funktionieren können.

Dieses Auseinanderziehen von Datenschutz und Datensicherheit für die Aspekte einer intelligent gesteuerten Stromversorgung bedeutet beispielsweise, dass Sie erst einmal noch gar nichts für den Datenschutz tun, wenn Sie in ihrem System ganz viel für Datensicherheit machen, indem Sie bspw. mit SSL Verschlüsselungs- und Authentisierungsvorgänge die Interaktionen zwischen Client und Server absichern. Gleichwohl ist Datenschutz auf Techniken der Datensicherheit angewiesen. Ohne eine IT, die datensicher gefahren wird, kann kein Datenschutz sichergestellt werden. Insofern ist das Verhältnis von Datenschutz und Datensicherheit kompliziert, weil in bestimmten Aspekten sind Datensicherheit und Datenschutz zueinander komplementär und in anderen widersprüchlich.

The big picture

Auf der nachfolgenden Grafik sehen Sie das big picture, das heute moderne Datenschützer vor Augen haben, wenn Sie ihre Aktivitäten planen. Ich möchte diese Grafik nun nicht im Detail erläutern. Nur so viel: Wir gehen von den geltenden gesetzlichen Normen aus mit dem Ziel, Organisationen daran zu hindern, mit Personen als verfügbare Objekte beliebig umzuspringen. Dazu müssen Organisationen über ein Datenschutzmanagement verfügen, das über spezifische Schutzziele reguliert ist bzw. gesteuert wird.



Es ist dabei inzwischen unerlässlich, dass auch die Prozesse des Datenschutzmanagements per key performance indicators, oder noch besser: durch key risc indicators, wie sie im CoBIT-Paradigma vor gut zwei Jahren entwickelt wurden, kontrolliert würden. Damit der Nachweis geführt werden kann, dass Datenschutz umzusetzen tatsächlich zur Mehrwertschöpfung einer Organisation beiträgt. Und nicht nur kostet. Im Zentrum der Steuerung und Regulation der Datenschutzprozesse stehen dabei, ganz konventionell gedacht, Schutzziele. Diese sind auszuweisen. Es geht nicht um irgendwelche „Prinzipien“ oder nur normative formulierte Anforderungen, sondern darum, dass ganz konkret umsetzbare Ziele des Datenschutzes

ausweisbar sind, auf die hin Prozesse angepaßt werden können und für die eigens Controlling-Prozesse aufzusetzen sind.

Ich komme nun zur inneren Systematik der **Neuen Schutzziele**, die ich nachfolgend etwas näher im Detail ausleuchten möchte.

Die Systematik der Neuen Schutzziele

Wenn Sie sich Schutzziele speziell der Datensicherheit angucken, so kennen Sie die drei Standard-Schutzziele CIA, nämlich die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Diese wurden bspw. besonders prominent 1995 vom Department of Defense ausgeführt. Zur Systematik der Schutzziele hatte Prof. Andreas Pfitzmann, Inhaber des Lehrstuhls für Datensicherheit und Datenschutz an der TU-Dresden, in 2001 einen Aufsatz geschrieben. Danach kam der wissenschaftliche Diskurs in dieser Hinsicht etwas zur Ruhe. Gleichwohl stellte in einem 2008 verfassten internen Arbeitspapier Herr Pfitzmann dann aber überraschend fest, dass Verfügbarkeit und auch Vertraulichkeit sowohl komplementär zueinander - man muss immer beides zugleich von sicheren IT-Architekturen fordern – als

auch widersprüchlich sind. Ein Datum, das verfügbar sei, sei nicht mehr vertraulich und gleiches gälte umgekehrt. Diese strukturell gegebene innere Widersprüchlichkeit hatte Herrn Pfitzmann seit seinen Schutzziel-Untersuchungen so um das Jahr 2000 beunruhigt. Ich dagegen hatte, wenn ich als Prüfer oder Berater für IT-Systeme agierte, damals schlicht immer beide Schutzziele zugleich hochtreiben wollen, einfach weil ich den inneren Widerspruch zwischen den beiden Schutzzielen nicht gesehen hatte. Und als Praktiker vertraute ich darauf, dass die Verhältnisse zwischen den Schutzzielen theoretisch schon irgendwo geklärt sein dürften und man diese Schutzziele, und deren Schutzmaßnahmen einfach anwenden kann. Mir war nicht klar, dass man Schutzziele erst gegenseitig abwägen muss. Aber welche Schutzziele müssen es dann sein und warum? Ausgegangen waren wir damals von den drei, einfach unbestritten geltenden drei Standardschutzzielen der Datensicherheit.[1]

Jetzt frage ich Sie einmal pädagogisch hier in die Runde, wenn wir uns das Schutzziel Integrität vornehmen: Gibt es ein weiteres Schutzziel, das in einer gleichen Art wie zwischen Verfügbarkeit und Vertraulichkeit sowohl komplementär als auch widersprüchlich zur Integrität steht? Pfitzmann nennt diese Eigenschaft einer Relation ein Dual. Also erneut gefragt: Fällt Ihnen ein Dual zur Integrität ein? Das war die produktive Fragestellung, mit der uns Pfitzmann 2008 in seinem internen Arbeitspapier konfrontierte.

Die Antwort lautet: Intervenierbarkeit![2] Das soll heißen, dass in einen integer laufenden Prozess, idealer Weise also ein perfekter Automat, eingegriffen werden kann. Ein Eingriff macht die Perfektion dieses Automaten zunichte. Die Möglichkeit zum Eingriff bedeutet Angreifbarkeit der Integrität eines Prozesses. Aber man muss, wenn man ein System betreibt, in dieses eben auch eingreifen können, um dieses zu beherrschen, um es verändern zu können, wenn die Umwelt sich signifikant ändert. „Always be able to change a running system.“ Als Datenschützer ordne ich unter dieses Schutzziel dann zunächst einmal die Umsetzung der Betroffenenrechte auf Seiten einer Organisation ein. Wie kommt der Bürger, Kunde, Patient an die Daten heran, die eine Organisation von ihm speichert und verarbeitet? Und wenn ich eine Organisation dann noch tiefer gehend prüfe, dann verlange ich entsprechend der

[1] Diese Ziele galten als basale Schutzziele vernünftigerweise als irgendwie einfach gesetzt, alle anderen Schutzziele sollten aber in Bezug dazu gesetzt werden können.
[2] In der Diskussion wurde zunächst geprüft, ob Intrigität oder Kontingenz geeignet gewesen wären, das Dual zur Integrität zu bilden. Intrigität wäre kaum mehr ein schönes Wortspiel gewesen, Kontingenz ist dagegen ein Aspekt, der nicht auf Daten oder Information, sondern mehr auf das Umfeld, auf die Struktur eines Datenaustauschs oder der Beobachtung derselben paßte.

Zielvorgabe Intervenierbarkeit sicherzustellen, dass die Organisation sowohl über ein funktionierendes Projektmanagement als auch ein gesteuertes Configuration-, Patch-, Incident-, Problem- und vor allem Changemanagement verfügt. Organisation müssen wissen, was sie tun, damit sie angemessen sowohl auf die konkreten Einzelfälle von Personen als auch auf die Strukturaufgabe von Aufsichtsbehörden reagieren können.

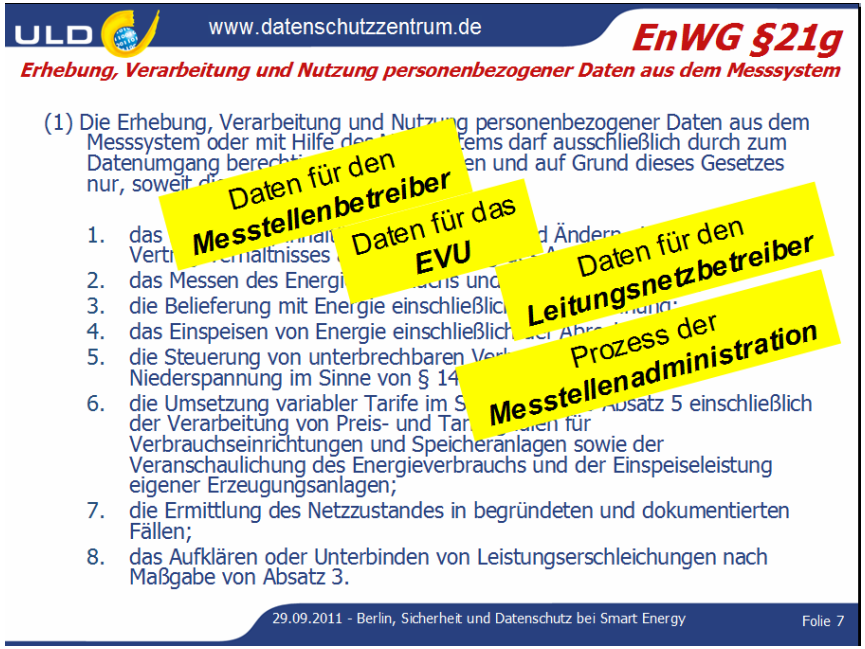
Wir bewegen uns allerdings bislang überwiegend noch im Bereich der Schutzziele, die primär zur Erreichung von Datensicherheit für Organisationen sind. Wie kommt nun der Datenschutz in den Gesamtaufriss? Wenn Sie in das Bundesdatenschutzgesetz hineinsehen oder in die Landesdatenschutzgesetze, dann finden Sie dort Vorgaben bzgl. der Kontrollierbarkeit von Prozessen, etwa was den Zugriff auf Systeme oder auf Applikationen angeht. Vorraussetzung für Kontrollierbarkeit ist insofern Transparenz. Organisationen, die personenbezogene Daten verarbeiten, müssen prüffähig nachweisen, dass sie ihre Prozesse beherrschen. Sie müssen dazu Transparenz herstellen können - für sich selber als Organisation; prüffähig aber auch für die Personen, deren Daten eine Organisation verarbeitet; und prüffähig für externe Aufsichtsinstanzen, mit denen nicht nur Rechnungshöfe oder Wirtschaftsprüfer, sondern auch die Datenschutz-Institutionen gemeint sind. Transparenz ist somit zweifelsfrei als ein eigens herauszuhebendes Schutzziel für IT-Infrastrukturen gesetzt wie die drei anderen Schutzziele der Datensicherheit. Somit stellt sich erneut methodisch die Frage: Wie lautet das Dual zu Transparenz?

Antwort: Nichtverkettbarkeit! Nichtverkettbarkeit bedeutet, dass Dinge nicht in Beziehung gesetzt werden, obwohl ihre Verkettbarkeit naheläge, also Objekte und Eigenschaften in Beziehung gesetzt werden könnten. Nichtverkettbarkeit ist, als Negation zur Transparenz, die Herstellung von gesicherter Intransparenz. Funktional betrachtet bietet Nichtverkettbarkeit den Vorteil, dass ein Fehler, der in einem System an einer Stelle entsteht, sich nicht trivial fortpflanzen kann, weil eine Grenze, etwa im Sinne einer Brandmauer, vorhanden ist bzw. gezogen wurde. Man muss eine solche Verkettungs-Grenze eigens konstruktiv aus einer übergeordneten strukturellen Logik heraus einziehen, gerade weil sie aus einer anderen Erwägung heraus nicht auf der Hand liegt. Nichtverkettbarkeit ist der operative Ausdruck für Grenzsetzungen, die am Markt als Konkurrenz oder die in der Sphäre der öffentlichen Verwaltung als Gewaltenteilung thematisiert wird. Aus rein technokratisch-organisatorischer Sicht sind diese Mechanismen vor allem eines: lästig und teuer. Damit sind wir am Kern der Funktionalität, der Dienstleistung, die der Datenschutz für die Gesellschaft leistet.

Datenschutz sorgt dafür, dass die Verarbeitung personenbezogener Daten durch Organisationen nur zugespitzt zweckgebunden geschieht bzw. geschehen soll. Ohne eine solche Grenze würde das Risiko bestehen, dass über diese Daten die parallel bestehenden Strukturierungsprinzipien der Gewaltenteilung, des Marktes und der freien Diskurse sozusagen einseitig von der Exekutive auf nur ein Ziel hin, nämlich allein das ihre, durchorganisiert werden. facebook und google machen derzeit genau das, im Kurzschluß personenbezogener Daten unterlaufen beide Markt, Gewaltenteilung und freie Diskurse.

Man muss beim Entwurf von IT-Systemen, das gilt insbesondere für eine gesellschaftlich abgestimmte intelligente Energiesteuerung, immer zumindest diese sechs elementaren Schutzziele gemeinsam betrachten und gegeneinander abwägen. Man kann dabei, wenn man weitere Regeln zulässt, aus diesen sechs elementaren Schutzzielen zu insgesamt 14 weiteren Schutzzielen kommen. Darauf möchte ich jetzt und hier aber nicht abstrakt weiter eingehen sondern stattdessen fragen, was hat man nun davon hat, wenn man im Bereich der Smart Energy mit dem Konzept der Schutzziele arbeitet.

Die Antwort liegt auf der Hand und zielt auf die innere Systematik und die Methodik ab. Man kann sich nämlich des bestehenden Methoden-Kanons etwa nach BSI-Grundschutz oder, speziell für das Datenschutzmanagement, der ISO27001 bedienen, die nur um zusätzliche, gesondert zu betrachtende Schutzziele zu erweitern sind. Und für die es dann Listen mit Maßnahmen gibt, mit denen die spezifischen Schutzziele des Datenschutzes auch für die Steuerung von Energieflüssen umsetzbar sind. Das Zusammenspiel der Steuerung der Energieversorgung und Datenschutz ist in einem ersten Ansatz im Energiewirtschaftsgesetz geregelt. Für den Datenschutz ist insbesondere der §21g EnWG heranzuziehen, der zwar noch sehr viele ganz wesentliche Fragen der Regelung offen lässt, aber aus dem immerhin deutlich wird, mit welchen Daten und Rollen bei Smart Metering und Smart Grid nun auf jeden Fall zu rechnen ist.

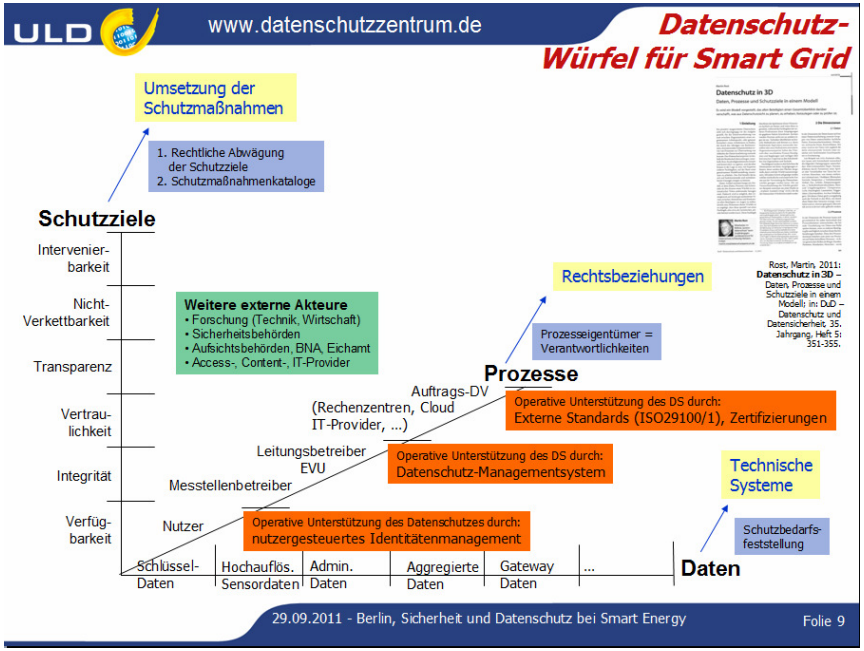


Bevor ich Ihnen das Modell, das wir mit diesen Angaben entwickelt haben, vorstelle, möchte ich noch eine Frage stellen, die bislang nirgends beantwortet wurde, die aber großen strukturellen Einfluß hat: Wem gehört das zentrale Kommunikations-Gateway, das ehemals als MUC bezeichnet wurde und für das das Protection Profile des BSI formuliert wurde? Man darf vermuten: Es gehört demjenigen, der das Garteway bezahlt. Ist die Option, dass der

Kunde das Gateway bezahlt in den Konzepten der Messtellenbetreiber oder Energielieferanten vorgesehen? Falls ja, dann wäre das operative Analogon zur Einwilligung in die Datenverarbeitung und Kommunikation zwischen Kunde und Organisation ein **Ein/Aus-Schalter**. Unabhängig von der Frage, wem das Gateway gehört muss es aus unserer Sicht in jedem Falle spätestens dann einen Ein/Aus-Knopf geben, wenn das Gateway bidirektionale und Fernwirkungs-Smart-Grid-Funktionalitäten beinhalten wird. Denn wenn ein Kunde bspw. mit seiner Lithium-Ionen-Batterie seines E-Mobiles selber zur kleinen EVU wird, dann haben wir es mit einer Rechtsbeziehung auf Augenhöhe zwischen dem Prosumer und der EVU zu tun. Wenn der eine von beiden Ein- oder Ausschalten können will, etwa wenn ein EVU säumige Kunden fernabschalten können möchte, dann muss es der andere grundsätzlich auch können, um als Energieproduzent eine unfair agierende, etwa falsch abrechnende EVU stoppen zu können. Sie sehen, dass ich hier entsprechend der Anforderung argumentiere, die sich aus der Berücksichtigung der Schutzziele Transparenz und Intervenierbarkeit ergibt.

Datenschutzwürfel für Smart Grid

Kommen wir nun zu unserem Modell, in dem das gesamte System der Energiesteuerung auf einer gleichmäßigen Granularität dargestellt ist, mit der sowohl Techniker als auch Juristen als auch Betriebswirte etwas anfangen können sollen. Dieses Modell ist eine Arbeitsgrundlage, mit der wir das Protection Profile des BSI analysiert haben und mit dem wir bis zum Ende diesen Jahres noch Usecases entwickeln werden, um mit deren Hilfe klären zu können, welche Daten dabei zu welchem Zweck von wem wohin fließen müssen.



Wir haben in der Y-Achse die Schutzziele, die ich eben erläutert habe. Wir haben in der Z-Achse die Prozesse und Rollen abgebildet. Und wir haben in der X-Achse die Daten, die bei Smart-Metern prozessiert werden könnten, bei Smart-Grid kämen noch Steuerungsdaten zum Fernwirken hinzu, die per se einen mehr als nur hohen Schutzbedarf hätten.

Die Z-Achse der Prozess- und Rollendimension schlüsselt sich in drei Domänen auf: Es gibt den einzelnen Nutzer, also konkret den Haushalt. Dann haben wir als zweite Domäne die Leitungsbetreiber, die Messstellenbetreiber, die Energielieferanten. Und wir haben drittens die Dienstleister der Dienstleister. Man denke hier an Cloudbetreiber, Rechenzentren oder generell IT-Dienstleister (Hardware- und Software-Hersteller, IT-Wartungsarbeiten), die für die Organisation aus der zweiten Domäne, etwa im Rahmen einer Auftragsdatenverarbeitung agieren.

Auf der Y-Achse, also der Dimension der Daten, sind verschiedene Datentypen unterscheidbar. Ich habe hier versucht, die Daten von vermutlich sehr hohem Schutzbedarf zu normalem Schutzbedarf anzuordnen. Methodisch entscheidend ist nun, dass man entsprechend der BSI Grundschutzmethode den Schutzbedarf dieser Daten ermittelt und

diesen Schutzbedarf der Daten dann vom dem gesamten technisch-organisatorischen System, mit dem diese Daten verarbeitet werden, geerbt wird. Wir müssen vermuten, dass wir stellenweise sehr hohen Schutzbedarf bei Smart Metering und auf jeden Fall bei Smart Grid haben werden. Also: Dieser sehr hohe Schutzbedarf vererbt sich somit auf das gesamte System, also auch auf das gesamte Rechenzentrum in der dritten Domäne der Prozess-Dimension. Methodisch heißt es für den Entwurf einer Smart-Metering-Architektur, mit der Ermittlung zunächst der Datentypen zu beginnen und deren Schutzbedarf festzulegen, um die nötige Sicherheit und Datenschutz der IT-Komponenten entsprechend konzipieren zu können.

Auf der Z-Achse haben wir die Prozess-Eigentümer, können also Rechtsbeziehungen und Verantwortlichkeiten für Prozesse abbilden. Die Beteiligten bekommen ihre Rolle vor Augen geführt und können anhand der von ihnen genutzten Daten sowie den Schutzzielen, die für sie von besonderer Bedeutung sind, ermitteln, was sie in ihrer Rolle konkret, aus Sicht der Datensicherheit und des Datenschutz, tun müssen.

Die Dimension der Schutzziele unterliegt der Abwägung unter Einbeziehung insbesondere juristischer Intelligenz. Denn die Schutzziele haben generell die Funktion, rechtliche Anforderungen methodisch in technisch-organisatorische Maßnahmen transformierbar zu machen. Die Schutzziele sollen die Anforderungen des Datenschutzes in Deutschland operationalisieren. Zur Organisation des Zusammenspiels von Juristen, Technikern, Organisationsexperten und Betriebswirten benutzt man dann typischerweise eine „Gardner Spinne“, in der die Intensität der Umsetzungen der Schutzziele abgetragen und dann im Gesamtbild diskutiert wird. ob es ein bisschen mehr oder weniger Verfügbarkeit, Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit sein darf. Entsprechend kann der Kaufmann dann, anhand der von den Schutzzielen dirigierten Schutzmaßahmen, mit dem Kalkulieren beginnen.

Wenn die Bedeutung der Schutzziele auf die konkret anstehende Herausforderung geklärt ist und diese gegeneinander abgewogen sind, und dann das Maß der Intensität, mit der ein Schutzziel umzusetzen ist, bekannt ist, dann kennt man gemäß BSI Methodik auch die dazu gehörige Maßnahme(n). Die fallen nämlich aus der Tüte, sobald der Prozess des Abwägens beendet und eine Festlegung erfolgt ist. Man weiß, wie man die Integrität von Daten prüft, indem man Hashwerte vergleicht. Festzulegen ist, welche Daten wie und wie häufig von welcher Instanz dazu zu ermitteln und letztlich zu bewerten sind. Man weiß, wie man

verschlüsselt, man weiß auch, wie Transparenz und Nichtverkettbarkeit zu sichern ist. Um ein Beispiel für eine Maßnahme für Nichtverkettbarkeit zu nennen: Mit anonymen Credentials lässt sich sozusagen direkt eine Berechtigung nachweisen, die bspw. mit der Volljährigkeit zu tun hat, ohne dass dafür das Geburtsdatum zu nennen ist und ohne dass verschiedene Akte des Nachweises untereinander noch in Beziehung gesetzt werden können. Letzteres ist der eigentliche Clou anonymer Credential, weil ein solches Credential nach jeder Nutzung seine Gestalt ändert. Diese Techniken bzw. deren Einsatzszenarien sind sicher noch ungewohnt. Es klingt kompliziert in der Anwendung, aber ist es nicht wirklich. Entsprechende Entwicklungen wie U-Prove von Microsoft oder idemix von IBM stehen seit vielen Jahren zur Verfügung.[3]

Es ist außerdem noch auf weitere externe Akteure hinzuweisen, auf die auch Herr Hornung bereits hinwies, die in der Prozess- und Rollen-Dimension hier bislang nicht auftauchten, aber bei Smart-Meter eine latente Rolle spielen. So gilt es bspw. an Sicherheitsbehörden, die ebenfalls auf Smart-Meter Daten Zugriff haben wollen, zu denken. Zumindest dann, wenn wir einen Tick weiter in Richtung Smart Grid gehen: Kurz bevor eine Wohnung gestürmt wird, macht es vermutlich guten Sinn, diesem Haushalt den Strom zu entziehen. Eine Steuerprüfung könnte aus einem auffallenden Verbrauchsverhalten eines Haushalts Indikatoren gewinnen, dass ein Haushalt ein Profil wie ein Gewerbebetrieb aufweist. Ich halte es für durchaus legitim, dass solche Aktivitäten stattfinden. Was ich allerdings möchte ist, dass all diese Interessen an den Metering-Daten transparent gemacht und die Zugriffsmöglichkeiten unter rechtstaatlich kontrollierte Bedingungen gestellt werden. Um noch einen besonders heiklen Player zu nennen: Die Sozialforschung interessiert sich notorisch für diese Daten des Alltagslebens, zu vollkommen unbestimmten Zwecken. Letztlich wird all das, was facebook an Überwachung der Menschen bislang noch nicht gut zu fassen bekommt, dann von den Profilen des Smart Metering, der Home-Automation oder des Ambient Assistant Living erledigt. Am absehbaren Ende stünde der gläserne, voll vermessene Mensch, der sich in all seinen Aktivitäten, die nicht vollkommen auf den absehbaren Pfaden statistischer Normalität liegen, rechtfertigen müssen.

[3] Die datenschutzfördernde Technik sogenannter attribut-basierter Zertifikate („attribute-based credentials“) wird in dem von der EU geförderten Projekt ABC4Trust (www.abc4trust.eu) in einem Credential-System mit Pilotversuchen erprobt, das auf die Technologien von Microsofts U-Prove und IBMs Identity Mixer aufbaut. Diese ermöglichen es, genau die notwendigen Eigenschaften und Angaben nachzuweisen, ohne dabei die vollständige Identität zu offenbaren.

Gegen diese Entwicklung und zum Schutz der Menschen ließen sich in den drei Prozess-Domänen, die ich oben im Würfel-Modell in der Z-Achse auswies, Datenschutz-verbessernde Techniken einsetzen. Da wurde in Deutschland, insbesondere mit Hilfe von EU-Geldern, bereits vieles in den letzten Jahren entwickelt. Ich denke etwa an das nutzerkontrollierte Identitätenmanagement Typ 3, dessen wesentliche Funktionalität darin besteht, nichtverkettbare Pseudonyme und Credentials verschiedener Qualitäten zu erzeugen bzw. zu verwalten. Das Schöne am BSI-Protection-Profile für das Smart-Meter-Gateway besteht darin, dass man mit dem Gateway tatsächlich die für ein wirkungsvolles Identitätenmanagement relevanten Transaktionspseudonyme erzeugen kann. Das Kommunikations-Gateway bietet allein für sich genommen noch nichts für einen wirksamen Datenschutz, es steht aber zumindest auch nicht im Wege. Das ist schon viel.

Das Wesentliche, was wir in der Domäne 2 auf Seiten der EVU brauchen, ist ein gesteuertes Datenschutzmanagement. Die Energielieferanten, Verteilnetz- und und Messstellenbetreiber müssen nachweisen, dass sie ihre Prozesse der Datenverarbeitung geprüftermaßen beherrschen und dass sie an Fairness orientiert sind. Fairness heißt zunächst einmal nicht mehr, als dass sie sich einfach nur an Gesetze halten und das auch nachweisen können.

Und wir brauchen natürlich operativ gewendete Datenschutzstandards sowie externe Datenschutz-Audits, gerade auch für die Industrie. Auf uns zukommen werden absehbar wohl die ISO29100 und 101, die ein international abgestimmtes privacy-framework bzw. privacy-controls bieten. Darauf wollte ich Sie am Ende jetzt nur hingewiesen haben. Entscheidend ist, dass diese drei Mechanismen, nämlich Identitätenmanagement, Datenschutzmanagement sowie externe Auditierungen implementiert und aufeinander abgestimmt werden müssen, damit es nicht zum gläsernen Menschen kommt, der mehr oder weniger subtil, aber im Ergebnis doch eindeutig, von den großen Organisationen ferngelenkt wird.

Ich danke Ihnen für Ihre Aufmerksamkeit.