Weiter können – basierend auf ISO/IEC 27018 – zielgerichtet und schnell Vergleiche zwischen den verschiedenen Cloud-Anbietern gemacht werden, die dem jeweiligen Kunden einen sicheren Rahmen für seine Cloud-Aktivitäten bieten.

Was wird die Zukunft bringen?

Der Schutz personenbezogener Daten ist und bleibt ein zentrales Thema in der Cloud. Heute schon ist ein deutlich gestiegenes Problembewusstsein sowohl aufseiten des Anbieter wie auch des Kunden zu erkennen und es ist davon auszugehen, dass Weiterentwicklungen der bestehenden Normen diesen Trend unterstützen werden. Hierbei werden die Unterstützer dieser Normen Schritt für Schritt das Vertrauen in Cloud-Lösungen stärken und nachweisbaren „Privacy" (Datenschutz) für ihre Kunden bieten. ∎

Bedeutung der Internationalen Norm ISO/IEC 27018 im Kontext von Cloud-Lösungen

IT-Sicherheit

DATENSCHUTZ IM BEREICH DER „SMARTEN" LÖSUNGEN

Vom Smartphone bis hin zu „Smart Cities" – mit dem Einsatz moderner Informations- und Kommunikationstechnologie sollen intelligente Systeme dabei helfen, den Alltag einfacher, schneller, besser oder auch „nur" wirtschaftlicher zu gestalten. Dabei ist der Datenschutz eine der Achillesfersen aller so genannten „smarten" Lösungen[1]). Eine der grundlegenden Technologien der (neuen) smarten Anwendungen ist das Cloud Computing. Die neue Norm ISO/IEC 27018:2014 „Informationstechnik – Sicherheitsverfahren – Anwendungsregel für den Schutz von Personenbezogenen Daten (PII) in Public Clouds, die als PII Processor auftreten" (ein „Leitfaden für den Schutz personenbeziehbarer Informationen in Public Clouds für Datenverarbeiter") bietet Lösungen für Fragen des Datenschutzes im Cloud Computing und ermöglicht damit, viele der smarten Anwendungen auf ein sicheres Fundament zu stellen.

→ ***Prof. Dr. Knut Blind***
ist Leiter des Fachgebiets Innovationsökonomie an der Fakultät Wirtschaft und Management der Technischen Universität Berlin sowie Professor für Standardisierung in der Abteilung Technologie und Management der „Rotterdam School of Management" an der Erasmus Universität Rotterdam. Ferner ist er am Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) für Innovation und Technologietransfer zuständig.

Foto: Roman Konzack, CC-BY 3.0 de

→ ***Dipl.-Jur. Dipl.-Pol. Martin G. Löhe***
ist Wissenschaftlicher Mitarbeiter des Fachgebiets Innovationsökonomie an der Fakultät Wirtschaft und Management der Technischen Universität Berlin sowie Projektleiter am Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS) im Bereich eGovernment. Außerdem ist er Vorsitzender des Internet & Gesellschaft Collaboratory, einer Multistakeholder-Plattform zum digitalen Wandel in Politik und Gesellschaft.

Eigenschaften von Cloud Computing

Cloud Computing bedeutet, dass IT-Leistungen nicht auf einem leicht bestimmbaren Gerät – zum Beispiel dem Computer auf dem Schreibtisch – erbracht werden, sondern virtualisiert durch ein Netzwerk (Internet oder Intranet) verfügbar gemacht werden. So kann man die Speicherung von Daten „in die Cloud" verlagern oder Rechenleistung von einer Cloud abrufen, das heißt Programme ausführen. Cloud Computing ist dabei ein Trend, der sowohl für professionelle als auch für Privatanwender zunehmend an Bedeutung gewinnt. So greifen Unternehmen zum Beispiel auf „Software as a Service"-Dienste zurück, das heißt, Anwendungssoftware ist nicht auf dem Desktop-Computer gespeichert, sondern wird als Dienstleistung von einem Server abgerufen.

Je nach Gestaltung können sich unterschiedliche Vorteile für das Unternehmen ergeben, etwa weil für die Anwender weniger anspruchsvolle Hardware erforderlich ist oder dadurch, dass sich

[1]) Neben dem Datenschutz gehören weitere Fragen der IT-Sicherheit zu den neuralgischen Punkten, weshalb CEN, CENELEC und ETSI die gemeinsame Koordinierungsstelle Cyber Security Coordination Group (CSCG) geschaffen haben, vergleiche dazu *Jacumeit, Volker* (2014): „Computer- und Internetsicherheit", in DIN-Mitteilungen Dezember 2014, S. 6 bis 8.

die genutzte Software immer auf dem aktuellen Stand befindet. Außerdem ist Cloud Computing potenziell überall verfügbar, von wo aus man Zugriff auf das entsprechende Netzwerk (das heißt Internet oder Intranet) hat. Andererseits ist diese Netzwerkverfügbarkeit auch unbedingt erforderlich, das heißt, bei einer Cloud im Internet muss für eine ausreichende Bandbreite und Ausfallsicherheit der Internetverbindung gesorgt werden. Auch bei privaten Anwendungen hat das Cloud Computing seinen Siegeszug angetreten. So speichern viele Smartphones die Daten des Benutzers, also E-Mails, Kalendereinträge, Kontaktdaten, Fotos, Dokumente und so weiter in der Cloud. Von Vorteil ist, dass bei einem Verlust des Geräts nicht auch die Daten verloren sind. Andererseits gibt der Nutzer hier die Kontrolle seiner Daten aus der Hand.

Foto: unique3d – Fotolia.com

Intelligente Systeme sollen helfen, den Alltag einfacher, besser und schneller zu gestalten.

Aus wirtschaftlicher Perspektive verspricht Cloud Computing unter anderem Einsparungen durch Skaleneffekte und durch Outsourcing, weil benötigte Ressourcen in einem Pool (Cloud) konzentriert werden können und dieser von darauf spezialisierten Dienstleistern betrieben werden kann. Die Schaffung großer Datensammlungen, die durch das Cloud Computing vereinfacht werden, ist außerdem Voraussetzung für „Big Data" und die damit verbundenen Auswertungs- und Optimierungsmöglichkeiten. Für innovative und schnell wachsende Unternehmen sind agile und flexibel abrufbereite IT-Services oft erfolgsentscheidend. Kehrseite der Virtualisierung des Cloud Computings sind Herausforderungen für den Datenschutz. Zwar ist nicht immer der Anbieter eines digitalen Produkts (zum Beispiel einer Software) zugleich auch der Betreiber der zugrunde liegenden Cloud. Dennoch hat der Produktanbieter für das Funktionieren der Cloud – auch rechtlich – einzustehen. Doch wie kann der Nutzer einer Cloud oder der Anbieter eines Cloud-basierten Produkts sicher sein, welche Cloud er bekommt? Für den Markt von Cloud-Produkten ist es daher wichtig, dass Clouds bestimmte Datenschutzanforderungen erfüllen können, damit Haftungsfragen geklärt sind, Nutzer die Technologie akzeptieren und Cloud Computing seine ökonomischen Potenziale voll entfalten kann.

Entstehung von ISO/IEC 27018

Mit der neuen Norm ISO/IEC 27018 sollen diese Probleme gelöst werden. Dementsprechend sind auch die Ziele der Norm formuliert: Erstens sollen Anbieter von Cloud Computing dabei unterstützt werden, die Verpflichtungen, die sich aus der Rolle als Auftragsdatenverarbeiter von personenbeziehbaren Daten ergeben, zu erfüllen. Diese können zum Beispiel in Gesetzen oder Verträgen begründet sein. Zweitens sollen die Verfahren des Anbieters transparent gemacht werden. Drittens soll der Vertragsschluss zwischen Anbieter und Kunde vereinfacht werden und viertens soll die Überprüfung des Cloud-Anbieters bezüglich der Einhaltung von Compliance-Bedingungen so vereinfacht werden, dass diese durch Audits vorgenommen werden kann. Denn schließlich würde eine individuelle Überprüfung durch Kunden nicht nur technisch schwierig werden, sondern könnte selbst ein Risiko für die Sicherheit der Systeme darstellen.

Angelpunkt für ISO/IEC 27018 ist eine Vorschrift aus der Europäischen Datenschutzrichtlinie (95/46/EG), die in den jeweiligen nationalen Umsetzungen in allen europäischen Mitgliedsstaaten gilt. Dort heißt es in Artikel 17, dass derjenige, der für die Verarbeitung von Daten verantwortlich ist, geeignete Maßnahmen ergreifen muss, um Daten vor unberechtigter Änderung, Weitergabe, Zugang oder jeder anderen unrechtmäßigen Datenverarbeitung zu schützen. Das gelte insbesondere, wenn Daten in einem Netz übertragen werden. Wenn sich der Datenverarbeitungsverantwortliche dabei eines Auftragnehmers bedient, so muss er einen Anbieter auswählen, der entsprechende technische Sicherheitsmaßnahmen und organisatorische Vorkehrungen getroffen hat, und sich von deren Einhaltung überzeugen. Da Verstöße gegen geltendes Datenschutzrecht entsprechend sanktioniert werden, ergibt sich

[2] Article 29 Data Protection Working Party: „Opinion 05/2012 on Cloud Computing", 01037/12/EN, WP 196, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

für Unternehmen, die ihre Datenverarbeitung aus der Hand geben, ein besonderes Haftungsrisiko. Mit ISO/IEC 27018 soll es möglich werden, dieses Compliance-Problem zu lösen. Um die Anforderungen des europäischen Rechtsrahmens zu erfüllen, wurde mit der Norm eine Reihe von Maßnahmen definiert.

Dafür wurden zunächst die Gesetze identifiziert, die in der EU für die Cloud-basierte Datenverarbeitung von personenbezogenen Daten anwendbar sind. Im Zuge dessen wurden 70 neue „Controls", das heißt Maßnahmen für die Durchführung der Datenverarbeitung, geschaffen, die den Anforderungen der europäischen Gesetze entsprechen, wobei hier auch die Stellungnahmen der Datenschützer zu Cloud Computing berücksichtigt wurden. Die europäischen Datenschützer sind offiziell in der „Artikel-29-Datenschutzgruppe" organisiert, einer Gruppe, die durch den Artikel 29 der EU-Datenschutzrichtlinie geschaffen wurde. Sie besteht aus Vertretern der nationalen Datenschutzbehörden, des europäischen Datenschutzbeauftragten und der Europäischen Kommission. Die Gruppe prüft ständig die Umsetzung der Datenschutzrichtlinie, um zu einer einheitlichen Anwendung in Europa beizutragen. Sie untersucht aber auch das Schutzniveau in Drittländern und verfasst Stellungnahmen und Berichte zu allen anderen Fragen bezüglich des Datenschutzes in der Europäischen Union. Zum Cloud Computing hat sich die Artikel-29-Gruppe 2012 ausführlich in einer eigenen Stellungnahme geäußert[2]).

Die daraus abgeleiteten Anforderungen hat man dann mit den Inhalten von ISO/IEC 27002:2013 „Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen" verglichen. Diese Norm enthält umfangreiche Maßnahmen zur Informationssicherheit, ist jedoch weder spezifisch für Cloud Computing noch legt sie einen Fokus auf Fragen des Schutzes der Privatsphäre. Deshalb wurden in ISO/IEC 27018 erstens Richtlinien aufgestellt, wie die bereits in ISO/IEC 27002 bestehenden Sicherheitsmaßnahmen zum Schutz personenbeziehbarer Daten umgesetzt werden sollten. Zweitens wurden weitere – Cloud- und Privacy-spezifische – Maßnahmen in ISO/IEC 27018 definiert, ergänzt auch hier um Richtlinien zu deren Umsetzung. Grundlage für die Implementierung bietet dabei der Rahmen des bereits bestehenden Informationssicherheits-Managementsystems aus ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen".

Mit ihrem Anwendungsbereich ist ISO/IEC 27018 die erste Internationale Norm für Privatsphäre im Cloud Computing. Die Inhalte richten sich insbesondere an die Datenverarbeiter, das heißt die Anbieter von Cloud Computing. Die Compliance eines Cloud-Anbieters mit der Internationalen Norm – und damit mit den gesetzlichen Vorgaben – kann durch ein Audit festgestellt werden, das durch professionelle Zertifizierer durchgeführt werden soll. Kunden des Dienstes müssen also keine eigene Überprüfung durchführen und können eine unabhängige Bestätigung für die Erfüllung der Voraussetzungen der Norm erhalten.

Der besondere Vorteil einer Umsetzung von ISO/IEC 27018 ist, dass damit eine Rechtskonformität mit der EU-Datenschutzrichtlinie und den diese umsetzenden nationalen Regelungen – einschließlich der Safe-Harbor-Prinzipien – vermutet werden kann. Da die europäische Datenschutzregulierung als weltweit am strengsten gilt, werden Unternehmen, die ISO/IEC 27018-zertifizierte Cloud-Anbieter auswählen, auch mit Gesetzen außerhalb der EU kaum Compliance-Probleme erwarten können. Damit steht einer weltweiten Nutzung derselben zertifizierten Cloud aus Datenschutzperspektive nichts mehr im Wege, sodass die Vorteile des Cloud Computing global skalieren können.

Ziele und Maßnahmen von ISO/IEC 27018

Wie bereits erwähnt, besteht ISO/IEC 27018 aus zwei Teilen: Zum einen werden Maßnahmen aus ISO/IEC 27002 referenziert und um Hinweise für die Umsetzung bei der Verarbeitung auf Personen beziehbarer Informationen im Cloud Computing ergänzt. Zum anderen werden weitere spezifische Maßnahmen aufgelistet. Die Besonderheiten ergeben sich zum einen aus den sensiblen Daten und zum anderen daraus, dass es beim Cloud Computing gerade um die Verarbeitung von Daten im Auftrag geht (Zum Vergleich: Im Mittelpunkt der Informationssicherheits-Managementsysteme von ISO/IEC 27001 – grundlegend für die Normen der Reihe 27000 – steht der Schutz eigener Daten). Die Idee hinter ISO/IEC 27018 ist, den Schutz auf Personen beziehbarer Daten bereits bei der Konstruktion eines Cloud-Services zu berücksichtigen, weil das die Implementierung vereinfacht (so genanntes „privacy by design").

Im Rahmen der aus ISO/IEC 27002 referenzierten Maßnahmen mahnt ISO/IEC 27018 beispielsweise an, bei der Aufgabenteilung zwischen Cloud-Anbieter (als Datenverarbeiter) und Cloud-Kunde (als für die Datenverarbeitung Verantwortlicher) und gegebenenfalls Zulieferer die jeweiligen Zuständigkeiten explizit vertraglich zu regeln. Auch soll der Cloud-Anbieter dem Kunden einen Ansprechpartner speziell für die Angelegenheiten von auf Personen beziehbaren Daten benennen. Die Mitarbeiter des Cloud-Anbieters sollen zur Tragweite von Privatsphäreverletzungen für das Unternehmen, die Mitarbeiter und die Kunden (hier werden auch psychische Auswirkungen erwähnt) extra geschult werden. Auf technischer Seite sollen sichere Login-Verfahren angeboten werden und über die Nutzung von Kryptographie informiert werden. Zur Sicherheit sollten Speichermedien im Zweifel so behandelt werden, als enthielten sie personenbeziehbare Daten. Jeder Zugriff auf Daten soll protokolliert und diese Protokolle sollen gegebenenfalls Kunden zugänglich gemacht werden, wobei beachtet werden soll, dass Kunden nicht auf Protokolle zu Daten anderer Kunden zugreifen können.

Zur zweiten Gruppe, den für Cloud Computing spezifischen Maßnahmen, gehört zum Beispiel die Regelung, dass personenbeziehbare Daten nicht anders als vom Cloud-Kunden vorgesehen verarbeitet werden, insbesondere,

dass diese nicht durch den Cloud-Anbieter für Marketing und Werbung verwendet werden. Der Zugriff auf Daten durch Dritte darf durch dem Cloud-Anbieter nur gestattet werden, wenn er dazu rechtlich verpflichtet ist, und er soll den Kunden über derartige Vorgänge auch informieren (es sei denn, dass genau das verboten sein sollte). Die Einbindung von Dienstleistern durch den Cloud-Anbieter soll dem Kunden vorher angezeigt werden und, falls ein unautorisierter Zugriff auf Daten erfolgen sollte, soll das dem Kunden umgehend mitgeteilt werden. Außerdem sollen temporäre Daten regelmäßig gelöscht, Ausdrucke von Daten vermieden und über Netzwerke übertragene Daten verschlüsselt werden. Der Cloud-Anbieter soll außerdem angeben und dokumentieren, in welchen Ländern die personenbeziehbaren Daten gespeichert werden.

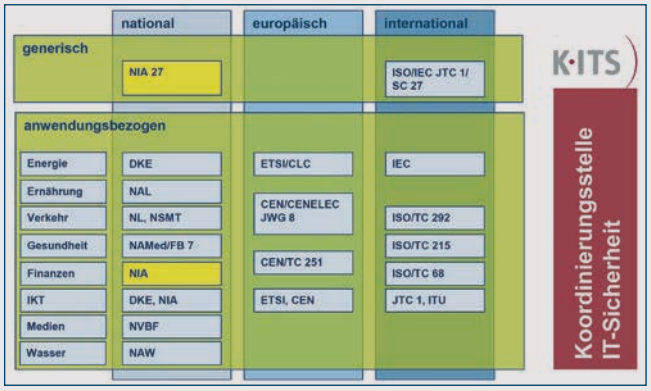
Das alles sind Beispiele für mögliche Maßnahmen. Aus dem sehr viel umfangreicheren Katalog wird für den konkreten Fall, das heißt für die jeweilige Konstellation des Cloud Computing, die konkrete Maßnahme ausgewählt werden müssen. Diese Auswahl wird unterschiedlich ausfallen je nachdem, um was für eine Cloud es sich handelt (zum Beispiel Software-as-a-Service oder Plattform-as-a-Service) beziehungsweise welche Rollen Cloud-Anbietern und Cloud-Nutzern zukommt (vergleiche dazu ISO/IEC 17789:2014 „Informationstechnik – Cloud Computing – Referenzarchitektur“) oder welche Art von Daten betroffen ist. Die dabei zu berücksichtigenden Anforderungen können von rechtlichen, regulatorischen oder vertraglichen Bedingungen ebenso abhängen wie von der Natur der Risiken (hierbei verweist die Norm auf ISO/IEC 27005:2011 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement“ und der geplanten ISO/IEC 29134 über Methoden der Datenschutzfolgeabschätzung oder von Unternehmensrichtlinien.

Bedeutung der Norm für Unternehmen und Innovationen

ISO/IEC 27018 trägt den veränderten Rahmenbedingungen, unter denen moderne IT-Services heute erbracht werden, mit einem umfangreichen Maßnahmenkatalog Rechnung. Mit dem Vormarsch des Cloud Computing lösen sich IT-Leistungen zunehmend von der Hardware und werden virtueller. Gleichzeitig müssen weiterhin rechtliche Anforderungen, aber auch die Wünsche der Kunden erfüllt werden können. Mit der neuen Norm ist es möglich, die Vorteile von Cloud Computing und der damit potenziellen weltweiten Skalierung zu nutzen – die Regelungen der Norm stellen Instrumente bereit, um Compliance- und Reputationskosten zu kontrollieren, die Transaktionskosten zwischen Kunden und Anbietern zu senken und für neue IT-getriebene Innovationsbereiche, zum Beispiel für Big-Data-Anwendungen oder internetbasierte Startups, eine sichere Basis zu schaffen. Nun ist es an den Cloud-Computing-Anbietern, ihre Prozesse mit ISO/IEC 27018 in Einklang zu bringen. Grundsätzlich können diese die durch die enge Abstimmung der Norm mit der EU-Datenschutzrichtlinie erlangte Rechtssicherheit nutzen, um sich im globalen Wettbewerb der Cloud-Computing-Dienstleistungen zu behaupten. Gleichzeitig besteht dadurch die Chance, die hohen Datenschutzanforderungen der EU auch global durchzusetzen.

Sicherheitsaspekte im Umfeld des E-Government

Das Thema IT-Sicherheit war in diesem Jahr auch Programmpunkt des 21. Berliner Anwenderforums „E-Government 2015“ der Firma INFORA in Berlin, das am 25. und 26. Februar stattfand. Unter der Überschrift „Normung und Standardisierung im IT-Sicherheitsumfeld – Einbindung deutscher Verwaltungen und IT-Unternehmen in die internationale Normung“ wurde vor dem Hintergrund, dass die Rückgewinnung von Vertrauen in die Anwendung von Informationstechnik eine Aufgabe ist, die kurzfristig und nachhaltig bearbeitet werden muss, den Teilnehmern des Anwenderforums nahegebracht, wie sich Verwaltungen und IT-Unternehmen – vor allem die, die ihre Leistungen im Rahmen von E-Government anbieten – hier beteiligen, um die deutschen Interessen auf europäischer und internationaler Ebene einzubringen.



IT-Sicherheitsnormung – Gremienübersicht

Die Notwendigkeit von internationalen Normen und Spezifikationen war zwar vielen Teilnehmern bewusst, jedoch wussten nur wenige, wie und wo hier Engagement deutscher Experten eingebracht werden kann. Nach dem Motto „Nicht zuschauen und meckern, sondern mitmachen“ wurden die Vorteile einer Beteiligung an der IT-Sicherheitsnormung anhand der aktuellen Themen erläutert.