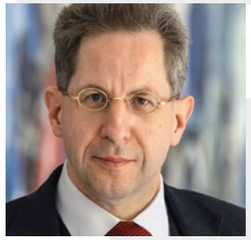
DATENSCHUTZ UND DATENSICHERHEIT BERICHT 2015

ERLEBEN, WAS VERBINDET.

REGELN
HONEYPOTS
SMARTPHONE
KRYPTOGRAFIE
INDUSTRIE 4.0
KONTROLLINSTANZ
BIG DATA
PASSWORT
VERNETZUNG
CLOUD-DIENSTE
CYBERSPACE
SPIONAGE
DATENSPARSAMKEIT
INTEGRITÄT
FIREWALL
GRUNDRECHTE
VERSCHLÜSSELUNG
REGELN
DDOS-ANGRIFF
VIRENSCHUTZ
SELBSTBESTIMMUNG
SICHERHEITSRICHTLINIE
IT-SICHERHEIT
REGELN
HONEYPOTS
HACKER
INDUSTRIE 4.0
VIRENSCHUTZ
SELBSTBESTIMMUNG
CYBER DEFENSE CENTER
PERSÖNLICHKEITSSCHUTZ

INHALT



DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

ELEMENTARER SCHRITT ZU FAIREM WETTBEWERB

Terror und die Flüchtlingskrise haben das Jahr 2015 geprägt. Ein Jahr, das in Bezug auf Datenschutz und -sicherheit wesentliche Änderungen gebracht hat. Die EU mag beim Umgang mit Flüchtlingen noch weit von einer Einigung entfernt sein. Beim Datenschutz ist ihr der Durchbruch gelungen: Die europäischen Institutionen haben sich auf eine Datenschutzgrundverordnung geeinigt. Das neue europäische Datenschutzrecht schafft ein hohes Datenschutzniveau und ermöglicht neue digitale Geschäftsmodelle. Entscheidend ist, dass es jetzt konkrete Regeln, zum Beispiel zur Pseudonymisierung, gibt. Eine wichtige Rolle spielt zudem der Aspekt, dass die europäischen Datenschutzregeln für alle Unternehmen gelten, wenn sie ihre Dienste hier anbieten wollen. Das ist ein elementarer Schritt auf dem Weg zu fairen Wettbewerbsverhältnissen zwischen hiesigen Telekommunikations- und großen Internetunternehmen aus Übersee.

Die transatlantischen Beziehungen beeinflusst hat auch die Entscheidung des Europäischen Gerichtshofs, das Safe-Harbor-Abkommen mit den USA auszusetzen. Das Gericht hat klargestellt: Die Daten europäischer Bürger sind in den Vereinigten Staaten derzeit nicht ausreichend geschützt. Von der Aussetzung ist die Telekom kaum betroffen. Wir verarbeiten grundsätzlich keine Daten aus Europa in Übersee. Wenn große Unternehmen wie Microsoft ihre Daten lieber in unseren deutschen Rechenzentren speichern, können wir von der Entscheidung des Gerichtshofs sogar profitieren.

„DIE DEUTSCHE TELEKOM VERARBEITET GRUNDSÄTZLICH KEINE DATEN AUS EUROPA IN ÜBERSEE."

In Deutschland ist zudem das IT-Sicherheitsgesetz in Kraft getreten, das höhere Schutzanforderungen und Meldepflichten bei Angriffen vorschreibt. Erfreulich ist, dass auch Hard- und Softwarehersteller sowie Dienstanbieter einbezogen werden. Derzeit wird auf europäischer Ebene ebenfalls eine Richtlinie dazu erstellt. Wir müssen darauf achten, dass auch dort die gesamte Wertschöpfungskette berücksichtigt wird. Nur so erreichen wir wirklich mehr Sicherheit.

Heftig umstritten war die Wiedereinführung der Vorratsdatenspeicherung, die der Bundestag beschlossen hat. Wir als Telekom können nicht wirklich beurteilen, wie sehr Strafverfolgungsbehörden auf diese Daten angewiesen sind. Es liegt an den Behörden, das möglichst transparent zu machen, um die Bürger von der Sinnhaftigkeit zu überzeugen. Die Politik hat die heikle Aufgabe, Freiheits- und Persönlichkeitsrechte gegenüber Sicherheitsbedürfnissen abzuwägen. Grundsätzlich gilt: Unter dem Eindruck von Terroranschlägen steigt die Bereitschaft, Freiheitsrechte zugunsten von mehr Sicherheit einzuschränken. Bei der Abwägung muss aber die Balance gewahrt bleiben: Wir verteidigen unsere Freiheit nicht, indem wir sie aufgeben.

Dr. Thomas Kremer

ist seit Juni 2012 Vorstandsmitglied Datenschutz, Recht und Compliance der Deutschen Telekom. Zuvor arbeitete der Jurist als Generalbevollmächtigter für die thyssenkrupp AG, wo er 2003 die Leitung des Rechtsbereichs übernahm. 2007 ernannte ihn der ThyssenKrupp Konzern zum Chief Compliance Officer.

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

AM ANFANG EINER MODERNEN DATENPOLITIK

DATENSCHUTZ UND DATENSICHERHEIT WAREN IM JAHR 2015 GEGENSTAND VIELFÄLTIGER GESETZGEBERISCHER TÄTIGKEITEN: IN DEUTSCHLAND DAS IT-SICHERHEITS-GESETZ, IN DER EU DIE NIS- UND PNR-RICHTLINIEN SOWIE DIE DATENSCHUTZGRUNDVERORDNUNG.

Auf nationaler Ebene trat im Juli 2015 das IT-Sicherheitsgesetz in Kraft. Mit dem Gesetz werden die Betreiber kritischer Infrastrukturen aus Bereichen wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet, Mindeststandards einzuhalten. Auf EU-Ebene einigten sich Europäisches Parlament und Rat der Europäischen Union im Dezember 2015 auf die NIS-Richtlinie. Darin werden – dem nationalen IT-Sicherheitsgesetz vergleichbar – Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der EU getroffen.

Eine politische Einigung gab es im Dezember 2015 weiterhin in Bezug auf die Datenschutzgrundverordnung. Diese wird das Datenschutzrecht EU-weit vereinheitlichen und die Rechte der Betroffenen stärken. Außerdem steht auch die Datenschutzrichtlinie für die Datenverarbeitung durch Polizei und Justiz kurz vor ihrer Verabschiedung.

Schließlich fanden das Europäische Parlament und der Rat einen Kompromiss bei der PNR-Richtlinie. Diese regelt die Übermittlung von Fluggastdaten durch die Fluggesellschaften an die EU-Mitgliedstaaten und die Verarbeitung dieser Daten durch die Mitgliedstaaten zu Strafverfolgungszwecken. Die bloße Zahl der gesetzgeberischen Aktivitäten ist beeindruckend. Die Geschwindigkeit, in der sich die technologische Entwicklung vollzieht, erzeugt allerdings auch erheblichen Handlungsdruck.

Die Politik muss jedoch nicht auf jede Modeerscheinung des digitalen Lebens reagieren, denn davon gibt es viele. Nach „Internet 2.0“ und „Internet 3.0“ kam „Internet 4.0“, dem „Cloud Computing“ folgten das „Internet der Dinge“ und „Industrie 4.0“, nach „Big Data“ kommt „Big Data for Good“ und „Behavioral Tracking und Targeting“ sowie „Predictive Analytics“ schließt sich jetzt „Artificial Intelligence“ an. Selbst wenn hinter diesen Schlagwörtern jeweils gewaltige Herausforderungen für den Einzelnen und für die Gesellschaft stehen: Es bedarf einer sorgfältigen und kühlen Analyse der Frage, ob im Einzelfall ein Eingreifen der Politik erforderlich ist.

Ich habe schon immer die Auffassung vertreten, dass in der digitalen und in der analogen Welt prinzipiell dieselben Wertungen vorgenommen werden müssen. Abgesehen davon, dass eine scharfe Entgegensetzung von „online“ und „offline“, von „digital“ und „analog“ ohnehin überholt sein dürfte, müssen hier wie dort derselbe Zugang, dieselben Methoden, dieselben Bewertungen, dasselbe Staatsverständnis und dasselbe Grundrechtsverständnis gewährleistet sein. Natürlich benötigt man im Internet zum Teil andere Regelungsmechanismen, andere Instrumente. Prinzipiell lehne ich es jedoch ab, zu sagen, dass die Onlinewelt einen eigenen, in sich geschlossenen Regulations- und Wertemechanismus braucht. Will man die Herausforderungen der Zukunft an einem Begriff festmachen, der über allem zu stehen scheint, dann ist dies der Begriff der Daten.

Wir finden ihn in „Datensicherheit“ und in „Datenschutz“, in „Big Data“ und in „Open Data“. Daten seien, so wird behauptet, die neuen Treiber der Wirtschaft. Die Digitalisierung führe zur Datafizierung, also zur Umwandlung vieler Aspekte des menschlichen Lebens in messbare und durch Algorithmen analysierbare Aussagen über uns. Manche sehen dadurch das zweite Zeitalter der Aufklärung heraufziehen. Nach dem Wissen über die Dinge folge jetzt die Erlangung der Macht über die Dinge durch Daten und Vernetzung. Anderen macht diese Entwicklung Sorgen und sie fürchten nichts weniger als den Verlust menschlicher Freiheit durch die Datafizierung des Menschen.

Es steht außer Zweifel, dass das einzelne Datum beziehungsweise „die Daten“ neben der Vernetzung in den Mittelpunkt des Interesses von Wirtschaft, Wissenschaft und Politik geraten sind. Es ist daher auch an der Zeit, sich über eine kohärente Datenpolitik Gedanken zu machen. Datensicherheit und Datenschutz werden dabei gemeinhin als zwei Seiten einer Medaille angesehen. Doch eine vernünftige Datenpolitik muss den Blick weiten für weitere Fragen jenseits der hergebrachten Konzepte von Datenschutz und Datensicherheit: Welche Rechte an Daten soll es geben, wenn Daten als Wirtschaftsgut anzusehen sind?

Wir kennen heute noch kein Eigentum an Daten. Nur im Urheberrecht gibt es Rechte an Sammelwerken und an Datenbankwerken, weil die Auswahl oder Anordnung der Daten hier eine persönliche geistige Schöpfung darstellt. Außerdem können Daten wettbewerbs- und strafrechtlich als Geschäfts- oder Betriebsgeheimnis geschützt sein und damit einer Nutzungsbeschränkung unterliegen. Im Übrigen aber gibt es keine Eigentumsordnung in Bezug auf Daten. Lediglich in Bezug auf die Meinungs-, Presse- und Informationsfreiheit existiert eine Kommunikationsordnung und in Bezug auf den Datenschutz gibt es Verarbeitungsbeschränkungen.

Die gegenwärtigen Regeln sind aber nicht in Stein gemeißelt und sie reichen womöglich nicht aus, um die Herausforderungen der digitalen Welt zu meistern. Im Internet der Dinge (zum Beispiel beim autonomen und vernetzten Fahren) stellen sich komplizierte Fragen der Zuordnung und des Zugangs zu Fahrzeug-, Maschinen-, Sensor-, Netz- und Gebäudedaten sowie der Verantwortlichkeit. Dasselbe gilt für komplexe Onlineakteurnetzwerke, in denen Plattformbetreiber, Cloud-Anbieter und die verschiedensten Nutzer zusammenwirken.

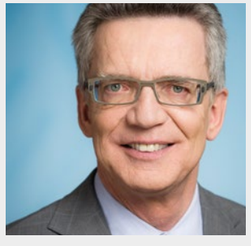
Insbesondere im Datenschutz besteht entgegen der technologischen Entwicklung die Tendenz, Daten wie Gegenstände zu behandeln, die der Betroffene jederzeit zurückholen und gegen deren Verarbeitung er jederzeit widersprechen kann. In diese Richtung gehen auch Vorschläge, personenbezogene Daten kommerzialisierbar zu machen – etwa analog zu den Nutzungsrechten im Urheberrecht. In die entgegengesetzte Richtung geht die „Open Data“-Bewegung. Diese will Daten von Besitzansprüchen befreien. Unter dem Stichwort „Open Private Data“ wird sogar von einer Datenabgabepflicht Privater gesprochen. Selbst die gerade ausgehandelte Datenschutzgrundverordnung enthält schon in ihrem Titel zwei Ziele: den Schutz des Einzelnen und den freien Datenverkehr.

In der Tat stellt sich immer aufs Neue die Frage, wo die Schutzpflicht des Staats endet und das freie Spiel (in diesem Fall: der Daten) beginnt. Eine Grenze hat das Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 aufgezeigt, in dem es feststellt, dass der Einzelne gerade keine „absolute“ Herrschaft über „seine“ Daten hat, der Schutz der Privatsphäre nur kontextbezogen erfolgen und der Schutz personenbezogener Daten durch das Allgemeininteresse beschränkt werden kann. Ich möchte hinzufügen, dass der Schutz personenbezogener Daten auch dort seine Grenze finden kann, wo der Schutz anderer Grundrechte (insbesondere Meinungs-, Presse- und Informationsfreiheit, aber auch die unternehmerische Freiheit) beginnt.

Eine weitere Frage lautet: Was machen wir, wenn Datenschutz und Datensicherheit einmal nicht zwei Seiten einer Medaille sind? Wenn Datenschutz sogar dem Schutz der Privatsphäre schadet? Ich denke hier beispielsweise an die Möglichkeiten von Telemedienanbietern, zum Schutz der Kunden in ihren Systemen vorsorglich Verkehrsdaten zu speichern, um Angriffe von außen erkennen und abwehren zu können. Aus datenschutzrechtlichen Gründen – und damit im vermeintlichen Interesse der Kunden – sind die Befugnisse hierzu sehr begrenzt. Das muss nicht immer richtig sein. Die Kundendaten vor dem Zugriff des Telemedienanbieters zu schützen, dadurch aber Cyberkriminellen den Einbruch in die Systeme zu erleichtern, ist für mich ein Widerspruch.

Der Schutz der Privatsphäre unterliegt darüber hinaus auch dem gesellschaftlichen Wandel. Mit den Mitteln des Datenschutzrechts allein kann die Privatsphäre im digitalen Zeitalter nicht geschützt werden. Über viele Themen sollten wir diskutieren. Neben den klassischen Themen Datenschutz und Datensicherheit auch über Diskriminierungsverbote, die Kontrolle von „Big Data“-Algorithmen, Investitionen in die digitale Bildung und den Aufbau digitaler Souveränität, intelligente Regelungen für Plattformen und Onlinevermittler, der Grundsatz der Datenverkehrsfreiheit, für die öffentliche Verwaltung das Once-Only-Prinzip, Regelungen über den digitalen Nachlass, eine vernünftige Abgrenzung von personenbezogenen und nicht personenbezogenen Daten, erweiterte „Open Data“-Initiativen, um nur einige zu nennen. Das alles sind Facetten einer sich abzeichnenden modernen Datenpolitik, an deren Anfang wir stehen. Diese Datenpolitik wollen wir in den nächsten Jahren klug gestalten – und wir werden sie klug gestalten müssen.

Dr. Thomas de Maizière



ist seit 2009 Mitglied des Deutschen Bundestags. Vor seinem Amtsantritt als Bundesminister des Innern im Dezember 2013 war de Maizière von März 2011 bis Dezember 2013 Bundesminister der Verteidigung und zuvor von 2009 bis 2011 Bundesinnenminister. Von 1999 bis 2005 hatte der gebürtige Bonner verschiedene politische Funktionen in den Länderregierungen von Mecklenburg-Vorpommern und Sachsen. Unter anderem als Staatsminister der Finanzen, Justiz und des Innern sowie als Leiter der Sächsischen Staatskanzlei.

DATEN-SICHERHEIT UND DATEN-SCHUTZ SIND WICHTIGE THEMEN FÜR DEN VERFASSUNGS-SCHUTZ

MIT DER RASANT ANSTEIGENDEN ZAHL VON DATEN UND DER ZUNEHMENDEN VERNETZUNG ALLER LEBENSBEREICHE STEIGT DAS BEDÜRFNIS NACH DIGITALER SICHERHEIT. WIRTSCHAFTSUNTERNEHMEN, FORSCHUNGSINSTITUTE UND BEHÖRDEN ODER POLITIKER SIND REGELMÄSSIG ZIEL VON CYBERATTACKEN.

Die Häufigkeit und Intensität der Angriffe haben in den letzten Jahren deutlich zugenommen, wie der Cyberangriff auf das Datennetz des Deutschen Bundestags zeigt – den wir detektiert und auf den wir die Bundestagsverwaltung im Mai 2015 aufmerksam gemacht haben. Die Sicherheit ihrer Daten ist also auch ein Thema für den Bundesverfassungsschutz: Gemeinsam mit anderen Behörden kümmern wir uns um die Abwehr von Cyberangriffen. Dass bei unserer Arbeit in diesem wie in anderen Bereichen sensible Daten anfallen, liegt in der Natur der Sache. Um das nachrichtendienstliche Informationsbedürfnis mit den Belangen des Datenschutzes auszubalancieren, haben sich für die Erfassung von Daten umfangreiche rechtliche Vorgaben und Kontrollmechanismen etabliert.

WIRTSCHAFTSSCHUTZ UND DATENSICHERHEIT

Die globalisierte Wirtschaft ist heute geprägt von beschleunigten Innovationszyklen und der Intensivierung des Wettbewerbs. Die Zeiträume für die Nutzung von Innovationsvorsprüngen werden immer kürzer. Dies gilt im Besonderen für die deutsche Wirtschaft, die eine der wissensintensivsten weltweit ist. Eine entscheidende Bedeutung kommt dem Schutz des firmeneigenen Know-how zu, also beispielsweise den Entwicklungs-, Produktions- oder Vertriebsgeheimnissen.

Im digitalen Zeitalter erfolgen Angriffe auf die essenziellen Betriebsgeheimnisse häufig in elektronischer Form, wobei es wegen der Möglichkeiten zur Verschleierung und Anonymisierung oftmals schwer ist, zwischen Angriffen konkurrierender Unternehmen und staatlicher Nachrichtendienste zu unterscheiden. Unsere Aufgabe besteht in dem Schutz der deutschen Unternehmen vor Wirtschaftsspionage – nicht vor Konkurrenzausspähung – und den mit dem illegalen Datenabfluss einhergehenden Wettbewerbsnachteilen.

Die Rolle des Verfassungsschutzes definiert sich in erster Linie dadurch, eine präzise Einschätzung der Gefährdungslage durch „elektronische Angriffe“ vorzunehmen. Wir analysieren gemeldete Angriffe und ordnen sie bekannten Angreifern zu – nicht zuletzt, um sie für die präventive Gefahrenabwehr zu nutzen. Sofern ein Angriff auf eine IT-Infrastruktur nicht verhindert werden konnte, können wir die aus der Analyse gewonnenen Erkenntnisse zumindest dazu nutzen, weitere potenzielle Opfer zu sensibilisieren und zu schützen. Unter dem Leitmotiv „Prävention durch Information und Dialog“ bieten wir im Verbund mit den Verfassungsschutzbehörden der Länder im Wirtschaftsschutz ein breites Spektrum von Informations- und konkreten Beratungsangeboten an.

RECHTLICHE VORGABEN UND DATENERFASSUNG

Die Arbeit des Verfassungsschutzes berührt dabei auch datenschutzrechtliche Belange, was den Datenschutz im eigenen Haus zu einem wichtigen Thema für uns macht. Die Erfassung von Daten erfolgt weder massenhaft noch ohne Grund, wie vielfach behauptet wird. Bei der Cyberabwehr wie auf dem Feld der Terrorismus- und Extremismusabwehr unterliegt der Bundesverfassungsschutz klaren rechtlichen Vorgaben. Es gelten eine ganze Reihe von spezialgesetzlichen Bestimmungen, die sicherstellen, dass sensible und insbesondere personenbezogene Daten nur zu ganz bestimmten Zwecken erhoben, gespeichert und übermittelt werden dürfen. Nur beispielhaft seien hier das Bundesverfassungsschutzgesetz (BVerfSchG), das Sicherheitsüberprüfungsgesetz (SÜG) oder das Artikel 10-Gesetz (G10-Gesetz) genannt.

Der Einsatz von sogenannten nachrichtendienstlichen Mitteln, zu denen neben dem Einsatz von V-Leuten und der Observation auch die Telekommunikationsüberwachung gehört, kommt immer erst dann in Betracht, wenn alle anderen Mittel der Nachrichtenbeschaffung erschöpft sind oder keine Aussicht auf Erfolg versprechen. Im G10-Gesetz befinden sich die Bestimmungen, die dem BfV unter engen Voraussetzungen erlauben, in das Brief-, Post- und Fernmeldegeheimnis des Art. 10 des Grundgesetzes einzugreifen. Hierbei ist wichtig, dass solch ein Eingriff stets eine Individualmaßnahme darstellt und sich konkret und zielgenau auf einzelne Personen bezieht.

STRINGENTE KONTROLLE UND KONSEQUENTER DATENSCHUTZ

Die Verfassungsschutzarbeit findet aber nicht nur im Rahmen klarer rechtlicher Vorgaben statt, sie wird auch stringent kontrolliert. Im Rahmen der Verwaltungskontrolle übt das Bundesministerium des Innern (BMI) die Dienst- und Fachaufsicht über das BfV aus. Ein weiterer wesentlicher Teil der Kontrolle wird durch den Deutschen Bundestag und die von ihm eingesetzten Gremien ausgeübt. Spezielle parlamentarische Kontrollen erfolgen durch das Parlamentarische Kontrollgremium (PKGr), das Vertrauensgremium des Haushaltsausschusses sowie durch die G10-Kommission. Letztere entscheidet über die Zulässigkeit und Notwendigkeit der bereits erwähnten Eingriffe in Art. 10 des Grundgesetzes. Das PKGr verfügt über weitreichende Kontrollbefugnisse, was unter anderem auch ein Recht auf Akteneinsicht und ein Zutrittsrecht zu sämtlichen Dienststellen der Nachrichtendienste einschließt. Neben dem BfV gehören hierzu auch der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD).

Für den spezifischen Aspekt des Datenschutzes ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig. Sie übt nach Maßgabe des Bundesdatenschutzgesetzes (BDSG) und des BVerfSchG eine kontinuierliche datenschutzrechtliche Kontrolle über den Bundesverfassungsschutz aus. Die BfDI hat ein Recht auf Auskunft und verfügt über ein Einsichtsrecht, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, die im Zusammenhang mit der Kontrolle stehen. Ihr ist jederzeit Zutritt zu allen Diensträumen zu gewähren. Von diesem Recht wurde in der Vergangenheit auch Gebrauch gemacht.

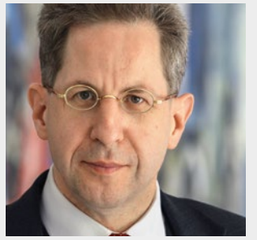
Neben der externen Kontrolle findet zeitgleich eine interne Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen statt. Diese führt der eigene behördliche Datenschutzbeauftragte des BfV durch, wie es vom BDSG vorgeschrieben wird. Um seinen Aufgaben unabhängig nachkommen zu können, ist er organisatorisch unmittelbar bei der Amtsleitung angesiedelt und in der Ausübung seiner Funktion weisungsfrei.

ZUKUNFT DER DATEN

Es ist offensichtlich, dass die bereits vorhandene und weiter wachsende Menge an sensiblen Daten Unternehmen wie Bürger und natürlich auch Behörden zum Nachdenken über den Umgang mit diesen Daten zwingt. Elektronische Angriffe werden immer raffinierter und zielgenauer und die Möglichkeiten des Missbrauchs von persönlichen Informationen immer unübersichtlicher. Die Erfüllung der gesetzlichen Aufgaben des Bundesamts für Verfassungsschutz erfordert in einer Reihe von Fällen die Erhebung und Nutzung von zum Teil sensiblen Daten. Dabei handeln wir in einem rechtlich klaren und transparenten Raum.

Wir werden auch in Zukunft auf eine gute Datengrundlage zum Schutz der Wirtschaft vor Cyberangriffen und zum Schutz der Menschen vor Terrorismus und Extremismus angewiesen sein. Um diesen Bedrohungen zu begegnen, bedarf es über den nationalen Rahmen hinaus auch eines Datenaustauschs auf internationaler Ebene, was weitere Fragen des Datenschutzes aufwirft. Bei alldem ist der rechtmäßige und verantwortungsvolle Umgang mit sensiblen Daten für den Verfassungsschutz aber nicht nur eine Pflicht, sondern auch eine Möglichkeit, das Vertrauen der Öffentlichkeit in unsere Arbeit zu stärken.

Dr. Hans-Georg Maaßen



ist seit dem 1. August 2012 Präsident des Bundesamts für Verfassungsschutz (BfV). Seit 1991 war der Jurist in verschiedenen Abteilungen im Bundesministerium des Innern tätig. Im Jahr 2000 wurde er persönlicher Referent des Sicherheitsstaatssekretärs. 2001 übernahm er die Leitung der Projektgruppe Zuwanderung und wurde 2002 zusätzlich Referatsleiter für Ausländerrecht. Im August 2008 wurde er Leiter des Stabs Terrorismusbekämpfung in der Abteilung Öffentliche Sicherheit im Bundesministerium des Innern.

Foto: Bundesamt für Verfassungsschutz

EIN GROSSER SCHRITT VORWÄRTS IN RICHTUNG DIGITALE REVOLUTION

ZUM ENDE DES JAHRES 2015 GELANG ES, EINE HISTORISCHE ERRUNGENSCHAFT FÜR DEN SCHUTZ PERSÖNLICHER DATEN ZU VERMELDEN: ES GELANG INNERHALB DER VOM EUROPÄISCHEN RAT ANVISIERTEN ZIELVORGABE DIE EINIGUNG VON RAT, KOMMISSION UND PARLAMENT DER EU AUF DIE DATENSCHUTZGRUNDVERORDNUNG SOWIE EINE DATENSCHUTZRICHTLINIE FÜR POLIZEI UND STRAFJUSTIZ.

Gemeinsam haben wir es geschafft, zwei Prioritäten voranzubringen, die ganz oben auf der Liste von Präsident Juncker und seiner Kommission stehen: der einheitliche digitale Binnenmarkt in Europa und ein einheitlicher Rechtsraum für Justizwesen und Grundrechte. Von diesen beiden Instrumenten werden gleichermaßen Unternehmen, öffentliche Verwaltungen und Bürger profitieren. Und sie kommen keinen Moment zu früh.

Insbesondere die Datenschutzgrundverordnung adressiert aktiv die Bedürfnisse aller Beteiligten in einer Zeit des beschleunigten technologischen Wandels, indem sie auf den bewährten Grundlagen der europäischen Datenschutzrichtlinie aus dem Jahr 1995 aufbaut und diese fortschreibt. Seitdem hat die digitale Revolution beträchtliche ökonomische Chancen und bedeutende Innovationen mit sich gebracht. Doch die rasanten Entwicklungssprünge haben zu viel Raum für Inkonsistenzen, Unsicherheiten und administrative Belastungen gelassen, sodass Unternehmen alle Hände voll damit zu tun haben, einen Flickenteppich von Regelwerken und Vorschriften zu verstehen und zu befolgen. Dieser musste dringend modernisiert werden, um nicht nur den grundrechtlichen Anforderungen zu genügen, sondern um diese zugleich mit jenen des Geschäftsverkehrs in Einklang zu bringen

DATENSCHUTZ: EIN WIRTSCHAFTLICHER WEGBEREITER, DER AUF VERTRAUEN BASIERT

Wir brauchen einen zukunftssicheren Datenschutz, der Innovationen ebenso den Weg ebnet wie dem fundamentalen Recht auf Schutz der persönlichen Daten und der Privatsphäre – unabhängig von der Technologie, die wir anwenden. Die neuen Regelungen ermöglichen uns das, indem sie das ökonomische Potenzial der digitalen Revolution aufgreifen und gleichzeitig den Bürgem die nötige Sicherheit geben, um in das benötigte wirtschaftliche Wachstum zu investieren.

Daten sind die Währung unserer heutigen digitalen Wirtschaft und das Vertrauen der Bürger ist der Schlüssel zu wirtschaftlichem Wohlstand, der allen zugutekommt. Persönliche Daten beinhalten und repräsentieren das Leben eines einzelnen Menschen. Persönliche Daten können nicht einfach wie Verbrauchsgüter gehandelt werden, sondern benötigen Schutz. Wenn sie außer Landes „reisen“, muss dieser Schutz mit ihnen reisen. Das fordert unsere Charta der Grundrechte der Europäischen Union.

Befürchtungen, dass ein verstärkter Datenschutz der Wirtschaft schade, sind unbegründet. Tatsächlich ist es gerade die Unsicherheit der Bürger, wie mit ihren persönlichen Daten umgegangen wird, die das Wachstum von Unternehmen bremst. Sechs von zehn Europäern vertrauen weder Telekommunikationsunternehmen noch Internetprovidern und sieben von zehn zeigen sich besorgt darüber, dass ihre Daten zu anderen als den angegebenen Zwecken benutzt werden könnten. Die Datenschutzgrundverordnung sorgt nun für eine Lösung, die diese Befürchtungen gegenstandslos macht, indem sie einen positiven Kreislauf aus robusten Datenschutzgrundsätzen, Sicherheitsmaßnahmen und wirtschaftlichem Wohlstand schafft. Durch diese Grundsätze und Absicherungen werden Bürger dazu ermuntert, das wirtschaftliche Potenzial ihrer persönlichen Daten zu entfesseln, dessen Wert Prognosen zufolge bis 2020 auf eine Billion Euro jährlich anwachsen soll.

Die Datenschutzgrundverordnung betont darüber hinaus, dass das grenzübergreifende ökonomische Potenzial von dem Grundsatz „Ein Recht für einen Kontinent“ abhängt. Daher ersetzen die neuen Regelungen 28 stark unterschiedliche Gesetzgebungen durch ein einheitliches, europaweit gültiges Regelwerk. Dieser gemeinsame Gesetzesrahmen ist ein entscheidender Schritt, der Rechtssicherheit und Schutz für Unternehmen und Bürger in der gesamten EU schafft. Zudem sorgt das System der jeweils einen, zentral zuständigen Anlaufstelle („One-Stop Shop“) für erheblich höhere geschäftliche Effizienz. Unternehmen haben künftig nur mit der nationalen Datenschutzaufsichtsbehörde zu tun, in deren Land ihr Hauptsitz liegt – unabhängig davon, in wie vielen anderen Ländern sie tätig sind. Dies entschlackt die Bürokratie und reduziert den Verwaltungsaufwand, wodurch Unternehmen den Spielraum für Expansion erhalten, den sie benötigen.

Darüber hinaus befördern die neuen Regelwerke einen maximalen Schutz für Unternehmen, indem sie für einen integrierten und standardisierten Datenschutz („by design and default“) eintreten. Die empfohlenen Schutzmaßnahmen wie Anonymisierung und Pseudonymisierung zielen darauf ab, das Risiko zu minimieren, das Firmen bei der Verarbeitung großer Mengen von persönlichen Daten eingehen, und die für Datenmissbrauch vorgesehenen Geldstrafen zu vermeiden.

Diese robusten Regelungen finden auf alle Unternehmen Anwendung, die europäischen Bürgern Produkte oder Dienstleistungen anbieten, unabhängig davon, ob es sich um europäische oder außereuropäische Unternehmen handelt. Damit entstehen gleiche Wettbewerbsbedingungen für alle Unternehmen und ein solider Schutz der Bürger vor jedem, der ihre Daten verwendet. Gleichzeitig vermeidet die Datenschutzgrundverordnung ein für alle gleiches Universalrezept und ermöglicht stattdessen einen rationalen, risikobasierten Ansatz, der zugeschnitten ist auf das jeweilige Unternehmen, seine Geschäftsaktivitäten und die damit verbundenen Risiken für die Grund- und Freiheitsrechte von Einzelpersonen. So sind beispielsweise nur jene Unternehmen, zu deren Kernaktivitäten risikobehaftete Datenverarbeitungsprozesse gehören, dazu verpflichtet, einen Datenschutzbeauftragten (Data Protection Officer) zu bestellen.

Alle diese Maßnahmen sollen Bürgern die Sicherheit vermitteln, dass der Umgang mit ihren Daten auf einer sicheren und fairen Basis abläuft. Die Bürger müssen die Kontrolle über ihre persönlichen Daten wiedergewinnen, bevor sie sich damit anfreunden können, dass Unternehmen sie nutzen. Ihr Recht auf den Schutz persönlicher Daten ist in Artikel 8 der Europäischen Grundrechtecharta verankert und es ist unsere gemeinsame Verantwortung, ein solches Recht zu schützen. Dies schließt das „Recht auf Vergessenwerden“ ebenso ein wie das Recht, über jede Verletzung von Datenschutz oder Datensicherheit informiert zu werden.

EIN „SICHERER HAFEN“, DER WIRKLICH SICHER IST

Das Recht auf eindeutige und zugängliche Informationen über die eigenen persönlichen Daten bildet geradezu den Ausgangspunkt des neuen Regelwerks: Es muss für Bürger immer klar ersichtlich sein, wie ihre persönlichen Daten verarbeitet und übermittelt werden. Die „Datenübertragbarkeit“ (Data Portability) zwischen Serviceprovidern wird so einfacher und macht sowohl den Bürgern als auch den Unternehmen das Leben leichter, wenn sie auf freiwilliger und gut informierter Zustimmung beruht. Denn eines steht fest: Die Person darf nicht zum Datenobjekt werden. Das Bürgerrecht auf den Schutz der eigenen persönlichen Daten ist ausschlaggebend für den Erfolg von Unternehmen.

Selbstverständlich gilt dieses Recht auf Schutz der persönlichen Daten nicht nur für Europa. Es erstreckt sich auf sämtliche Datenübertragungen innerhalb wie auch außerhalb der EU, einschließlich der USA. Daher ist es für mich der Abschluss eines besseren Safe-Harbor-Abkommens von oberster Priorität. Ich habe eng mit unseren US-amerikanischen Ansprechpartnern zusammengearbeitet, um eine Vereinbarung zu erreichen, die Bürgern und Unternehmen auf beiden Seiten des Atlantiks nützt. Dabei ist das Grundrecht der EU-Bürger auf Datenschutz unsere Richtschnur, insbesondere im Lichte des Schrems-Urteils des Europäischen Gerichtshofs.

Lassen Sie mich das ganz klar sagen: Wir brauchen auch die Fortführung der Datenflüsse über den Atlantik. Sie sind wichtig für unsere Wirtschaft. Ich habe mich bereits mit Unternehmensvertretern getroffen und verstehe ihre Sorgen nach der Aussetzung von „Safe Harbor“ vollkommen. Die Unternehmen benötigen eine Handlungsrichtlinie, Klarheit und die Versicherung, dass der Transfer von persönlichen Daten, auf den so viele von ihnen angewiesen sind, so bald wie möglich wieder auf Kurs gebracht wird. Die Alternativen wären nur eine vorübergehende Lösung und Unternehmen müssten sich mit Ausnahmeregelungen und Abweichungen auseinandersetzen.

Daher liegt es in unser aller Interesse, eine Vereinbarung zu erreichen, die den Standards des Schrems-Urteils entspricht. Das bedeutet: robuste Schutzmaßnahmen für die persönlichen Daten der Bürger. In einer globalisierten Wirtschaft müssen Menschen sicher sein können, dass ihre persönlichen Daten geschützt werden, wo auch immer sie gesendet, verarbeitet oder gespeichert werden. Nur mit dieser Sicherheit kann das Vertrauen in transatlantische Transfers wiederhergestellt werden und das Geschäft florieren.

Wenn wir darin erfolgreich sein wollen, benötigen wir klare, verbindliche Zusagen von unseren US-Kollegen. Wir arbeiten sehr eng mit ihnen zusammen, um so schnell wie möglich die richtige Lösung zu finden. Derzeit dauern die Verhandlungen noch an.

Derweil begrüße ich die Datenschutzgrundverordnung als einen Sieg für Unternehmen und Bürger gleichermaßen. Mit diesem neuen, gestrafften und modernisierten Verfahren sind wir bereit für eine digitale Revolution, in der eine boomende Wirtschaft und die Grundrechte Hand in Hand gehen.

Věra Jourová

ist seit November 2014 EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung. Zuvor war sie Ministerin für regionale Entwicklung in der tschechischen Regierung. Věra Jourová ist die populärste Politikerin in Tschechien und genießt großes Vertrauen in der Bevölkerung.

Foto: Chara Kaminara-Pipitsouli

„DIE DATENSCHUTZ-GRUNDVERORDNUNG STÄRKT DIE STÄRKEN DER EUROPÄISCHEN IT-WIRTSCHAFT.“

NACH FAST VIERJÄHRIGER DEBATTE HABEN SICH MITTE DEZEMBER 2015 DER EUROPÄISCHE RAT, DAS EUROPÄISCHE PARLAMENT UND DIE EUROPÄISCHE KOMMISSION ÜBER DEN ENDGÜLTIGEN INHALT DER EU-DATENSCHUTZGRUNDVERORDNUNG GEEINIGT. DIE ZUSTIMMUNG DES PARLAMENTS WIRD VORAUSSICHTLICH IM FRÜHJAHR 2016 ERFOLGEN. IN KRAFT TRITT DIE VERORDNUNG NACH EINER ÜBERGANGSPHASE ANFANG 2018. JAN PHILIPP ALBRECHT, FÜR BÜNDNIS 90/DIE GRÜNEN ALS ABGEORDNETER IM EUROPÄISCHEN PARLAMENT UND STELLVERTRETENDER VORSITZENDER DES INNEN- UND JUSTIZAUSSCHUSSES, IST DATENSCHUTZEXPERTE UND BERICHTERSTATTER DES EUROPÄISCHEN PARLAMENTS FÜR DIE DATENSCHUTZGRUNDVERORDNUNG DER EUROPÄISCHEN UNION.

Herr Albrecht, sind Sie nach fünf Jahren zäher Verhandlungen zur EU-Datenschutzgrundverordnung zufrieden mit dem Ergebnis?
Jan Philipp Albrecht: Mit dem erzielten Ergebnis können alle gut leben und arbeiten. Wir haben aus 28 unterschiedlichen nationalen Gesetzen eine einheitliche Verordnung geschaffen. Damit legen wir den Grundstein für den digitalen Binnenmarkt in Europa. Dieses „Single Level Playing Field“, also diese einheitlichen gleichen Wettbewerbsbedingungen, wird insbesondere den europäischen Unternehmen zugutekommen.

Wie erfolgte letztendlich die Zustimmung zum jetzt vorliegenden Entwurf?
Jan Philipp Albrecht: Der federführende Innen- und Justizausschuss im Europäischen Parlament sowie die ständigen Vertreter im Ministerrat haben dem Ergebnis der Trilogverhandlungen mit über 90 Prozent zugestimmt. Im Ministerrat hat sich nur Österreich enthalten, da es den Österreichern zu wenig Datenschutz war. Im Parlament haben drei Abgeordnete wegen zu viel Datenschutz dagegen gestimmt. Im nächsten Schritt wird der Entwurf formal vom Plenum des Parlaments und vom Ministerrat bestätigt. Theoretisch könnte es noch zu einer Ablehnung kommen, die allerdings dann eine absolute Mehrheit braucht. Ich sehe dieses Risiko aber nicht, da alle Fraktionen im Ausschuss am Ende zugestimmt haben.

Was sind für Sie die Meilensteine der Verordnung?
Jan Philipp Albrecht: Dazu gehört sicherlich das Marktortprinzip. Jedes Unternehmen muss sich zukünftig unabhängig von seinem Standort an das europäische Datenschutzrecht halten. Wer sich nicht daran hält, muss empfindliche Sanktionen hinnehmen. Die Strafen können bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen. Das ist ein scharfes Schwert des europäischen Rechts. Weiterhin werden die individuellen Rechte der Verbraucherinnen und Verbraucher gestärkt, insbesondere in Bezug auf Transparenz und Informationspflicht. Und es wird einfacher für die Bürgerinnen und Bürger, diese Rechte zu verstehen, sodass sie selbstbestimmt entscheiden können. So gibt es jetzt auch das Recht auf Datenportabilität. Das heißt, wenn eine Verbraucherin oder ein Verbraucher einen Anbieter wechseln wollen, muss der bisherige Anbieter alle vom Kunden oder der Kundin gespeicherten Daten bereitstellen. Das sorgt für mehr Wettbewerb, da Verbraucherinnen und Verbraucher nun einfacher zu datenschutzfreundlicheren Anbietern wechseln können. Das Recht auf „Vergessenwerden“ ist konkreter ausformuliert und es geht deutlicher hervor, wie das Recht umgesetzt werden kann.

Aber lassen sich die Strafen durchsetzen und könnten Länder nicht unterschiedlich streng mit den Strafen umgehen? Dies würde wieder eine Benachteiligung bedeuten.
Jan Philipp Albrecht: Diese Befürchtung hatten wir von Anfang an. Daher haben wir einen Mechanismus eingebaut. Das Parlament und der Rat haben beschlossen, dass der europäische Datenschutzausschuss im Zweifelsfall Mehrheitsentscheidungen über den Kopf der jeweiligen nationalen Behörde hinweg treffen kann. In diesem Ausschuss sind alle Datenschutzbehörden der Mitgliedsländer vertreten. Wenn also eine nationale Behörde eine Strafe verhängt, die deutlich zu niedrig oder zu hoch ausfällt, dann wird die europäische Behörde die Möglichkeit haben, dies zu korrigieren. Und das können alle einklagen.

Behindert die Verordnung die Wirtschaft?
Jan Philipp Albrecht: Es wird immer Kritik an jeder Einigung geben. Aber die deutliche Mehrheit hat nun entschieden, dass es ein sehr guter Kompromiss ist. Gerade für die mittelständischen Unternehmen in der Europäischen Union und insbesondere in Deutschland bedeutet die Verordnung im Vergleich zum jetzigen Recht einen großen Schritt nach vorn. Natürlich können Leute fordern, dass wir uns an den rechtlichen Vorgaben wie zum Beispiel im Silicon Valley hätten orientieren können. Das wäre aber nicht mehr mehrheitsfähig gewesen. Ich habe eher den Eindruck, dass sich große Unternehmen aus dem Silicon Valley durch die Einigung ermutigt sehen, sich an diesen Standard zu halten. Und auch die US-Regierung scheint ihre Haltung ändern zu wollen. Das ist ein guter Impuls, den wir in der EU setzen. Denn es entsteht eine Dynamik, die datenschutzrechtlich freundliche Technologien deutlich voranbringen wird. Dies stärkt die Stärken der europäischen IT-Wirtschaft.

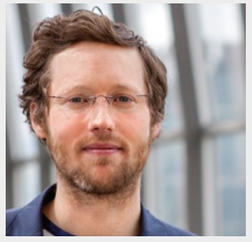
Es soll aber weiterhin nationale Ausnahmeregeln geben?
Jan Philipp Albrecht: Das ist der Fall. Gerade im Bereich der öffentlichen Behörden konnten wir nur Grundsätze festlegen. Dies wird weiterhin im nationalen Recht geregelt bleiben. Auch im Bereich der privatwirtschaftlichen Datenverarbeitung gibt es Ausnahmen, beispielsweise wenn es um sehr sensible Daten wie genetische oder biometrische Informationen geht. Hier haben sich die Mitgliedsstaaten vorbehalten, weitere Standards zu verankern. Gleiches gilt für den Arbeitnehmerdatenschutz. Wir hätten uns gewünscht, dass wir auch hier weiterkommen. Aber dafür war es zu früh.

Auch die Pflicht zur Meldung von Datenschutzvorfällen soll aufgeweicht worden sein.
Jan Philipp Albrecht: Das Parlament hat klargestellt, dass es nur eine Ausnahme von der Meldepflicht geben darf, wenn der Datenverarbeiter ausreichend darlegen kann, dass es kein Risiko für die Betroffenen gibt. Nur dann kann er auf eine Meldung verzichten. Diese Vorgabe bedeutet eine hohe Schwelle für die Unternehmen. Deshalb ist davon auszugehen, dass sie einen Vorfall lieber melden werden.

Datenschützer bemängeln, die Pflicht Datenschutzbeauftragte zu bestellen, würde aufgeweicht.
Jan Philipp Albrecht: Das müssen wir gesamteuropäisch bewerten. Die Stellung der betrieblichen Datenschutzbeauftragten ist nun EU-weit einheitlich geregelt. Das ist ein großer Fortschritt für die deutschen Unternehmen, die schon lange Datenschutzbeauftragte bestellen müssen. Das gab es so in fast keinem anderen EU-Staat. Zudem ändert sich der Schlüssel, wann ein Unternehmen einen Datenschutzbeauftragten bestellen muss. Weniger als die Größe des Unternehmens ist jetzt die Sensibilität der Daten, mit denen ein Unternehmen umgeht, das Kriterium. Für den Datenschutz scheint mir dies das sinnvollere Kriterium zu sein. Und Staaten, denen das nicht ausreicht, können die Bestellpflichten ergänzend regeln. So dürfte in Deutschland die bestehende Gesetzgebung bezüglich der Bestellpflicht weiter existieren, sofern der Gesetzgeber dem zustimmt.

Nach fünf Jahren Verhandlungen sind Sie am Ziel. Mit welchem Thema befassen Sie sich jetzt?
Jan Philipp Albrecht: Der Datenschutz muss sich angesichts der Digitalisierung weiterentwickeln. Es wird also kein Ende der Diskussion geben. Zudem gibt es genug andere Richtlinien, die den Datenschutz berühren. Etwa die Revision der E-Privacy-Richtlinie, die den Datenschutz bei der elektronischen Kommunikation regelt. Oder das ewige Thema der Vorratsdatenspeicherung.

Jan Philipp Albrecht



Jahrgang 1982, hat Rechtswissenschaften studiert. Der Wolfenbütteler ist seit 1999 Mitglied bei den Grünen. Seit 2009 sitzt er als jüngster deutscher Abgeordneter im Europäischen Parlament. Er ist Berichterstatter des Europäischen Parlaments für die Datenschutzgrundverordnung, stellvertretender Vorsitzender des Innen- und Justizsuchschusses und stellvertretendes Mitglied im Ausschuss für Binnenmarkt und Verbraucherschutz. Während seiner ersten Legislaturperiode von 2009 bis 2014 war er Mitglied im Innen- und Justizausschuss und stellvertretendes Mitglied im Rechtsausschuss. Von Dezember 2012 bis Oktober 2013 war Jan Philipp Albrecht auch Koordinator für den Sonderausschuss gegen organisiertes Verbrechen, Korruption und Geldwäsche.

Foto: Fritz Schumann

WEGWEISENDES URTEIL

FÜR DIE GESAMTE INTERNET-WIRTSCHAFT

NACHDEM DER EUROPÄISCHE GERICHTSHOF (EUGH) DIE SAFE-HARBOR-VEREINBARUNG ZWISCHEN DER EU UND DEN USA GEKIPPT HAT, MUSS DIE TRANSATLANTISCHE DATENÜBERTRAGUNG AUF EINE NEUE BASIS GESTELLT WERDEN. UM DEN HOHEN EUROPÄISCHEN DATENSCHUTZSTANDARDS ZU GENÜGEN, MUSS SICHERGESTELLT SEIN, DASS ES KEINEN UNBESCHRÄNKTEN ZUGRIFF AMERIKANISCHER SICHERHEITSBEHÖRDEN AUF DATEN EUROPÄISCHER BÜRGER GIBT. DAS IST DER MASSSTAB, DEN DER EUGH MIT SEINEM WEGWEISENDEN URTEIL IM RECHTSSTREIT SCHREMS GEGEN FACEBOOK FESTGELEGT HAT.

Die Reaktionen in den Medien waren eindeutig: Die Entscheidung sei ein Paukenschlag, welcher in dieser Deutlichkeit nur von den wenigsten erwartet wurde. Erst recht nicht so kurz nach dem Votum des Generalanwalts Yves Bot. Die Safe-Harbor-Entscheidung der EU-Kommission vom Juli 2000 wird durch den EuGH für ungültig erklärt, und das ohne jede Übergangsfrist. Sehr klar sagt der EuGH, dass in den USA kein angemessenes Schutzniveau für personenbezogene Daten bestehe, weil die Daten europäischer Kunden nicht ausreichend vor dem Zugriff amerikanischer Sicherheitsbehörden geschützt seien.

Die EU-Kommission hatte im Jahr 2000 im Zuge des sogenannten Safe-Harbor-Abkommens die USA zu einem solchen „sicheren Hafen“ erklärt. US-Unternehmen konnten sich danach selbst bescheinigen, dass sie europäische Datenschutzbestimmungen erfüllen. Sie müssen dafür gegenüber der US-Handelskommission (FTC) einige Selbstverpflichtungen zum Datenschutz eingehen.

KEINE WIRKSAME DURCHSETZUNG DER GRUNDSÄTZE

Mehr als 4400 Unternehmen hatten, der Safe-Harbor-Entscheidung folgend, ihre Verpflichtung auf sieben essenzielle europäische Datenschutzgrundsätze gegenüber der amerikanischen FTC erklärt. Eine wirksame Durchsetzung dieser Grundsätze in den Unternehmen fand aber nicht statt und der Rechtsschutz für die betroffenen europäischen Bürger ist in den USA eingeschränkt und wenig effektiv. Zudem wurde durch die Enthüllungen von Edward Snowden einer breiteren Öffentlichkeit klar, dass US-Sicherheitsbehörden in weitaus größerem Ausmaß auf personenbezogene Daten, die in die USA übermittelt werden, zugreifen, als bisher bekannt war.

Foto: Gerichtshof der Europäischen Union

Diese Situation war nicht hinnehmbar. Bei uns in Europa gehört der Schutz personenbezogener Daten zu den gemeinsamen Grundwerten, die uns alle verbinden und die effektiv geschützt werden müssen. Daher haben wir als Deutsche Telekom schon früh gefordert, die bestehende Safe-Harbor-Regelung nicht mehr anzuwenden und durch ein neues System mit effektiven Schutzmechanismen für personenbezogene Daten zu ersetzen. Nach dem EuGH-Urteil sind die Bundesregierung, die EU-Kommission und die USA erst recht aufgefordert, eine geeignete Basis für den Datenaustausch zwischen Europa und den USA zu schaffen. In unserer zunehmend digitalisierten Welt ist ein sicherer transatlantischer Datenaustausch unverzichtbar.

Die Europäische Datenschutzgrundverordnung, die nach den erfolgreich abgeschlossenen Trilog-Verhandlungen wahrscheinlich im Frühjahr 2016 durch das Europäische Parlament verabschiedet wird, enthält das sogenannte Marktortprinzip. Danach ist das europäische Datenschutzrecht auf all diejenigen anwendbar, die in Europa ihre Produkte und Dienstleistungen anbieten – unabhängig davon, wo der Anbieter seinen Sitz hat: in Europa, in den USA oder Asien. Die EU-weite Gesetzgebung bietet zukünftig zahlreiche Schutzmechanismen, wenn Daten doch außerhalb Europas gespeichert werden sollen. Unternehmen können sich beispielsweise auf die Standards der Datenschutzgrundverordnung zertifizieren lassen. Dies gewährleistet, dass auch Unternehmen aus Staaten außerhalb der EU sich an die europäischen Datenschutzstandards halten, wenn sie Daten von europäischen Bürgern verarbeiten.

DETAILS VON EU-US-PRIVACY SHIELD OFFENLEGEN

Diese Prinzipien dürfen durch eine neue transatlantische Vereinbarung zur Datenübertragung nicht ausgehebelt werden. Ein unkontrollierter und undifferenzierter Zugriff auf Daten europäischer Bürger durch amerikanische Sicherheitsbehörden ist zu verhindern. Der EuGH hat das bereits eindeutig in seinem Urteil in der Sache Schrems gegen Facebook festgestellt. Die Daten europäischer Bürger sind aktuell in den USA nicht ausreichend geschützt. Die EU-Kommission sollte daher so schnell wie möglich die Details der neuen „EU-US-Privacy Shield“-Vereinbarung offenlegen. Nur so lässt sich feststellen, ob die neue Vereinbarung hält, was sie verspricht, und alle Betroffenen können sich ein eigenes Urteil bilden.

Die Telekom hatte schon vor der Entscheidung des EuGH vorgesorgt: Wir verarbeiten grundsätzlich keine Daten aus Europa in Übersee. Auch große amerikanische Partner verarbeiten die Daten deutscher Kunden in unseren Rechenzentren in Deutschland. In den Fällen, in denen die Verarbeitung in Europa nicht gegeben ist, machen wir das den Kunden transparent. Unsere Regelungen zum Datenschutz haben wir mit Partnerunternehmen zudem in Standardvertragsklauseln vereinbart. Hinzu kommen Anforderungen an die Auftragsdatenvereinbarung nach deutschem Recht, die Teil der Verträge sind. Innerhalb des Konzerns gelten die Binding Corporate Rules beziehungsweise äquivalente Vereinbarungen, sofern Daten überhaupt übertragen werden.

Wenn Daten beim Transport durch das Internet keine Umwege durch andere Rechtsräume wie zum Beispiel die USA mehr nehmen, wird der Datenverkehr insgesamt sicherer. Daher haben wir schon frühzeitig ein „Internet der kurzen Wege“ gefordert, durch das beim Transport von Daten der direkte Weg vom Absender zum Empfänger gewährleistet wird. In unseren Netzen haben wir das bereits umgesetzt. Wir wollen den unerlaubten Zugriff von außerhalb auf die in Europa transportierten Daten deutlich erschweren und setzen uns dafür ein, dass sich möglichst viele Internetprovider der Idee des Internets der kurzen Wege anschließen.

Zum Schutz der personenbezogenen Daten ist auch das Thema sichere Verschlüsselung der Kommunikationsinhalte wichtig. Eine wirksame Ende-zu-Ende-Verschlüsselung, die auch für Verbraucher einfach zu handhaben ist, sorgt für mehr Sicherheit auch gegenüber unangemessenen Zugriffen von Sicherheitsbehörden.

Für die Deutsche Telekom bedeutet das Urteil des EuGH: Wir müssen Verantwortung übernehmen. Schon jetzt zeigen uns Gespräche, dass unsere europäischen Unternehmenskunden einer Datenspeicherung im außereuropäischen Ausland kritisch gegenüberstehen und die Nachfrage nach Cloud Services „made in Europe“ steigt. Mit unseren Verschlüsselungstechnologien tragen wir dem Bedürfnis nach sicherem Datentransfer Rechnung. Zudem garantiert die Telekom in allen ihren Rechenzentren, nicht nur in den deutschen, die gleichen hohen Sicherheitsstandards. Diese werden jährlich überprüft.

Bei Kooperationen mit Unternehmen aus Nicht-EU-Ländern verlangen wir, dass die angebotenen Lösungen auf unseren Rechnern gespeichert und verarbeitet werden. Sollte das nicht möglich sein, verlangen wir die Einhaltung der EU-Standardvertragsklauseln. Sollte der Partner die Standardvertragsklauseln nicht akzeptieren, verzichten wir auf die Leistung oder machen sie unseren Kunden transparent, sodass sie die freie Wahl haben.

Kommentar von Dr. Thomas Kremer, Vorstand Datenschutz, Recht und Compliance, Deutsche Telekom

EUROPA UND SEIN „PRIVACY SHIELD“

IM JAHR 2016 GEHÖRT DIE ERKENNTNIS, DASS DATEN DER ROHSTOFF DES 21. JAHRHUNDERTS SIND, ZU BELIEBTEN ALLGEMEINPLÄTZEN IN DEN DEBATTEN ZUR DIGITALISIERUNG. DASS DATEN FÜR DIE DIGITALE WIRTSCHAFT EINE GROSSE STRATEGISCHE BEDEUTUNG HABEN IST UNBESTRITTEN – VOR ALLEM IM WETTBEWERB MIT DEN USA.

Wenn wir von Industrie 4.0, Big Data und Cloud-Diensten sprechen, wird schnell deutlich, dass Europa ohne die Hoheit über die dort generierten Daten beim digitalen Wandel eine digitale Kolonie wird. Ein entscheidendes Element für die Hoheit über Daten ist das Datenschutzrecht. Hier bestehen erhebliche Unterschiede zwischen der Europäischen Union und den USA. Rückblickend ist das inzwischen fünfzehn Jahre alte „Safe Harbor“-Modell ein ziemlich untauglicher Versuch gewesen, die Systemunterschiede des Datenschutzrechts zwischen der EU und den USA zu überbrücken. Faktisch kam es einem Blanko-Scheck zum Datenexport für US-amerikanische Unternehmen gleich. Erste kritische Stimmen haben in Europa bereits 2005 die Datentransferpraxis hinterfragt. Und die deutschen Datenschutzaufsichtsbehörden haben 2010 beschlossen, dass sich Datenexporteure in Deutschland nicht auf die Behauptung einer „Safe Harbor“-Zertifizierung von US-amerikanischen Unternehmen verlassen dürften.

GESELLSCHAFTLICHEN KONSENS ERZIELEN

Der Europäische Gerichtshof hat dann 2015 für Klarheit gesorgt, indem er festgestellt hat, dass in den USA derzeit kein mit der EU vergleichbares Datenschutzniveau besteht. Die Aufhebung der „Safe Harbor“-Entscheidung der Europäischen Kommission war daher nur konsequent. Sie kommt aber im Grunde viel zu spät. Dabei geht es nicht nur um die Frage, ob und wie europäischen Bürgerrechten in den USA effektiv Rechnung getragen werden kann. Es geht vor allem darum, in welcher digitalen Welt wir leben wollen. Es muss in Europa gelingen, über die Ausgestaltung dieser digitalen Welt einen breiten gesellschaftlichen Konsens zu erzielen. Dazu gehört auch die Frage, wie wir einerseits selbstbestimmt in Europa mit Daten umgehen und andererseits den transatlantischen Handel stärken und weiter entwickeln wollen.

Der Erfolg der Verhandlungen über das Transatlantische Freihandelsabkommen wird von entscheidender Seite an eine schnelle Nachfolgeregelung für „Safe Harbor“ gekoppelt. Eine Koppelung, die aufgrund der eingangs erwähnten wirtschaftlichen Bedeutung von Daten nicht abwegig ist – im Gegenteil. Das Anfang Februar vorgestellte „EU-US Privacy Shield“ soll ein Datentransfermodell sein, das einen gemeinsamen sicheren Datenraum schafft. Bei den Abstimmungen zu TTIP und der schriftlichen Ausgestaltung des „EU-US Privacy Shield“ sollte deshalb das Europäische Parlament und die Mitgliedsstaaten die strategische Bedeutung einer datenbasierten Ökonomie in den Vordergrund rücken.

US-amerikanische Unternehmen konnten über Jahre hinweg riesige Datenmengen sammeln, stets direkt oder indirekt legitimiert durch den vermeintlich „sicheren Hafen“ der USA für Daten aus Europa, und uns so veredelte Digitalprodukte teurer zurückverkaufen. Eine Entwicklung, die Europa zunehmend zu einem digitalen Absatzmarkt herabsinken lässt und volkswirtschaftlich bedenklich ist, da mit ihr auch ein erheblicher Verlust von Kompetenzen und Innovationsfähigkeit verbunden ist. Ohne die Innovationsfähigkeit der Unternehmen aber, allen voran unseres Mittelstands, ist eine Wirtschaft nicht wachstumsfähig, mit unmittelbar negativen Folgen für das Wohlstandsniveau.

EINFACHE LÖSUNGEN FÜR TRANSATLANTISCHEN DATENAUSTAUSCH

Die Rechtsunsicherheit, die das „Safe Harbor“-Urteil geschaffen hat, muss aber deshalb möglichst schnell behoben werden, da die Auswirkungen, vor allem für kleine- und mittelständische Unternehmen, enorm sind. Es braucht gerade für diese einfach anwendbare Lösungen für den transatlantischen Datenaustausch. Ob das neue „Privacy Shield“ hält, was sein Name verspricht, wird sich nicht nur anhand des in den kommenden Wochen zu erwarteten finalen Textes zeigen. Es wird sich auch daran messen lassen müssen, ob es sowohl den Praxistest als auch eine zu erwartende erneute Befassung durch den EuGH überstehen wird.

Allen Diskussionen um Systemunterschiede zum Trotz dürfen der transatlantische Handel und die damit verbundenen Investitionen nicht beschädigt werden. Gleichzeitig müssen aber die Regelungen der neuen Datenschutzgrundverordnung konsequent angewendet werden. Dies ist wichtig, um europäischen Bürgern verloren gegangenes Vertrauen zurück zu geben. Auch müssen für europäische und außereuropäische Unternehmen gleiche Wettbewerbsbedingungen im globalen Datengeschäft geschaffen werden. Dies kann nur ermöglicht werden, wenn das neu verhandelte Abkommen den Anforderungen des EuGH-Urteils – so etwa die Gewährleistung eines effektiven Rechtsschutzes – vollumfänglich gerecht wird. Erst wenn die USA ein mit der EU vergleichbares Datenschutzniveau aufweisen, darf eine entsprechende Adäquanzentscheidung ergehen, um die Datenverarbeitung zwischen Firmen verschiedener Wirtschaftsräume zu ermöglichen. Allerdings sind erhebliche Zweifel angebracht, ob das neue „Privacy Shield“ diesem Anspruch gerecht wird. Zu vage sind noch die belastbaren Informationen, zu schwammig noch die Zusagen, vor allem der US-Seite.

MARKTORTPRINZIP KONSEQUENT DURCHSETZEN

Hiervon unabhängig muss die Datenschutzgrundverordnung und das in ihr verankerte Marktortprinzip dort, wo personenbezogene Rohdaten für Unternehmen das zentrale Geschäftsmodell sind, konsequent durchgesetzt werden. Das „I agree“-Geschäftsmodell großer Plattformen muss der Vergangenheit angehören. Darin wird sich ein Stück weit unsere digitale Souveränität in Europa beweisen. Umsetzbar sind die Anforderungen für die vorgenannten Unternehmen allemal, da sie in Europa über umfangreiche Rechenkapazität verfügen.

Das Urteil des EuGH ist eine große Chance, verlorenen Boden wieder gutzumachen, indem außereuropäische Unternehmen endlich zur Beachtung eines Datenschutzniveaus verpflichtet werden, wie wir es seit Jahren in Deutschland und Europa kennen und das durch die Datenschutzgrundverordnung weiter gefestigt wird. Hier ist Vertrauen nicht verhandelbar. Es wäre wünschenswert, wenn Politik hier im Sinne Europas handeln würde und die Verantwortung nicht allein der Justiz überträgt. Aber auch die Industrie selbst ist gefordert, produktseitig selbst Handlungsalternativen für Unternehmen anzubieten. Die Deutsche Telekom ist hier beispielsweise bei Cloud-Diensten Vorreiter. So fungieren wir für Microsoft und andere global tätige Unternehmen als Datentreuhänder und wirken damit vertrauensbildend. Denn durch eine Datenspeicherung in den Rechenzentren der Deutschen Telekom in Deutschland findet deutsches Recht Anwendung und damit die Wahrung der Rechtsstaatlichkeit für europäische Bürger.

Wolfgang Kopf, LL.M.

leitet seit November 2006 den Zentralbereich Politik und Regulierung der Deutschen Telekom. Sein Verantwortungsbereich umfasst neben der nationalen und internationalen politischen Interessenvertretung, die Verbands-, Frequenz und Medienpolitik sowie sämtliche Regulierungsfragen im Konzern. Wolfgang Kopf studierte Rechts- und Geisteswissenschaften an der Universität Mainz, der Verwaltungshochschule Speyer sowie der University of London.

ZEHNPUNKTEPROGRAMM FÜR MEHR SICHERHEIT IM NETZ

DIE MASSIVE ÜBERWACHUNG DURCH AUSLÄNDISCHE GEHEIMDIENSTE SOWIE IMMER NEUE FÄLLE VON CYBERKRIMINALITÄT GEFÄHRDEN DIE DIGITALE ENTWICKLUNG. SICHERHEIT IST DIE ACHILLESFERSE EINER VERNETZTEN GESELLSCHAFT. SIE BRAUCHT MEHR TRANSPARENZ, KLARE VERANTWORTLICHKEITEN UND ZUSÄTZLICHE EXPERTISE FÜR EINEN BESSEREN SCHUTZ VON DATEN UND INFRASTRUKTUR. DAZU HAT DIE TELEKOM ZEHN KONKRETE MASSNAHMEN DEFINIERT:

1. Die Erkenntnisse, die Edward Snowden zur Verfügung gestellt hat, müssen vollständig offengelegt und zugänglich gemacht werden. Nur so können mögliche Schwachstellen im Netz identifiziert und unverzüglich geschlossen werden.

2. Innerhalb der EU sollten die Mitgliedsländer auf gegenseitiges Ausspionieren des Telekommunikations- und Internetverkehrs verzichten. Auch mit den USA sollte weiterhin ein Abkommen über einen Spionageverzicht angestrebt werden.

3. Sicherheitsbehörden sollten transparent machen, welche Informationen sie über Telekommunikations- und Internetnutzer abfragen. Dazu gehören Anzahl und Art der erfolgten Anfragen und Auskünfte sowie der überwachten Anschlüsse.

4. Unternehmen müssen Transparenz über Sicherheitsstandards und erfolgte Angriffe schaffen. Nur durch gegenseitige Ergänzung wird ein möglichst umfassender Schutz vor Cyberangriffen erreicht. Die Telekom hat ihre technischen Sicherheitsstandards unter **www.telekom.com/sicherheit** veröffentlicht und macht Cyberangriffe unter **www.sicherheitstacho.eu** transparent.

5. Forschung und Bildung zu Cybersicherheitsthemen müssen verstärkt werden. Die Telekom richtet einen Lehrstuhl für Datenschutz und Datensicherheit an der Hochschule für Telekommunikation in Leipzig ein. Mit der Plattform Teachtoday.de stellt die Telekom zudem Unterrichtsmaterialien für Schulen zum Themenkomplex Sicherheit und Datenschutz bereit.

6. Analytik und Forensik zur Netzsicherheit müssen verstärkt werden. Dafür sollten die Cyber Emergency Response Teams (CERT) in den Unternehmen ausgebaut und enger verzahnt werden. Neben der Verstärkung ihres Teams fördert die Telekom die Ausbildung von Spezialisten: Gemeinsam mit der IHK Köln wurde 2014 ein neues Qualifikationsprogramm „Cyber Security Professional“ geschaffen. Die Telekom wird in den nächsten Jahren mehrere Hundert Mitarbeiter zu IT-Sicherheitsexperten weiterqualifizieren.

7. Perspektivisch sollten Inhalte auf dem Übertragungsweg Ende zu Ende verschlüsselt werden. Hier sind Hersteller, Netzbetreiber und Diensteanbieter gleichermaßen gefordert, einfache Lösungen für Kunden zu entwickeln. Die Telekom setzt sich bei den Standardisierungsgremien für einheitliche Verschlüsselungstechniken ein.

8. Netzbetreiber dürfen sich nicht von einzelnen Herstellern kritischer Infrastrukturkomponenten abhängig machen. Die Telekom führt für diese Elemente eine sogenannte georedundante Dual-Vendor-Strategie ein. Bei kritischen Komponenten setzt die Telekom Produkte von mindestens zwei Herstellern aus unterschiedlichen geografischen Regionen ein.

9. Hersteller von Hard- und Software müssen genauso wie Netz- und Diensteanbieter bekannte Schwachstellen unverzüglich beseitigen. Die Telekom wird ihre Zulieferer dazu verpflichten. Bei besonders kritischen Komponenten sollte die Sicherheit der Produkte durch eine unabhängige Prüfstelle nachgewiesen werden. Das IT-Sicherheitsgesetz sowie die entsprechende Richtlinie der EU sollten das aufgreifen.

10. Daten dürfen beim Transport durch das Internet keine Umwege durch andere Rechtsräume nehmen. Im Telekom-Netz ist das Internet der kurzen Wege bereits realisiert. Diesen Ansatz will die Telekom mit einer Selbstverpflichtung aller Internetprovider weiter vorantreiben. Damit würde ein unberechtigter Zugriff auf die in Europa transportierten Daten von außerhalb deutlich erschwert. ■

INDUSTRIE 4.0 BRAUCHT NEUE SICHERHEITSKONZEPTE

DAS VERNETZTE AUTO SYMBOLISIERT DIE ZUKUNFT DER DIGITALISIERUNG, DES INTERNETS DER DINGE UND DER INDUSTRIE 4.0. EIGENSTÄNDIG RUFT ES IM NOTFALL HILFE, BESTELLT ERSATZTEILE, WARNT ANDERE FAHRZEUGE IN ECHTZEIT VOR GEFAHREN, FÄHRT AM ENDE AUTONOM – UND FORDERT NICHT ZULETZT NEUE SICHERHEITSKONZEPTE.

2015 bekam der Traum vom vernetzten, autonom fahrenden Auto einen leichten Dämpfer. Chrysler rief 1,4 Millionen Fahrzeuge zurück, weil Hacker per Mobilfunk das Bremssystem und die Klimaanlage eines Autos gekapert hatten. Kein Einzelfall: Mehrfach gelang es Autohackern, in die Bordelektronik von Modellen verschiedener Hersteller einzudringen. Zum Glück nur zu Demozwecken.

Die Autohacks zeigen, dass die zunehmende Vernetzung von Geräten und Maschinen bis hin zu ganzen Produktionsprozessen die produzierende Industrie mit neuen Risiken konfrontiert. Diese hat das erkannt und wertet IT-Sicherheit als eine der großen Herausforderungen auf dem Weg zu Industrie 4.0. Laut einer VDE-Studie sehen 70 Prozent der Entscheider die IT-Risiken als größtes Hindernis für den Erfolg einer vernetzten Produktion. Heutige Angriffstechniken können sich massiv auf die industrielle Produktion auswirken. Dazu gehören der Diebstahl von geistigem Eigentum und Betriebsgeheimnissen, Produktionsausfälle und physische Beschädigungen von Anlagen und Geräten bis zu gefälschten Sensordaten und falschen Anzeigen in den Kontrollsystemen.

Die Vielzahl aktiver oder passiver Elemente einer industriellen IoT-Lösung stellt de facto in ihrer Komplexität eine wesentliche Herausforderung für die Sicherheit dar. Unternehmen müssen zum einen die Sicherheit der zum Einsatz kommenden Software, Infrastrukturen sowie Anwendungs- und Rechnersysteme gewährleisten. Zum anderen müssen sie sich mit den Auswirkungen möglicher Cyberangriffe auf die Betriebssicherheit von Geräten und Anlagen beschäftigen, die mit dem Internet verbunden sind. Das Management von Sicherheit geht im IoT zudem über das eigene Unternehmen hinaus, da sie ihre Netze und Systeme teilweise für Kunden, Lieferanten und Partner öffnen müssen.

Ein industrielles Internet der Dinge erfordert also ein umfassendes Sicherheitsmanagement, um den Zugriff auf Schnittstellen, Systeme, Sensoren, (Fern-)Wartungszugänge und Geräte auf einen dafür autorisierten Personenkreis oder dafür autorisierte Prozesse zu beschränken. Um die Kommunikation in IoT-Lösungen erfolgreich einzusetzen, müssen die Entwickler bereits in der Entwicklungsphase Sicherheitsaspekte in die Anforderungen einbeziehen. Statt wie bislang üblich nachträglich und reaktiv Security-mechanismen einzuziehen, wird künftig proaktiv ein integrierter Ansatz zur Produkt- und Prozessentwicklung notwendig sein, der den Schutz von Anlagen und IT-Infrastruktur umfasst.

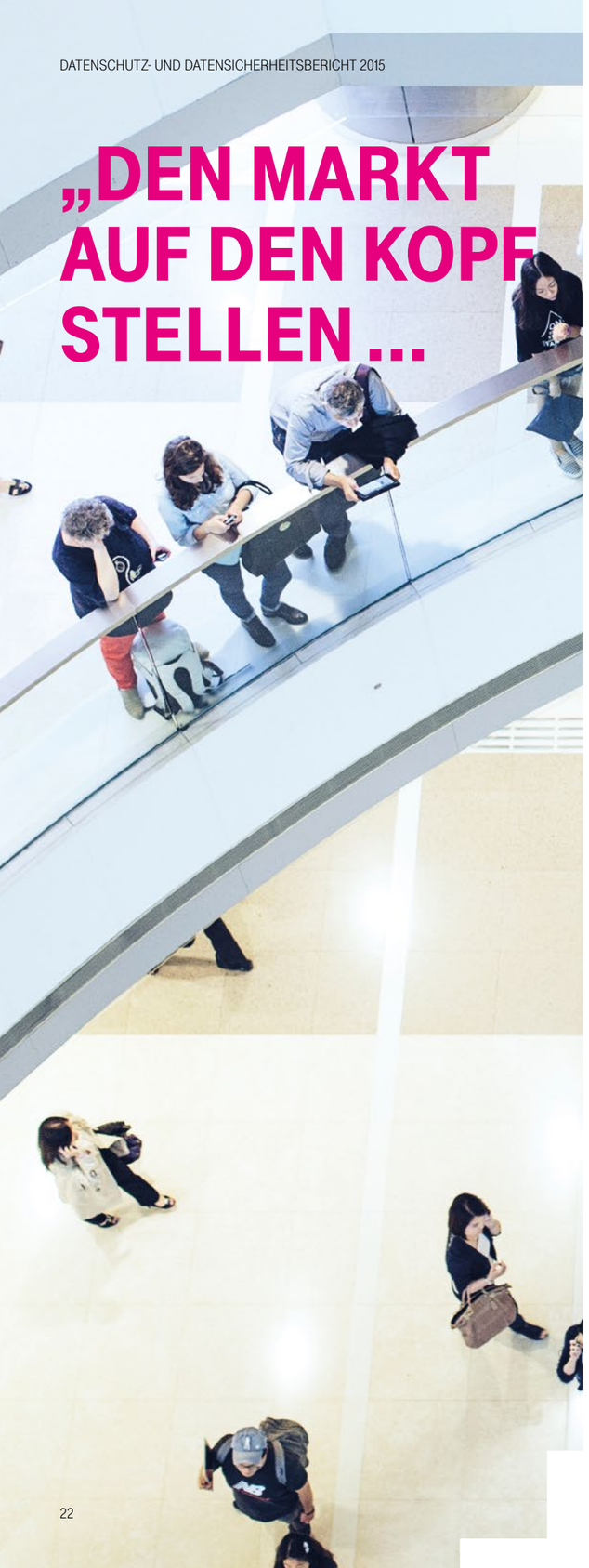
Und die Industrie reagiert schon: Laut dem Cyber Security Report 2015 hat sich schon mehr als die Hälfte der Unternehmen in der verarbeitenden Industrie mit speziellen IT-Sicherheitskonzepten für den Produktionsbereich auf die zunehmende Digitalisierung eingestellt. 45 Prozent verfügen über Sicherheitslösungen für den Datenaustausch zwischen Produktionssteuerung und Produktion. Zum Glück: Denn 44 Prozent der Unternehmen in den industriellen Kernbranchen nutzen gemäß Bitkom heute bereits Industrie-4.0-Anwendungen. Und einer PwC-Studie zufolge wollen Industrieunternehmen in den kommenden fünf Jahren in digitale Anwendungen investieren – im Durchschnitt 3,3 Prozent ihres Jahresumsatzes.

Fehlende Sicherheitslösungen würden dem prognostizierten Wachstumsschub durch Industrie 4.0, insbesondere in den Branchen Maschinen- und Anlagenbau, Elektrotechnik, Automobilbau, chemische Industrie, Landwirtschaft sowie Informations- und Kommunikationstechnologie, einen Dämpfer versetzen. Dies müssen wir industrieübergreifend verhindern, um die starke Wettbewerbsfähigkeit unserer produzierenden Industrien zu behaupten. ■

Reinhard Clemens

ist seit dem 1. Dezember 2007 im Vorstand der Deutschen Telekom verantwortlich für das Systemgeschäft des Konzernvorstandsbereichs T-Systems und zugleich Chief Executive Officer (CEO) der Großkundensparte T-Systems. Seit 1. Januar 2012 verantwortet Clemens auch alle internen IT-Aktivitäten des Konzerns.

„DEN MARKT AUF DEN KOPF STELLEN …



DIE DEUTSCHE TELEKOM BÜNDELT DIE BISHER IM KONZERN VERTEILTEN AKTIVITÄTEN FÜR INTERNE UND EXTERNE SICHERHEIT IM NEUEN GESCHÄFTSFELD „TELEKOM SECURITY“. DR. FERRI ABOLHASSAN IST GESCHÄFTSFÜHRER T-SYSTEMS UND VERANTWORTLICH FÜR DEREN IT-DIVISION UND TELEKOM SECURITY.

Herr Abolhassan: Warum ist der Markteintritt von Telekom Security gerade jetzt wichtig und richtig?
Ferri Abolhassan: Weil die Zeit reif ist – und das gleich in dreierlei Hinsicht: für den Markt, die Kunden und für uns. Erstens: Der Markt wächst. Denn die Cyberrisiken wachsen sowohl für Privatanwender als auch für geschäftliche Nutzer. Bereits mehr als ein Drittel der deutschen Unternehmen wird nach eigener Aussage mehrmals die Woche oder täglich von Cyberkriminellen angegriffen. Und neun von zehn Unternehmen sind bereits Opfer von IT-Angriffen geworden. Gleichzeitig stehen, zweitens, gerade Unternehmen in der Pflicht, ihre Geschäftsmodelle zu digitalisieren. Fast 90 Prozent der Entscheider aus Politik und Wirtschaft sehen dabei, laut unserem aktuellen Cyber Security Report, die IT-Sicherheit als die größte Herausforderung beispielsweise für die Umsetzung von Industrie 4.0 an.

Und als Deutsche Telekom haben wir, drittens, natürlich den – wenn man so möchte – „besonderen Vorteil“, Cyberbedrohungen tagtäglich als Konzern zu erleben und zu managen. Und genau diese über Jahre entwickelte Erfahrung und Expertise für interne Sicherheit bündeln wir jetzt konzernweit mit unserer Security-Kompetenz in Sachen Netz, Rechenzentrum und auch Beratung vor Kunde. Verbunden mit dem strengen deutschen Datenschutz und unserem eigenen Anspruch an Sicherheit – um nur die wichtigsten Punkte zu nennen. Dieser Mix zeichnet uns aus und hebt uns deutlich vom Wettbewerb ab.

Stichwort Digitalisierung – warum ist die Deutsche Telekom gerade dafür prädestiniert, Unternehmen den Weg in die Digitalisierung zu ebnen?
Ferri Abolhassan: Gerade erst hat uns Experton als eines von insgesamt nur sieben Unternehmen – unter 600 IT-Anbietern übrigens – ausgezeichnet. Allein dieser kleine Kreis ist demnach in der Lage, Kunden in der digitalen Transformation ganzheitlich zu begleiten. Das kennzeichnet eine Bestätigung unserer Arbeit und für mich Beleg unserer Rolle in puncto Digitalisierung. Wir haben alles an Bord: das sichere Netz, mehr als zehn Jahre Cloud-Erfahrung mit unseren Kunden, darunter auch die größte SAP HANA Einzelinstallation für Big Data, hochperformante Rechenzentren und Systemintegrations-Know-how – um nur einige wesentliche Punkte zu nennen. Und ganz besonders wichtig: das Ganze verbunden mit einem maximalen Anspruch an Qualität und Sicherheit. Sicherheit ist Teil unserer DNA. Seit Jahren denken wir Datenschutz und Datensicherheit mit – angefangen von der internen Cyberabwehr über die Sicherheit unserer Rechenzentren bis hin zu Produkten und Lösungen für unsere Kunden. Für Privatkunden genauso wie für Mittelstand und Großunternehmen.

Als Geschäftsführer IT-Division sind Sie für 6000 Geschäftskunden verantwortlich, darunter Dax und Fortune-500-Unternehmen. Vor welchen Herausforderungen stehen diese Schwergewichte?
Ferri Abolhassan: Machen wir uns nichts vor: in erster Linie wollen unsere Kunden, dass ihr Geschäft läuft. Egal, ob Mittelstand oder Weltkonzern. Dazu muss ihre klassische IT weiterhin sicher und zuverlässig laufen. Gleichzeitig aber müssen sich Unternehmen digital neu erfinden, neue Geschäftsmodelle und Services an den Start bringen, also Innovationen schaffen. Dazu brauchen sie IoT-Technologien, Big Data, Cloud & Co. Security ist für sie aber eine notwendige Voraussetzung, um digital voranzukommen. Der CIO eines der größten Unternehmen weltweit hat es vor Kurzem folgendermaßen präzisiert: Security macht Innovationen langsam. Aber eine Cyberattacke macht Innovationen noch langsamer. In der digitalen Transformation funktioniert das eine also nicht ohne das andere.

… das bedeutet?
Ferri Abolhassan: … übersetzt heißt das, für Telekom Security wird es darum gehen, umfassende Lösungen vor allem schnell bereitzustellen. Wir wollen Digitalisierung sicher und zuverlässig machen. Sicherheit über die gesamte Wertschöpfungskette zu bieten, aber dann auch umsetzen zu können – mit Telekom Security machen wir das möglich. Auch hier sind wir wie in vielen anderen Kerngeschäftenjedoch nicht allein unterwegs. Ich glaube fest an smarte Partnerings, die disruptiv und zügiger Marktanteile schaffen …

… Marktanteile sind das richtige Stichwort …
Ferri Abolhassan: Exakt, der IT-Sicherheitsmarkt in Deutschland hat heute ein Volumen von 10,8 Milliarden Euro und wächst jährlich um 7,5 Prozent. Auf dem deutschen Markt sind wir bereits Marktführer, wollen allerdings unsere Position mit neuen Lösungen und disruptiven Partnerschaften ausbauen. Mit Telekom Security monetarisieren wir unser Know-how am Markt in Geschäft und Wachstum. Mit einem ganzheitlichen Angebot für Privatkunden, den Mittelstand bis hin zum Weltkonzern wollen wir überzeugen und am internationalen Markt erfolgreich sein. Definiertes Ziel ist, führend in Europa zu werden.

Mit welchen Lösungen?
Ferri Abolhassan: Ein gutes Beispiel hierfür ist „Cyber Defense as a Service“. Es überwacht das Verhalten von Netzwerk- und IT-Systemen kontextbezogen und in Echtzeit. Damit lassen sich Angriffe sehr viel schneller erkennen und Gegenmaßnahmen ergreifen – bevor Schaden entsteht. Das bieten wir nun in standardisierter Form als Service aus der Cloud oder on-premise insbesondere mittelständischen Unternehmen an. Erste Pilotkunden haben wir bereits überzeugt. Zusammengefasst: Wie kein anderer können wir für eine ganze Bandbreite unserer Produkte und Lösungen eine Ende-zu-Ende-Sicherheit bieten – vom Endgerät und von der Anwendung aus der Cloud beim Kunden über die Netze bis hin zu unseren Rechenzentren.

… LEICHT, SCHNELL UND SICHER“

Ferri Abolhassan

ist Geschäftsführer von T-Systems und verantwortlich für die IT-Division. Er war unter anderem von 1992 bis 2001 und ab 2005 in unterschiedlichen Führungsfunktionen bei SAP tätig – zuletzt als Executive Vice President EMEA. 2008 übernahm er die Leitung des Bereichs Systems Integration bei T-Systems und ist verantwortlich für Telekom Security.

DATEN SIND DER SENSIBLE **ROHSTOFF** DER DIGITALISIERUNG

SUCHMASCHINEN, ONLINE-SHOPS, SOCIAL MEDIA ODER APPS: DIGITALE GESCHÄFTSIDEEN BASIEREN AUF DATEN – OFT AUCH AUF PERSONENBEZOGENEN DATEN. SIE GILT ES ZU SCHÜTZEN, OHNE DEN ANSCHLUSS AN DIE WIRTSCHAFTLICHE ENTWICKLUNG ZU VERLIEREN.

Daten sind wesentlicher Bestandteil der Geschäftsmodelle der Zukunft. Manche bezeichnen sie auch als „Rohstoff der Zukunft“. Sie sollen zur Wirtschaft gehören wie Kohle und Stahl, so Bundeskanzlerin Angela Merkel Mitte September 2015 auf einem CDU-Kongress zum digitalen Wandel. Dem lässt sich von der Bedeutung der Daten her kaum widersprechen. Daten zu erheben, zu analysieren, zu nutzen und zu verwalten wird Geschäftsmodelle in allen Branchen prägen.

Im Vergleich zu den Rohstoffen der Vergangenheit gibt es jedoch einen gravierenden Unterschied. Denn anders als Stahl und Kohle stehen hinter personenbezogenen Daten Menschen und deren Schicksale. Und anders als Stahl und Kohle sind die Informationen über die Menschen auch dann gesetzlich geschützt, wenn sie sich bereits in den Händen der Unternehmen befinden. Bei aller Berechtigung von geschäftlichen Interessen ist die sogenannte digitale Souveränität der Menschen zu schützen. Daten sind eben nicht nur ein Rohstoff wie jeder andere. Datenschutz und Datensicherheit müssen gewährleistet sein, wenn die Menschen digitalen Geschäftsmodellen vertrauen können sollen.

INTERESSENAUSGLEICH DURCH GESETZLICHE RAHMENBEDINGUNGEN

Personenbezogene Daten stehen in Deutschland unter der Obhut des Bundesdatenschutzgesetzes. Der darin niedergelegte Schutzstandard wird von der Ende 2015 abschließend verhandelten Europäischen Datenschutzgrundverordnung im Wesentlichen beibehalten. Die Verordnung wird allerdings erst Anfang 2018 greifen. Die Mehrheit der Bürger und auch der europäischen Wirtschaft begrüßt den dort angelegten harmonisierten Umgang mit personenbezogenen Daten.

Doch es gibt in der Wirtschaft auch kritische Stimmen, die fürchten, dass der Datenschutz die Zukunft der Wirtschaftsstandorte Deutschland und Europa gefährden könnte – trotz aller Erkenntnisse, die uns Edward Snowden gebracht hat. Denn digitale Geschäftsmodelle leben von Daten. Wer diese nicht so freizügig nutzen dürfe wie Unternehmen in Ländern außerhalb Europas, verliere den Anschluss – so die einfache Formel der Kritiker, die sich insbesondere während der Verhandlungen zur EU-Datenschutzgrundverordnung vermehrt zu Wort gemeldet haben.

DATENSCHUTZ ALS TEIL DES GESCHÄFTSKONZEPTS

Anders als bei den früheren Rohstoffen sind Daten nicht nur eine Ressource zur Verarbeitung, sondern unterliegen auch dem Selbstbestimmungsrecht der Kunden. Schon allein aus diesem Grund – der Kundenbindung – ist ein achtsamer Umgang mit den Daten vonnöten, wenn Unternehmen langfristig wirtschaftlich handeln wollen. Wenn ein Unternehmen nicht über eine faktische Monopolstellung verfügt, steht es dem Kunden grundsätzlich frei, seine Daten bei anderen Angeboten einzubringen. Das war bei Kohle und Stahl anders.

Die datenschutzrechtlichen Rahmenbedingungen des Bundesdatenschutzgesetzes und zukünftig der EU-Datenschutzgrundverordnung sorgen für Rechtssicherheit. Datenschutz wird so zu einer festen Größe der Geschäftskonzepte von Unternehmen – ebenso wie Kostenkontrolle, Marktanalysen und Marketingstrategien. Wenn Daten ein Rohstoff sind, sollte damit auch entsprechend umgegangen werden: sparsam und mit Bedacht. Zudem mit maximaler Transparenz, sodass Menschen verstehen, was mit ihren Daten passiert – und gegebenenfalls Nein sagen können.

ERST DENKEN, DANN HANDELN

Der Grundsatz „Erst denken, dann handeln“ gilt auch für Unternehmen. Wer sich frühzeitig Gedanken darüber macht, für welchen Zweck er die vorhandenen Daten wirklich braucht, spart Geld. Denn Daten sind erst wirklich von Wert, wenn Unternehmen wissen, wie sie ihren Geschäftsideen tatsächlich Nutzen bringen. Nicht nur der Datenschutz verlangt eine zweckbezogene Planung von Lösungen. Auch die IT-Abteilung muss wissen, was sie in Bezug auf die Anwendungsszenarien entwickeln soll.

Bei vielen digitalen Geschäftsmodellen ist es in vielen Fällen nicht notwendig, die personenbezogenen Daten als Klardaten zu verarbeiten. Um beispielsweise den Einsatz von öffentlichen Verkehrsmitteln besser zu planen, spielt es keine Rolle, wer die einzelnen Personen sind. Deshalb können die personenbezogenen Daten anonymisiert oder pseudonymisiert werden. Bei der Pseudonymisierung ist der Rückbezug auf die Person grundsätzlich möglich. Allerdings muss der Kunde dafür seine Zustimmung geben. Das wird eher der Fall sein, wenn der Kunde einen persönlichen Mehrwert in der Auswertung seiner Daten sieht, etwa eine bessere Medikation.

TRANSPARENZ SORGT FÜR DIGITALE SOUVERÄNITÄT

Datenschutz und Transparenz können ein Wettbewerbsvorteil sein. Das haben auch US-amerikanische Unternehmen erkannt. So hat Microsoft die Deutsche Telekom zum Treuhänder für ihr Cloud-Angebot in Deutschland auserkoren. Microsoft-Kunden können nun ein Datenschutzniveau wählen, das die Anforderungen an deutsche Unternehmen erfüllt und den Umgang mit den Daten vollkommen transparent darstellt. Kunden haben so eine Wahlmöglichkeit und können selbst über den gewünschten Datenschutz entscheiden. Transparenz sollte als Grundprinzip für alle Unternehmen gelten, wenn sie personenbezogene Daten verarbeiten. Datenschutzfreundliche Voreinstellungen geben dem Kunden die Entscheidungshoheit zurück und erhöhen damit die Kundenakzeptanz und -zufriedenheit.

Doch das ist erst der Anfang. Die neuen Geschäftsmodelle im Bereich Industrie 4.0 und Internet of Things machen die Datenverknüpfungen derart komplex, dass sich nur schwer feststellen lässt, wer wann wo und in welchem Umfang auf Informationen zugreifen kann und was damit gemacht wird. Wir brauchen also Rahmenbedingungen, die die Gestaltung neuer Produkte rechtssicher und nachvollziehbar macht. Dafür muss klar sein, wer für welche Daten verantwortlich ist.

MEHR DATENSCHUTZ-KNOW-HOW

Um das zu gewährleisten, muss das Datenschutz-Know-how in den Unternehmen wachsen. Denn Datenschützer sollten die Umsetzung jeder Geschäftsidee begleiten. So, wie einige Unternehmen bereits den Chief Digital Officer (CDO) eingeführt haben, brauchen wir auch den CDPO, den Chief Data Privacy Officer, in zunehmendem Maße. Die Telekom hat hier eine Vorreiterrolle – und sich damit einen Vertrauensvorsprung in der ITK-Branche erarbeitet. Nachhaltig ist ohnehin nur der transparente und nachvollziehbare Umgang mit Kundendaten. Sicher nicht das ungebremste Ausnutzen der Daten für den kurzfristigen Geschäftserfolg.

Was sollten also die Grundprinzipien einer digitalen Wirtschaft sein? Achtsamkeit im Umgang mit den uns anvertrauten Daten, Transparenz gegenüber den betroffenen Menschen und die Nutzung von technischen Mitteln zur Gewährleistung von „Privacy by Design“-Ansätzen wie Pseudonymisierungs- und Anonymisierungsverfahren. Und wenn sich alle daran halten, muss niemand fürchten, einen Wettbewerbsnachteil zu erleiden.

Dr. Claus-Dieter Ulmer

ist Konzernbeauftragter für den Datenschutz der Deutschen Telekom. Zuvor leitete der promovierte Jurist den Datenschutz von T-Systems International und debis Systemhaus und war nach seinem Studium als Rechtsanwalt mit Schwerpunkt im Unternehmensrecht tätig.

KRITISCHE BEGLEITER

Der Datenschutzbeirat der Deutschen Telekom berät den Vorstand als unabhängiges Beratungsgremium und ermöglicht einen konstruktiven Austausch mit führenden Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen zu datenschutzrelevanten Themen. Der Datenschutzbeirat wurde im Februar 2009 gegründet und ergänzt seitdem die interne Datenschutz- und Sicherheitsorganisation der Deutschen Telekom um einen unabhängigen und gesellschaftlich vielfältigen Blick von außen.

Zum Aufgabenfeld des Datenschutzbeirats gehört ein breites Spektrum: Er befasst sich mit Geschäftsmodellen und -prozessen zum Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit von entsprechenden Maßnahmen, mit internationalen Datenschutzfragen sowie mit den Implikationen neuer gesetzlicher Regelungen. Nach rund sieben Jahren Arbeit und 32 Sitzungen hat der Datenschutzbeirat der Telekom insgesamt 158 Empfehlungen mit auf den Weg gegeben. Die Telekom hat bisher jede Empfehlung umgesetzt oder die Umsetzung in Angriff genommen.

Im Jahr 2015 wurde das bisher zwölfköpfige Gremium mit dem ehemaligen Datenschutzbeauftragten des Bundes, Peter Schaar, hochkarätig ergänzt. Der Datenschutzbeirat kam zu vier Sitzungen zusammen. Im Fokus standen neben neuen digitalen Geschäftsmodellen, beispielsweise aus dem Bereich der vernetzten Gesundheit, die Überprüfung des neuen Prozesses zur Missbrauchserkennung und insbesondere die Besprechung der Anforderungen und Auswirkungen aktueller Themen aus der Regulierung wie zum Beispiel das Urteil des Europäischen Gerichtshofs in Sachen Schrems gegen Facebook, das IT-Sicherheitsgesetz, das Gesetz zur Vorratsdatenspeicherung und nicht zuletzt auch die Europäische Datenschutzgrundverordnung.

DATENSCHUTZVORFÄLLE 2015

Fristlose Kündigung – Bei einer Prüfung eines Callcenter-Partners ist im Dezember 2015 unter anderem aufgefallen, dass der Partner ein nichtgenehmigtes Subunternehmen beschäftigt und diesem Kundendaten zur Verfügung gestellt hat. Das stellte einen erheblichen Verstoß gegen die Vereinbarung zur Auftragsdatenverarbeitung mit der Telekom dar. Die Telekom hat den Vertrag mit dem Callcenter daher fristlos gekündigt.

Kundencenter-App – Mit der Kundencenter-App verwalten Kunden mobil ihre Mobilfunk- und Festnetzanschlüsse. Es waren Einzelfälle bekannt geworden, bei denen Nutzern im Mobilfunkbereich der App falsche Daten angezeigt wurden. Die Telekom hat im Mai zunächst die App vorsorglich deaktiviert und anschließend den Bereich Festnetz darin wieder aktiviert. Der Bereich Mobilfunk der App blieb vorsorglich deaktiviert. Es waren keine weiteren Anwendungen der Telekom betroffen. Die Telekom hat ihren Kunden mit Android- und iOS-Geräten ein Update angeboten, nach dem die App wieder komplett zur Verfügung steht.

DIE AKTUELLEN MITGLIEDER DES DATENSCHUTZBEIRATS:

- **Jan Philipp Albrecht:** Abgeordneter des Europäischen Parlaments, Mitglied im Innenausschuss und stellvertretendes Mitglied im Ausschuss für Binnenmarkt und Verbraucherschutz, Verhandlungsführer des Europäischen Parlaments für die geplante Datenschutzgrundverordnung
- **Wolfgang Bosbach**: CDU, MdB, Rechtsanwalt und Vorsitzender des Bundestags-Innenausschusses
- **Peter Franck**: Mitglied des Vorstands Chaos Computer Club (CCC)
- **Professor Dr. Hansjörg Geiger:** Honorarprofessor für Verfassungsrecht an der Johann-Wolfgang-Goethe-Universität in Frankfurt und von 1998 bis 2005 Staatssekretär im Bundesministerium der Justiz, Präsident des Bundesamts für Verfassungsschutz und des Bundesnachrichtendienstes a. D.
- **Professor Peter Gola:** Ehrenvorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit (GDD), Autor / Mitautor zahlreicher Publikationen zum deutschen Datenschutzrecht
- **Bernd H. Harder:** Rechtsanwalt, Mitglied des Hauptvorstands des Bitkom e. V., Lehrbeauftragter an der Hochschule der Medien Stuttgart und an der Technischen Universität München (TMU)
- **Gisela Piltz:** Mitglied im Bundesvorstand der FDP, stellvertretende Vorsitzende der FDP NRW
- **Gerold Reichenbach**: SPD, MdB, Mitglied im Innenausschuss (Berichterstatter für Datenschutz sowie Bevölkerungsschutz und Katastrophenhilfe)
- **Peter Schaar:** ehemaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit und Vorstandsvorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz
- **Dr. Gerhard Schäfer:** Vorsitzender Richter am Bundesgerichtshof i. R.
- **Lothar Schröder:** Vorsitzender des Datenschutzbeirats, Mitglied des ver.di Bundesvorstands und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG
- **Halina Wawzyniak:** Die Linke, MdB, Obfrau im Ausschuss für Recht und Verbraucherschutz, Mitglied im Ausschuss Digitale Agenda
- **Professor Dr. Peter Wedde:** Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt / Main, Direktor der Europäischen Akademie der Arbeit an der Universität Frankfurt am Main

DATENSCHUTZ SCHAFFT VERTRAUEN

Kaum machte Mitte Dezember 2015 die Meldung vom erfolgreichen Abschluss der Trilogverhandlungen zur EU-Datenschutzgrundverordnung die Runde, meldeten sich die Bedenkenträger wieder zu Wort. „Dem europäischen Gesetzgeber ist es nicht gelungen, moderne und zukunftssichere Regeln für den Umgang mit Daten im 21. Jahrhundert zu schaffen“, schreibt der Bundesverband Digitale Wirtschaft. Und der Zentralverband der deutschen Werbewirtschaft sieht im neuen EU-Datenschutzrecht erhebliche Rechtsunsicherheit für die Wirtschaft.

Warum tut sich die Wirtschaft so schwer mit dem Datenschutz? Ist es der Datenschutz an sich oder geht es nicht vielmehr nur um die mehrfach angeprangerte Wettbewerbsverzerrung durch ungleiche Marktbedingungen – vor allem für die Unternehmen, deren Geschäftskonzepte auf Daten aufbauen?

Genau dieses Ungleichgewicht wird doch die EU-Datenschutzgrundverordnung aufheben. Sie wird auch außereuropäische Unternehmen zum gleichen Umgang mit personenbezogenen Daten zwingen wie die bisher in diesem Punkt benachteiligte europäische – und besonders deutsche – Wirtschaft. Und die Verordnung geht noch weiter: Sie stellt den Verbraucher in den Mittelpunkt. Zu Recht. Denn die Verbraucher machen sich mehr Gedanken über den Umgang mit ihren persönlichen Daten, als die Unternehmen wahrhaben wollen.

Dies zeigt sich an den katastrophalen Umfrageergebnissen zum Vertrauen der Bürger in die Wirtschaft. So lauten die Schlagzeilen zu den Umfrageergebnissen einer repräsentativen Studie des TNS Infratest zum Thema Big Data: „In Deutschland regiert Misstrauen“, „Fast die Hälfte der Verbraucher misstraut Unternehmen beim Datenschutz“ oder „Deutsche sehen Weitergabe ihrer Daten besonders kritisch“. Das Meinungsforschungsinstitut hatte mehr als 8000 Menschen in acht europäischen Ländern befragt. Die meisten Europäer trauen kaum jemandem: weder dem Staat, den Banken, Telekommunikationsunternehmen, Suchmaschinen noch den Anbietern von sozialen Netzwerken. Auf den Punkt gebracht: Das Vertrauen ist weitgehend zerstört.

Auf der einen Seite also die klagenden Unternehmen, auf der anderen Seite die misstrauischen Verbraucher. Schadet oder schützt der Datenschutz? Wie lautet die richtige Antwort auf dieses Paradoxon? Für die Telekom ist sie eindeutig: Die Unternehmen müssen das verloren gegangene Vertrauen wiedergewinnen. Wir wollen die Daten unserer Kunden um jeden Preis schützen und wenden die Datenschutzregeln konsequent an. Denn nur so wird das Geschäftsmodell der Telekom langfristig funktionieren. Ich bin sogar davon überzeugt, dass früher oder später das strenge deutsche – und bald europäische – Datenschutzrecht zum Exportschlager wird.

Bereits jetzt orientieren sich außereuropäische Staaten an der wahrscheinlich im Jahr 2018 in Kraft tretenden EU-Datenschutzgrundverordnung.

Die Telekom jedenfalls profitiert schon heute vom Datenschutz. Dies zeigt der Sicherheitsreport 2015, nach dem die Bevölkerung der Telekom in der Telekommunikations- und Internetbranche die mit Abstand größte Vertrauenswürdigkeit im Umgang mit persönlichen Daten zuschreibt – mit 46 Prozent sogar deutlich vor den nächstplatzierten Unternehmen mit 24 Prozent. Die Telekom ist also auf gutem Weg, aber noch nicht angekommen. Denn Ziel muss es sein, noch mehr Menschen von der Vertrauenswürdigkeit zu überzeugen. Daran arbeiten wir auch gemeinsam im Datenschutzbeirat, der in seiner Zusammensetzung einen Querschnitt durch verschiedene Parteien und Institutionen repräsentiert – und in seinen Sitzungen konstruktiv über Datenschutz diskutiert sowie der Telekom zu noch mehr Vertrauen in der Bevölkerung verhelfen wird. Davon bin ich überzeugt.

Lothar Schröder

ist stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG und der Telekom Deutschland GmbH. Seit April 2006 leitet er im ver.di-Bundesvorstand den Fachbereich „Telekommunikation, Informationstechnologie, Datenverarbeitung“, ist zuständig für „Innovation und Gute Arbeit“ sowie für die Gruppe „Meisterinnen und Meister, Technikerinnen und Techniker, Ingenieurinnen und Ingenieure (mti)“.

Foto: Kay Herschelmann

VORRATS-DATEN-SPEICHERUNG RELOADED

„KEIN GRUND ZUM FEIERN“

DIE VORRATSDATENLOSE ZEIT GEHT ZU ENDE. MIT DER VERKÜNDUNG IM BUNDESGESETZBLATT AM 17. DEZEMBER 2015 TRAT DAS „GESETZ ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN“ IN KRAFT.

Die „Erbringer öffentlich zugänglicher Telefondienste“ müssen ab dem 1. Juli 2017 wieder Rufnummern und andere Kennungen der Kommunikationspartner mit genauen Zeitangaben, Internetzugangsdienste die jeweilige Internetprotokolladresse speichern. Bei mobilen Diensten sind zusätzlich die Daten über die zu Beginn der Verbindung genutzten Funkzellen festzuhalten.

Wird Deutschland tatsächlich sicherer, wenn die Telekommunikationsunternehmen erneut verpflichtet werden, Daten über das Kommunikationsverhalten ihrer Kunden zu speichern? Das zentrale Argument der Befürworter der Vorratsdatenspeicherung ist deren angebliche Notwendigkeit im Kampf gegen den Terrorismus. Insbesondere seit dem Massaker islamistischer Terroristen an den Redakteuren der Satirezeitschrift Charlie Hebdo im Januar 2015 in Paris hatten deutsche Politiker die Wiedereinführung der Speicherungspflicht gefordert.

VERSTOSS GEGEN GRUNDRECHTE-CHARTA

Die 2006 eingeführte Vorratsdatenspeicherung hatte das Bundesverfassungsgericht am 2. März 2010 für verfassungswidrig erklärt und der Europäische Gerichtshof (EuGH) annullierte am 8. April 2014 die Vorratsdatenspeicherungs-Richtlinie der EU, weil sie eklatant gegen die Grundrechte-Charta verstieß, und zwar gleichermaßen gegen den in Art. 7 garantierten Schutz der Privatsphäre und den durch Art. 8 verbrieften Schutz personenbezogener Daten. Legitime Zwecke der Strafverfolgung, der Gefahrenabwehr und der Terrorismusbekämpfung rechtfertigten die tiefen, mit einer anlasslosen, regional unbegrenzten, langfristigen und umfangreichen Speicherung personenbezogener Daten verbundenen Grundrechtseingriffe nicht. Entscheidend dabei sei, dass von einer solchen Maßnahme ganz überwiegend Unverdächtige betroffen sind.

Die Forderungen nach neuen Datensammlungen folgen einem Reaktionsmuster, das bereits nach den Terroranschlägen vom 11. September 2001 zu beobachten war. Sie lösten weltweit eine Welle von Überwachungsmaßnahmen aus, von denen wir heute wissen, dass sie die Welt nicht sicherer gemacht haben. Dies gilt ebenso für die Vorratsdatenspeicherung, die ja in Frankreich niemals ausgesetzt und auch vor den jüngsten terroristischen Anschlägen praktiziert wurde. Selbst die dortige zwölfmonatige Vorratsdatenspeicherung hat die schrecklichen Mordattentate vom Januar und November 2015 nicht verhindern können.

DEUTLICH KÜRZERE SPEICHERFRISTEN

Auch wenn immer mehr Untersuchungen die Nutzlosigkeit der undifferenzierten Datenspeicherung bei Terrorismusbekämpfung belegen, hat dies die Bundestagsmehrheit nicht davon abgehalten, die Speicherungspflicht erneut einzuführen. Obwohl die dabei festgelegten Fristen von zehn Wochen für Verkehrsdaten und IP-Adressen bzw. vier Wochen für Standortdaten deutlich unterhalb der Vorgaben der früheren Vorratsdatenspeicherung bleiben, steht die Maßnahme zu Recht in der Kritik:

- Es handelt sich um eine undifferenzierte Maßnahme, die ganz überwiegend unschuldige und unbescholtene Nutzerinnen und Nutzer elektronischer Dienste trifft. Selbst Daten von Berufsgeheimnisträgern wie Ärzten und Anwälten sollen lückenlos erfasst werden. Die gesetzlichen Verwertungsverbote schützen diese Daten nur unzureichend.
- Der Nachweis der Notwendigkeit des mit der verdachtslosen Speicherung verbundenen tiefen Eingriffs in die Grundrechte wurde nicht erbracht.
- Terroristische und andere Straftäter haben vielfältige Möglichkeiten, der Vorratsdatenspeicherung zu entgehen, etwa durch die Verwendung nicht registrierter Prepaidkarten oder von Kommunikationsdiensten, die nicht erfasst werden, insbesondere von „Over-the-top“-(OTT)-Diensten wie Skype, für die eine entsprechende Speicherverpflichtung nicht besteht.
- Die zusätzlich gespeicherten Daten erhöhen das Risiko einer unberechtigten Verwendung durch Innen- und Außentäter. Diesen Gefährdungen kann nur mit erheblichem technischem, personellem und finanziellem Aufwand entgegengewirkt werden, den letztlich alle Kundinnen und Kunden der verpflichteten Unternehmen und zum Teil auch die Steuerzahler zu tragen haben.

Vor diesem Hintergrund ist es mehr als verständlich, dass Verfassungsbeschwerden gegen die neue Vorratsdatenspeicherung angekündigt wurden – durchaus mit guten Erfolgsaussichten.

Peter Schaar

war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). In dieser Funktion war Schaar Mitglied der Artikel-29-Datenschutzgruppe der Datenschutzbeauftragten der EU-Mitgliedsstaaten, die er von Februar 2004 bis Februar 2008 leitete. Der Volkswirt engagiert sich in der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), deren Vorsitzender er seit September 2013 ist. Er ist Mitglied der Deutschen Gesellschaft für Informationsfreiheit, der Hamburger Datenschutzgesellschaft, der Humanistischen Union und der Gesellschaft für Informatik. Außerdem ist er Parteimitglied von Bündnis 90/Die Grünen.

SMART DATA

FÜR MEHR IT-SICHERHEIT

SCHUTZ DES PERIMETERS: SO LAUTET BIS HEUTE DAS GRUNDPRINZIP DER IT-SICHERHEIT. DOCH REICHT DIE BURGMAUER UM DAS UNTERNEHMENSNETZWERK NOCH AUS, UM PROFESSIONELLE HACKER AUFZUHALTEN? IN ZUKUNFT MÜSSEN UNTERNEHMEN ANGREIFER ZUSÄTZLICH IM INNEREN DER BURG BEKÄMPFEN.

Mit der IT-Sicherheit geht es so wie mit den mittelalterlichen Burgmauern und Wassergräben. Irgendwann reichte es nicht mehr aus, sich mit immer dickeren und höheren Burgmauern und tieferen Gräben gegen Feinde zu schützen. Spätestens als Kanonenkugeln das Hindernis einfach überflogen, war die Zeit der Schutzburgen vorbei.

So wie den Burgen könnte es bald den Unternehmen gehen, die sich nur mit Firewall und Virenscanner gegen Hacker wehren. Denn die Firewall arbeitet nach dem Prinzip des Perimeterschutzes: Was von draußen kommt, ist böse und wird gestoppt. Alles, was von drinnen rauswill, ist gut und darf passieren. Mit einer Ausnahme: die Kommunikation per E-Mail. Denn sie macht nur dann Sinn, wenn sie in beide Richtungen funktioniert.

KATZ-UND-MAUS-SPIEL

Genau diesen Schwachpunkt machen sich intelligente Angreifer zunutze. Sie schleusen Schadcode über E-Mails und Anlagen ins Unternehmensnetzwerk. Dort warten dann die Virenscanner, die die Schadsoftware erkennen und beseitigen sollen – was in den meisten Fällen auch noch immer gelingt. Doch wenn Hacker eine Schadsoftware individuell nur für einen Angriff auf ein Unternehmen entwickeln, versagt der Virenschutz in der Regel. Dabei spielt der Typ der Dateianlage immer weniger eine Rolle. Schadsoftware ist in Office Dokumenten genauso häufig versteckt wie in PDF- oder Multimediadateien.

Die Anbieter von IT-Sicherheitslösungen haben darauf reagiert und bieten aktuell Verfahren an, die sich alle E-Mails samt Anlagen genau anschauen und deren Verhalten bewerten. Versucht beispielsweise eine PDF-Datei ein Betriebssystem zu ändern, dann ist es mit großer Wahrscheinlichkeit eine Schadsoftware und die Sicherheitslösung macht sie unschädlich. Doch das Katz-und-Maus-Spiel zwischen Angreifern und ihren Opfern geht weiter. Intelligente Schadsoftware merkt inzwischen, ob sie geöffnet wird. Dann unterdrückt sie ihre Funktion.

SICHERHEIT BRAUCHT PARADIGMENWECHSEL

IT-Sicherheit braucht daher ein Paradigmenwechsel von der Abschottung gegenüber der Außenwelt hin zu einer Detektion im Inneren. Denn jedes Unternehmen muss davon ausgehen, dass ein Angreifer früher oder später in sein Netzwerk eindringen wird. Dann heißt es, dies möglichst schnell zu erkennen und zu beseitigen. Aber wie lassen sich Angreifer erkennen? Durch anomales Verhalten. So bewegen sie sich im Gegensatz zum normalen Nutzer seitwärts. Das heißt: Sie suchen überall im Unternehmensnetzwerk nach Dateien, in denen sie Passwörter und Nutzerkennungen abgreifen können. Mit diesen Daten können sie später ganz „legal“ ins Unternehmensnetzwerk eindringen. Diese Seitwärtsbewegung bietet die Chance, dem Angreifer eine Falle zu stellen – und ihn zu beseitigen.

Für diesen Schutz im Inneren braucht es Smart Data und künstliche Intelligenz. Es geht darum, den berechtigten Benutzer von den Angreifern zu unterscheiden. Am besten geht das durch verhaltensbasierte Analysesysteme. Dafür werden Verhaltensprofile der Angreifer und der Mitarbeiter nebeneinandergelegt und die Unterschiede identifiziert. Zukünftige Sicherheitslösungen verfügen über Kontrollpunkte, die dieses „anomale“ Verhalten erkennen und den Angriff abwehren. Auch Ärzte vergleichen Normal- mit Extremverhalten. Um den hohen Anforderungen des Datenschutzes dabei gerecht zu werden, geschieht all dies voll automatisiert und das Verhalten eines spezifischen Nutzers ist dabei vollkommen irrelevant.

RUNDUM-SORGLOS-PAKET IM ABOMODELL

Moderne Sicherheitslösungen für Smartphones wenden dieses Prinzip bereits an. Da Smartphones hoch entwickelte Computer sind und Nutzer Softwareupdates sowie Sicherheitssoftware eher selten einsetzen, konzentrieren sich Angreifer zunehmend auf Mobilfunkgeräte. Smartphones erzeugen aber permanent Verhaltensparameter wie Speicherausnutzung, Stromverbrauch oder Prozessorauslastung, sodass sich auffällige Abweichungen leicht erkennen lassen.

Der Schutz über Smart Data wird den klassischen Virenschutz, Firewalls und regelmäßige Softwareupdates nicht ablösen. Aber er wird ihn ergänzen. Kritiker bemängeln, dass eine solche Vorgehensweise zu komplex und für Unternehmen kaum zu managen sei. Die Lösung sind Provider, die den Schutz bereits in ihren Netzen umsetzen. Das reduziert die Komplexität für den Anwender, der sich zudem nicht mehr um Aktualisierung kümmern muss – quasi ein Rundum-sorglos-Paket im Abomodell. Zudem schützen Unternehmen und Privatverbraucher damit vernetzte Geräte wie Maschinen oder Fernseher, die sich mit zusätzlicher Sicherheitssoftware nicht schützen lassen.

Thomas Tschersich

ist Leiter der Sicherheitsabteilung der Telekom. Der Elektroingenieur verantwortete zuvor den Bereich IT-Sicherheit und Informationsschutz. Seit dem Jahr 2000 ist er in zahlreichen beratenden Funktionen bei Bundes- und Landesministerien und Behörden mit Bezug auf technische Sicherheitsanfragen tätig.

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

ZAHLEN, DATEN, FAKTEN

DIE ZAHL DER ANGRIFFE AUS DEM INTERNET STEIGT WEITER. DIE METHODEN DER ANGREIFER ÄNDERN SICH LAUFEND UND WERDEN IMMER PROFESSIONELLER. DIE TELEKOM SETZT ALLES DARAN, DIE CYBERANGRIFFE ZU ANALYSIEREN UND ABZUWEHREN.

67 MITARBEITER SIND BEI DER TELEKOM IM BEREICH GROUP PRIVACY TÄTIG

175
DATENSCHUTZKOORDINATOREN UNTERSTÜTZEN IM TELEKOM KONZERN BEI AUFGABEN RUND UM DEN DATENSCHUTZ

13.334
ANFRAGEN ZUM DATENSCHUTZ GINGEN AN DATENSCHUTZ@TELEKOM.DE

3.428
ENTWICKLUNGSPROJEKTE DURCHLIEFEN DAS PRIVACY AND SECURITY ASSESSMENTVERFAHREN (PSA)

97
DATENSCHUTZ- UND DATEN-SICHERHEITSAUDITS FÜHRTEN INTERNE UND EXTERNE AUDITOREN DURCH

7 INCIDENTS VERZEICHNETE DIE TELEKOM

96
PROZENT DER SCHADSOFTWARE TREFFEN AUFGRUND SEINES VERBREITUNGSGRADS DAS BETRIEBSSYSTEM ANDROID

80 DATA PRIVACY OFFICERS VERANTWORTEN DEN DATENSCHUTZ IM TELEKOM KONZERN

847 KRITISCHE SCHWACHSTELLEN HATTEN ALLEIN DIE 11 VERBREITETSTEN SOFTWAREPRODUKTE *

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

439 MILLIONEN SCHADPROGRAMMVARIANTEN FÜR PCS KURSIEREN IM INTERNET

70 PROZENT DER ENTSCHEIDER IN WIRTSCHAFT UND POLITIK STUFEN COMPUTERVIREN ALS GROSSE BEDROHUNG FÜR DEUTSCHLAND EIN ****

18/18
PROZENT DER UNTER-NEHMEN HABEN TÄGLICH, WEITERE 18 PROZENT EIN- ODER MEHRMALS PRO WOCHE MIT EXTERNEN ANGRIFFEN ZU KÄMPFEN ****

50 **60** PROZENT DER FÜHRUNGSKRÄFTE IN UNTERNEHMEN SIND ÜBERZEUGT, DASS IHR UNTERNEHMEN GUT AUF IT-SICHERHEITSRISIKEN VORBEREITET IST ****

50
PROZENT DER DEUTSCHEN UNTERNEHMEN WAREN STUDIEN ZUFOLGE BEREITS OPFER VON WIRTSCHAFTSSPIONAGE. DIE SCHÄDEN BELAUFEN SICH AUF 50 BIS 80 MILLIARDEN EURO JÄHRLICH.***

84
MILLIONEN NEUE MALWARE-EXEMPLARE WAREN IM UMLAUF: EIN ANSTIEG VON 9 MILLIONEN IM VERGLEICH ZU 2014 **

88
PROZENT DER FÜHRUNGSKRÄFTE IN UNTERNEHMEN SEHEN EINEN WIRKSAMEN SCHUTZ GEGEN CYBER-ANGRIFFE ALS GROSSE HERAUSFOR-DERUNG FÜR DIE UMSETZUNG VON INDUSTRIE 4.0 ****

371 STUNDEN UND DAMIT MEHR ALS 15 TAGE DAUERTE EIN VON KASPERSKY LAB FESTGESTELLTER DISTRIBUTED DENIAL OF SERVICE-ANGRIFF

48 PROZENT DER DEUTSCHEN SIND BEREITS OPFER VON INTERNETKRIMINALITÄT GEWORDEN

* Quelle: Die Lage der IT-Sicherheit in Deutschland 2015, BSI.
** Quelle: PandaLabs Jahresreport 2015.
*** Quelle: H.-G. Maaßen, Präsident des Bundesverfassungsschutzes.
**** Quelle: Cyber Security Report 2015.

VORRATSDATENSPEICHERUNG VERABSCHIEDET

AM 18. DEZEMBER 2015 IST DAS „GESETZ ZUR EINFÜHRUNG EINER SPEICHERPFLICHT UND EINER HÖCHSTSPEICHERFRIST FÜR VERKEHRSDATEN“, ALSO ZUR „VORRATSDATENSPEICHERUNG“, IN KRAFT GETRETEN. AUCH NACH WIEDEREINFÜHRUNG DER VORRATSDATENSPEICHERUNG GILT FÜR DIE DEUTSCHE TELEKOM: ES GEHT UM DAS VERTRAUEN DER MENSCHEN!

Telekommunikationsunternehmen müssen Telefon- und Internetverbindungsdaten nun zehn Wochen lang speichern. Sie erfassen nur Verbindungsdaten – also nicht den Inhalt der Kommunikation. Für Standortdaten, die bei Mobilfunkgesprächen anfallen, sieht das Gesetz eine kürzere Frist von vier Wochen vor. Der E-Mail-Verkehr ist von der Vorratsdatenspeicherung ebenso ausgenommen wie aufgerufene Internetseiten. Ausschließlich Strafverfolgungsbehörden dürfen auf die Daten zugreifen, und das auch nur mit Genehmigung eines Richters.

UMSETZUNG BIS JULI 2017

Die Bundesnetzagentur muss vor der Umsetzung einen Anforderungskatalog mit detaillierten Verpflichtungen erstellen und spätestens am 1. Januar 2017 veröffentlichen. Die Provider – also auch die Deutsche Telekom – müssen diese Pflichten dann spätestens ab dem 1. Juli 2017 erfüllen.

§ 113d Telekommunikationsgesetz (TKG) verpflichtet Provider, dass sie die gespeicherten Daten durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung schützen. Zu diesen Maßnahmen zählen

- der Einsatz besonders sicherer Verschlüsselungsverfahren;
- die Speicherung der Daten in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen;
- die Entkoppelung von aus dem Internet erreichbaren Datenverarbeitungssystemen;
- die Beschränkung des Zutritts zu den Datenverarbeitungsanlagen auf ausschließlich besonders ermächtigte Mitarbeiter der Provider sowie
- die notwendige Mitwirkung von mindestens zwei Personen beim Zugriff auf die Daten (Vieraugenprinzip).

Viele dieser Maßnahmen erfüllt die Deutsche Telekom bereits heute. Sie wird ihren Beitrag zur Herstellung beziehungsweise Gewährleistung des Vertrauens ihrer Kunden in die Datensicherheit dadurch leisten, dass sie Maßnahmen zur Datensicherheit mit besonderer Sorgfalt betreiben wird.

SICHERHEIT VERSUS PERSÖNLICHKEITSRECHTE

Die viel diskutierte Wiedereinführung der Vorratsdatenspeicherung ist eine Entscheidung der Politik. Als Anbieter von Telekommunikationsdiensten für die Öffentlichkeit wird die Deutsche Telekom den gesetzlichen Verpflichtungen nachkommen, die Daten sicher speichern, Missbrauch verhindern und sie löschen, sobald die Fristen abgelaufen sind. Jedoch muss der Staat seine Sicherheitsbedürfnisse gegenüber den Freiheits- und Persönlichkeitsrechten der Nutzer von Telekommunikationsdiensten angemessen würdigen. Bürger müssen sich in der Kommunikation frei und unbeobachtet fühlen können.

Unabhängig davon wird die Telekom ihre Transparenzbemühungen gerade auch im sensiblen Bereich der Telekommunikationsüberwachung und Datenherausgabe weiter fortsetzen. Denn Transparenz schafft Vertrauen und Vertrauen ist elementarer Bestandteil für die Nutzung digitaler Dienste und Services. Ein wesentlicher Baustein dafür ist der Transparenzbericht über die verpflichtende Zusammenarbeit mit Sicherheitsbehörden, den die Telekom 2016 aktualisieren und erstmals auf internationale Konzerngesellschaften ausweiten wird.

IT-SICHERHEITSGESETZ BRINGT NEUE PFLICHTEN

AM 25. JULI 2015 IST DAS NEUE IT-SICHERHEITSGESETZ IN KRAFT GETRETEN. MIT DEM GESETZ WILL DIE BUNDESREGIERUNG DIE IT-SICHERHEIT IN DEUTSCHLAND SIGNIFIKANT VERBESSERN.

Die Bundesregierung hat die Gewährleistung von Sicherheit im Cyberraum und den Schutz der „Kritischen Infrastrukturen“ zur wesentlichen Maßnahme der Cybersicherheitsstrategie erklärt. Das Gesetz soll unter anderem helfen, die heute sehr unterschiedlichen Schutzniveaus innerhalb der kritischen Sektoren – Energie, Transport- und Verkehrswesen, Wasser, Finanz- und Versicherungswesen, Gesundheit, Ernährung, Telekommunikations- und Informationstechnik – in Bezug auf deren IT anzugleichen.

KLAR GEREGELTE AUSKUNFTSPFLICHT

2015 SIND DIE DISKUSSIONEN ÜBER DIE SPIONAGETÄTIGKEITEN AUSLÄNDISCHER UND INLÄNDISCHER GEHEIMDIENSTE UND DEREN RECHTLICHE BEFUGNISSE FORTGESETZT WORDEN. DIE DEUTSCHE TELEKOM HAT SICH IN DIE DISKUSSION EINGEBRACHT UND DIE UMFASSENDE ÜBERWACHUNG DURCH AMERIKANISCHE GEHEIMDIENSTE KRITISIERT SOWIE DIE AUFKLÄRUNG DIESER VORGÄNGE GEFORDERT.

In der Debatte hat die Telekom sich für Transparenz hinsichtlich der gesetzlich zwingend vorgeschriebenen Mitwirkungspflichten der Telekommunikationsanbieter bei der Überwachung von Telekommunikationsverkehren eingesetzt.

Die Deutsche Telekom gewährt den Zugriff auf Telekommunikationsverkehre und -daten nur dann, wenn sie hierzu gesetzlich verpflichtet ist. Gänzlich verboten ist eine Kooperation mit ausländischen Geheimdiensten. Es gab und gibt auch keine Anhaltspunkte, dass jemand die Infrastruktur manipuliert und sich Geheimdienste selbst Zugang zu den technischen Einrichtungen verschafft haben könnten.

Die rechtliche Grundlage für die Pflicht aller Provider zur Zusammenarbeit mit deutschen Sicherheitsbehörden ergibt sich aus dem BND-Gesetz, dem G-10-Gesetz und dem Telekommunikationsgesetz (§§ 110 ff. TKG). Sie regeln detailliert, was die Sicherheitsbehörden dürfen und was die Telekom tun muss. Die technischen Bedingungen hat der Bund in der Telekommunikationsüberwachungsverordnung festgelegt.

So muss dem BND beispielsweise an einem Punkt im Inland die vollständige Kopie der zur Überwachung angeordneten Kommunikation übergeben werden. Telekommunikationsunternehmen haben in ihren Räumen den Zutritt von BND-Mitarbeitern zu ermöglichen und die Aufstellung von technischer Ausrüstung des BND zu dulden. Aber auch hier gilt: Die Deutsche Telekom hält sich streng an die rechtlichen Grundlagen, wahrt das Fernmeldegeheimnis und schützt die Kundendaten.

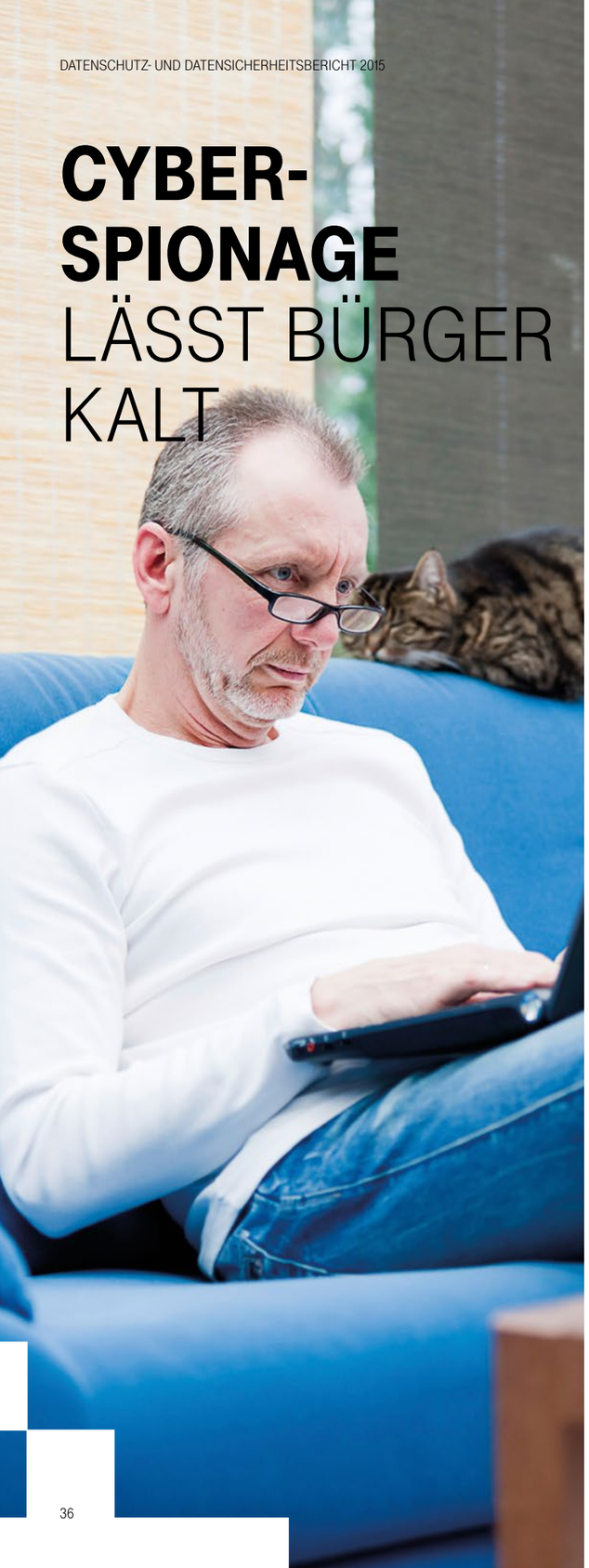
Gesetzlich verboten ist den Providern, über konkrete Überwachungsmaßnahmen zu sprechen. Wer das missachtet, macht sich strafbar. Die Deutsche Telekom beachtet dieses Verbot selbstverständlich im Rahmen ihrer Transparenzschaffung. Im NSA-Untersuchungsausschuss des Deutschen Bundestags haben sich Zeugen der Telekom daher immer dann nicht öffentlich geäußert, wenn eine öffentliche Aussage rechtlich verboten war.

Für die Zusammenarbeit mit Sicherheitsbehörden hat die Deutsche Telekom in Deutschland Regionalstellen für staatliche Sonderauflagen (ReSAs) eingerichtet. Die dortigen Mitarbeiter bearbeiten die Anordnungen von Gerichten und Behörden. Zudem müssen sie an die Inhabern von Film- und Musikrechten Auskunft zu IP-Adressen erteilen (§ 101 UrhG). Auch die Zusammenarbeit mit dem BND gehört zu ihren Aufgaben, beansprucht aber weniger als ein Prozent ihrer Arbeitszeit.

In Fall einer gerichtlichen oder behördlichen Anordnung prüft die Deutsche Telekom – soweit möglich –, ob die rechtlichen Voraussetzungen erfüllt sind. Die einzelnen Bearbeitungsschritte von behördlich angeordneten Überwachungsmaßnahmen werden ausführlich dokumentiert und unterliegen der regelmäßigen Kontrolle durch den Sicherheitsbevollmächtigten sowie durch die Bundesnetzagentur. Zusätzlich unterliegen diese Vorgänge der Prüfung des Datenschutzbeauftragten und der internen Revision der Telekom.

Die Deutsche Telekom war sowohl im Rahmen des Gesetzgebungsverfahrens als auch bei der noch andauernden Ausgestaltung der KRITIS-Verordnung als sachverständiges Unternehmen aktiv beteiligt. Aus dem Gesetz ergibt sich für die Telekom eine Reihe neuer Pflichten. Dazu gehören insbesondere weitreichende Informationspflichten gegenüber der Bundesnetzagentur (BNetzA) sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI). So muss die Telekom den Eintritt oder auch nur die Wahrscheinlichkeit des Eintritts von Störungen an Telekommunikationsanlagen und -diensten oder IT-Technik melden.

Sicherheitsrisiken für den Betrieb von Telekommunikations- und IT-Anlagen lauern oftmals in der von Nutzern eingesetzten Hard- und Software und können auch über soziale Netzwerke sowie Messenger (Over-the-top-Dienste OTT) schnell und unübersichtlich verteilt werden. Um das Sicherheitsniveau spürbar anzuheben, ist es unerlässlich, auch Hard- und Softwarehersteller sowie OTT dem Anwendungsbereich des IT-Sicherheitsgesetzes zu unterstellen. Europa ist hinsichtlich der Berücksichtigung der OTT einen Schritt weiter. Auch der deutsche Gesetzgeber sollte daher alle relevanten Marktteilnehmer schnellstmöglich einbeziehen.



CYBER-SPIONAGE LÄSST BÜRGER KALT

DER SICHERHEITSREPORT 2015 ZEIGT: TROTZ DER VIELEN MELDUNGEN ÜBER HACKERANGRIFFE, GESTOHLENE ZUGANGSDATEN UND NSA-ABHÖRMASSNAHMEN MACHEN SICH DIE BÜRGER HEUTE KAUM SORGEN ÜBER CYBERRISIKEN.

Beim Thema Datenbetrug im Internet machen sich derzeit 28 Prozent der Bevölkerung große Sorgen, zwischen 2011 und 2014 bewegte sich der Anteil zwischen 27 und 31 Prozent. Auch die Sorgen in Bezug auf den Missbrauch von persönlichen Daten durch Unternehmen oder Nutzer in sozialen Netzwerken bewegen sich am unteren Ende der bislang gemessenen Werte. In Computerviren sehen heute mit 21 Prozent ebenfalls kaum mehr Menschen ein Risiko als noch vor ein, zwei Jahren.

SORGE VOR ÜBERWACHUNG SINKT

Überraschend ist die Sorge, dass andere Staaten wie die USA oder China die Internet- und Telefonverbindungen deutscher Bürger überwachen könnten, im Vergleich zum Vorjahr von 19 Prozent auf 15 Prozent zurückgegangen. Aber: Gefragt, welche Risiken in Zukunft zunehmen werden, nennen etwa 70 Prozent der Befragten den Missbrauch persönlicher Daten durch Unternehmen sowie Datenbetrug im Internet.

Hier tritt ein offenbar widersprüchlicher Befund zutage: Einerseits kennt die Bevölkerung zwar die Risiken und geht davon aus, dass diese künftig weiter wachsen werden. Andererseits nehmen die persönliche Betroffenheit und Sorge nicht zu, mitunter sogar ab. Die Allensbacher Meinungsforscher erklären die vermeintlich widersprüchlichen Ergebnisse mit einem weitgehenden Gleichmut in der Gesellschaft gegenüber diesem wachsenden Problem sowie teilweise mit Informationsdefiziten. Aber auch Gewöhnungseffekte und ein gewisser Fatalismus sowie das Empfinden, persönlich nicht betroffen zu sein, kommen laut den Meinungsforschern in diesen Ergebnissen zum Ausdruck.

VERTRAUENSWÜRDIGE TELEKOM

Was den Umgang von Unternehmen der Kommunikations- und Internetbranche mit persönlichen Daten angeht, schenkt die Bevölkerung der Telekom mit Abstand das größte Vertrauen. 46 Prozent halten die Telekom für vertrauenswürdig. Damit hat die Telekom einen fast doppelt so großen Vorsprung vor den nächstplatzierten Unternehmen (24 Prozent).

Das Institut für Demoskopie Allensbach und das Centrum für Strategie und Höhere Führung haben den Sicherheitsreport 2015 im Auftrag der Deutschen Telekom erstellt. Das Institut Allensbach befragte im Sommer 2015 mit knapp 1.400 Interviews einen repräsentativen Querschnitt der Bevölkerung ab 16 Jahre.

SIND CYBERANGRIFFE DAS GRÖSSTE RISIKO FÜR INDUSTRIE 4.0?

INDUSTRIE 4.0 BRAUCHT FÜR DEN ERFOLG EINEN BESSEREN SCHUTZ VOR CYBERANGRIFFEN: FAST 90 PROZENT DER ENTSCHEIDER AUS POLITIK UND WIRTSCHAFT SEHEN LAUT CYBER SECURITY REPORT 2015 IT-SICHERHEIT ALS DIE GRÖSSTE HERAUSFORDERUNG FÜR DIE FLÄCHENDECKENDE UMSETZUNG VON INDUSTRIE-4.0-KONZEPTEN.

Mehr als die Hälfte (53) der Unternehmen in der verarbeitenden Industrie hat sich schon mit speziellen IT-Sicherheitskonzepten für den Produktionsbereich auf die zunehmende Digitalisierung eingestellt. 45 Prozent verfügen über Sicherheitslösungen für den Datenaustausch zwischen Produktionssteuerung und Produktion. Aus gutem Grund: Denn mehr als ein Drittel (36) der deutschen Unternehmen wird nach eigener Aussage mehrmals die Woche oder täglich von Cyberkriminellen angegriffen. Neun von zehn Unternehmen sind bereits Opfer von IT-Angriffen gewesen. „Wir müssen davon ausgehen, dass es zudem eine hohe Dunkelziffer unerkannter Angriffe gibt“, sagt Anette Bronder, Director der Digital Division von T-Systems und somit verantwortlich für Industrie 4.0. „Es gibt Untersuchungen, dass es oft mehrere Monate dauert, bis ein Angriff überhaupt erkannt wird.“

Trotz der hohen Zahl der Angriffe fühlen sich Unternehmen anscheinend sicher. Nur zwölf Prozent sehen ein sehr großes Risiko darin, dass ein Hackerangriff sie gravierend schädigen könnte. Dazu passt die Aussage von 60 Prozent der Entscheider in den Unternehmen, ihre IT sei so gut wie möglich auf Angriffe vorbereitet. Diese Aussagen bestätigen, dass das Gefühl der Bedrohung sehr eng mit konkreten Vorfällen korreliert. Passiert wenig oder dringen keine spektakulären Fälle in die Öffentlichkeit, dann verdrängen die Unternehmen die Gefahren wieder, da sie sich nach wie vor eher ungern mit dem Thema IT-Sicherheit befassen.

92 Prozent der Führungskräfte in mittleren und großen Unternehmen sagen, dass IT-Sicherheit in ihrem Unternehmen einen hohen bis sehr hohen Stellenwert hat. Teilweise deutlich gestiegen sind die Ausgaben für IT-Sicherheit: 29 Prozent geben jetzt erheblich mehr aus als vor einigen Jahren, knapp die Hälfte (49) etwas mehr. Hartnäckig hält sich die Meinung, dass Cloud Services unsicher sind. Nur 24 Prozent der Führungskräfte halten Cloud Computing für sicher. Damit hat sich das Vertrauen in Cloud Computing in den vergangenen fünf Jahren kaum verändert.

Die vom Institut für Demoskopie Allensbach und vom Centrum für Strategie und Höhere Führung Bodman im Auftrag der Deutschen Telekom durchgeführte repräsentative Studie stützt sich auf 645 Telefoninterviews mit Politikern (113 Abgeordnete) sowie Top-Führungskräften aus mittleren und großen Unternehmen (532).

EUROPÄISCHE SICHERHEITS-RICHTLINIE

AUCH DIE EUROPÄISCHE EBENE WILL DIE IT-SICHERHEIT VERBESSERN. IN DER LETZTEN TRILOGVERHANDLUNG IM DEZEMBER 2015 HABEN SICH RAT, PARLAMENT UND DER AUSSCHUSS DER STÄNDIGEN VERTRETER DER MITGLIEDSSTAATEN AUF EINEN KOMPROMISS GEEINIGT. DIE EU WILL EINE EUROPÄISCHE RICHTLINIE VERABSCHIEDEN, WELCHE MASSNAHMEN EINER HOHEN GEMEINSAMEN NETZ- UND INFORMATIONSSICHERHEIT (NIS-RICHTLINIE) DEFINIERT.

Der Kompromiss sieht vor, neben den Betreibern „klassischer“ kritischer Infrastrukturen wie beispielsweise Telekommunikation, Informationstechnologie, Energie und Wasser auch „Digital Service Provider“ (OTTs) mit Sicherheitsmaßnahmen in die Pflicht zu nehmen. Dazu gehören E-Commerce-Plattformen wie eBay und Amazon oder Suchmaschinen wie Google sowie Anbieter von Cloud-Services. Sie sollen aber einem leichteren Regelungsregime als Telekommunikationsbetreiber unterliegen. In der ersten Lesung des Entwurfs waren die OTTs zunächst komplett gestrichen worden. Auch die Telekom hatte gefordert, OTTs in den Anwendungsbereich der NIS aufzunehmen.

Hard- und Softwarehersteller sowie soziale Netzwerke bleiben dagegen außen vor. Sie sollen über neue Datenschutzregelungen stärker reguliert werden. Insoweit greifen deutsche und europäische Regelungen zur Anhebung der IT-Sicherheit heute noch zu kurz. Das deutsche IT-Sicherheitsgesetz (IT-SicherheitsG) räumt den Behörden zwar zumindest die Möglichkeit ein, Hard- und Softwarehersteller zur Mitwirkung bei der Störungsbeseitigung anzuhalten. Eine unmittelbar aus dem Gesetz folgende Verpflichtung dieser Marktteilnehmer sieht das IT-SicherheitsG aber nicht vor. Soziale Netzwerke werden von beiden Regelungswerken bislang nicht erfasst, obwohl sie Angreifern die Möglichkeit bieten, Angriffe auf Netze und Infrastrukturteile von IKT-Unternehmen zu realisieren, weswegen sie aus Sicht der Telekom zwingend einzubeziehen sind.

Parlament und Rat werden Anfang 2016 die Richtlinie formell beschließen. Die Mitgliedsstaaten müssen die Regelungen der NIS-Richtlinie dann innerhalb von 21 Monaten in nationales Recht umsetzen. Aus gesellschaftlicher, aus Unternehmens- und aus Kundensicht bleibt zu wünschen, dass die Pflicht zur Schaffung einer zufriedenstellenden IT-Sicherheit nicht auf den Kreis der heute bereits verpflichteten Unternehmen beschränkt bleibt, sondern schnellstmöglich alle sicherheitsrelevanten Marktteilnehmer ihren Beitrag leisten müssen.

DATENSCHUTZ IM TAGESGESCHÄFT

WIE SCHÜTZT MAN PERSONENBEZOGENE DATEN IN IT- UND KOMMUNIKATIONSSYSTEMEN? MIT EINEM NEUEN ROLLENKONZEPT SORGT DIE TELEKOM FÜR EIN EINHEITLICHES VORGEHEN UND KLARE VERANTWORTLICHKEITEN.

Welche Mitarbeiterdaten darf eine Personalsoftware nutzen, um Gehälter datenschutzkonform abzurechnen? Worauf darf eine CRM-Lösung zugreifen, um eine Marketingkampagne so durchzuführen, dass die Schutzrechte der Kunden gewahrt bleiben? Fragen wie diese stellen sich im Geschäftsalltag permanent und müssen verbindlich beantwortet werden. Wie die Vorgaben in der Praxis umgesetzt werden, ist von Unternehmen zu Unternehmen verschieden. Um das Vorgehen verbindlicher zu machen, führt die Telekom ab Anfang 2016 ein festes Rollenkonzept ein, das sukzessive auf die internationalen Gesellschaften übertragen werden soll.

Auf der Ebene des Managements setzt jede Gesellschaft einen Datenverantwortlichen ein. Dieser verantwortet neben dem Datenschutz auch den Umgang mit sonstigen sensiblen Daten wie etwa Geschäftsgeheimnissen. Nicht zu verwechseln ist der Datenverantwortliche mit dem Datenschutzbeauftragten. Der Datenschutzbeauftragte bildet eine gesetzliche Kontrollinstanz im Unternehmen, die unabhängig ist und die Einhaltung der gesetzlichen und unternehmensinternen Vorgaben überwacht. Demgegenüber hat der Datenverantwortliche die Aufgabe, diese Anforderungen in die Praxis umzusetzen. Hierzu muss er für jede IT-Lösung, in der zu schützende Daten verarbeitet werden, einen konkret zuständigen fachseitigen Systemverantwortlichen benennen.

Der fachseitige Systemverantwortliche klärt auf der Ebene des einzelnen Systems, welche Datenverarbeitung zulässig ist. Datenschutz- und geschäftsgeheimniskonform legt er fest, welche Daten verarbeitet werden dürfen, um die mit der Anwendung beabsichtigten fachlichen Zwecke zu erreichen. Zum Beispiel gibt er der bereits erwähnten Gehaltsabrechnung vor, dass das System nur auf die Namen und die Kontoverbindungen der Mitarbeiter zugreifen darf, nicht aber auf andere Informationen.

Der fachseitige Datenverantwortliche wird von sogenannten technischen Systemverantwortlichen unterstützt, welche in der Regel beim Dienstleister angesiedelt sind und die technische Umsetzung der fachlichen Anforderungen durchführen. Als IT-Dienstleister tragen sie außerdem Sorge dafür, dass alle Schutzvorgaben der Fachseite korrekt implementiert sind und die technischen und organisatorischen Sicherheitsmaßnahmen vollständig greifen.

DATENSCHUTZKENNTNISSE WEITER AUF HOHEM NIVEAU

WAS WISSEN MITARBEITER ÜBER DATENSCHUTZ? WIE STARK WENDEN SIE IHR KNOW-HOW IN DER PRAXIS AN? DAS KONZERNDATENSCHUTZAUDIT DER TELEKOM GIBT JÄHRLICH AUSKUNFT. 2015 BESTÄTIGTEN DIE KENNZAHLEN DAS HOHE NIVEAU DES VORJAHRES.

Verschlüsseln Sie vertrauliche E-Mails? Welche Informationen sind überhaupt vertraulich? Welche sogar streng vertraulich? Praxisbezogene Fragen wie diese stehen im Mittelpunkt des Konzerndatenschutzaudits, mit dem die Telekom den aktuellen Wissensstand ihrer Mitarbeiter zum Thema Datenschutz überprüft. Zudem blickt die jährliche Online-Umfrage auch auf die Anwendungspraxis. Wie stark nutzen die Mitarbeiter ihr Wissen im Tagesgeschäft? Machen sie zum Beispiel Gebrauch von Praxiswerkzeugen wie dem Passwortmanager, den der Konzern zentral anbietet?

2015 zeigte sich das Datenschutzniveau in der Telekom unverändert hoch. Die Hauptkennzahl, mit der die Prüfer die zahlreichen Einzelergebnisse ihres Audits zusammenfassen, erreichte sowohl national (9,5 von 10) als auch international (7,8 von 10) die Werte des Vorjahres. Insgesamt wurden 51.000 repräsentativ ausgewählte Mitarbeiter befragt. Die Rücklaufquote stieg vor allem in Deutschland noch einmal signifikant an. Mit 86 Prozent lag sie vier Punkte über dem Ergebnis von 2014.

Die Datenschützer der Telekom führen diesen Anstieg auf die verstärkte Zusammenarbeit mit ihren Kollegen von der Konzernsicherheit zurück, die ebenfalls eine jährliche Umfrage durchführen und darin das Sicherheitsbewusstsein der Mitarbeiter untersuchen. Beide Befragungen fanden nun erstmals zeitgleich statt. Dabei wurde sichergestellt, dass die zufällig ausgewählten Teilnehmer jeweils nur zu einer der beiden Umfragen eingeladen wurden. Angesichts der hohen Zahl der Befragten war es in den vorangegangenen Jahren immer wieder vorgekommen, dass Mitarbeiter doppelt befragt wurden. Dies ist mit der neuen, gemeinsamen Vorgehensweise ausgeschlossen.

WELTWEITE ZUSAMMENARBEIT IN DER DATENSCHUTZ-GOVERNANCE

DIE TELEKOM STÄRKT DIE ROLLE IHRER NATIONALEN DATENSCHUTZBEAUFTRAGTEN. VIELE NEHMEN INZWISCHEN SOGAR AN KONTROLLEN IM AUSLAND TEIL.

2015 hat der Konzerndatenschutz der Telekom damit begonnen, die Datenschutzbeauftragten der Landesgesellschaften an Kontrollbesuchen in anderen Ländern zu beteiligen. Mehr und mehr nationale Datenschützer nehmen die Gelegenheit zum internationalen Austausch wahr. Beispielsweise nahm ein Mitarbeiter der Datenschutzbeauftragten der rumänischen Telekom-Tochter im September an Kontrollbesuchen in Schweden und Dänemark teil, um die Kollegen der Konzernzentrale zu unterstützen.

Die Auslandseinsätze sind Teil des sogenannten Empowerment-Programms, mit dem die Konzerndatenschützer das Wissen und die Fähigkeiten ihrer nationalen Kollegen fördern wollen. Die Initiative zielt darauf ab, die Verantwortlichen aus den Landesgesellschaften noch einmal deutlich stärker als bisher in die Arbeit der Zentrale einzubeziehen. Ein weiterer wichtiger Baustein des Programms sind länderübergreifende Arbeitsgruppen zu aktuellen Themen, denen sich die Datenschützer weltweit stellen müssen. Auf der gemeinsamen Agenda stehen zum Beispiel Big Data oder die neue europäische Datenschutzgrundverordnung.

Der Ausbau der internationalen Zusammenarbeit geht inzwischen auch dahin, dass die nationalen Datenschutzbeauftragten an der zentralen Planung der Datenschutzkontrollen teilnehmen. Zudem schauen die Datenschützer der Telekom auch immer mehr über den eigenen Tellerrand hinaus. Um potenzielle Synergien besser auszuschöpfen, bilden sie Allianzen mit den Kollegen aus den Bereichen Konzernsicherheit und Revision. Ziel ist die engere Verzahnung der jeweiligen Fachprüfungen. 2015 führte dies unter anderem zur gemeinsamen Durchführung des Konzerndatenschutzaudits (vgl. nebenstehenden Artikel) und der Awareness-Umfrage der Konzernsicherheit.

WELTWEIT EINHEITLICHER DATENSCHUTZ

DURCH DIE BINDING CORPORATE RULES PRIVACY (BCRP) GILT INNERHALB DER TELEKOM WELTWEIT EINE EINHEITLICHE DATENSCHUTZRICHTLINIE FÜR ALLE TOCHTERGESELLSCHAFTEN. DAVON PROFITIEREN KUNDEN UND MITARBEITER GLEICHERMASSEN.

Ende 2015 war es so weit: Mit dem Beitritt der griechischen Telekom-Gruppe „OTE“ zum Kreis der Unterzeichner gilt die neue Konzernrichtlinie Datenschutz nun auch in Griechenland und bei deren Tochtergesellschaften in Rumänien. Zuvor hatten nahezu alle anderen europäischen sowie alle afrikanischen, asiatischen und lateinamerikanischen Landesgesellschaften die neu gefassten Datenschutzbestimmungen unterzeichnet. Auch in den Vereinigten Staaten nutzen die Deutsche Telekom Inc. und die T-Systems North America das gemeinsame Regelwerk, um den Datentransfer aus der Europäischen Union auf eine rechtssichere Basis zu stellen.

Die Binding Corporate Rules Privacy (BCRP) treten an die Stelle des Privacy Code of Conduct aus dem Jahr 2004. Die Richtlinie regelt den Umgang mit Daten von Kunden, Mitarbeitern und Geschäftspartnern. Umfassend legen die BCRP fest, zu welchen Zwecken personenbezogene Daten erhoben, gespeichert und verarbeitet werden dürfen. Das Regelwerk steht im Einklang mit dem Bundesdatenschutzgesetz und der Europäischen Datenschutzrichtlinie. Gleichzeitig werden bereits heute die wesentlichen Anforderungen erfüllt, die durch die Einführung der Europäischen Datenschutzgrundverordnung künftig von den Unternehmen eingehalten werden müssen.

Neben den Kunden profitiert davon auch das Unternehmen: Durch den erfolgreichen Abschluss eines umfangreichen europäischen Genehmigungsverfahrens wird die Konzernrichtlinie von allen europäischen Datenschutzaufsichtsbehörden anerkannt. Daher können die europäischen Landesgesellschaften personenbezogene Daten an außereuropäische Schwesterunternehmen übermitteln, ohne dafür jeweils noch Einzelfallgenehmigungen einholen zu müssen.

Weiterer Vorteil: Da sich die BCRP am vergleichsweise weit reichenden europäischen Datenschutzrecht orientieren und in Teilbereichen sogar darüber hinausgehen, haben außereuropäische Landesgesellschaften eine gute Ausgangsposition, um Verschärfungen ihres jeweiligen Landesrechts gelassen mitnehmen zu können. So geschehen in Südafrika, wo es lange Zeit keine staatlichen Datenschutzregelungen gab. Ersatzweise hatte die dortige Landesgesellschaft ihren Umgang mit personenbezogenen Daten nach den Vorgaben der BCRP geregelt. Als die südafrikanische Regierung dann 2014 relativ kurzfristig eine neue Gesetzgebung verabschiedete, entsprach das Vorgehen der Telekom bereits den neuen Anforderungen.

TELEKOM APPS AUF DEM PRÜFSTAND

WIRD BEI DER ENTWICKLUNG VON APPS DER DATENSCHUTZ VERNACHLÄSSIGT? SIND SIE UNSICHERER ALS PC-PROGRAMME? DIE TELEKOM WOLLTE ES GENAUER WISSEN UND PRÜFTE DAS DATENSCHUTZ- UND DATENSICHERHEITSNIVEAU DER 30 BELIEBTESTEN TELEKOM APPS.

Der App-Markt wächst unaufhaltsam. 2015 sollen die Deutschen laut Branchenverband Bitkom 3,4 Milliarden Apps auf ihre Smartphones und Tablets heruntergeladen haben. Tendenz weiter steigend – zumal die Zutrittsbarrieren in den App-Markt niedrig erscheinen. Mit agilen Methoden lassen sich Programme vergleichsweise schnell und unkompliziert entwickeln. Da ist die Gefahr groß, dass App-Anbieter Datenschutz- und Datensicherheitsanforderungen nicht im nötigen Umfang berücksichtigen. Dies birgt einigen Zündstoff, denn Apps können Zugriff auf große Mengen personenbezogener Daten haben.

Im Oktober 2015 überprüften die Datenschutz- und Datensicherheitsexperten der Telekom das Schutzniveau der unternehmenseigenen Apps. Dabei lag der Fokus auf den Apps, die in den Downloadstores von Apple und Google am meisten nachgefragt sind. Die Spannweite der so getesteten 30 Apps reichte von der Cloud-Speicherlösung „Mediencenter“ über die Telekom Mail App bis zur Smart Home App, mit der sich die Smart-Home-Komponenten eines Wohnhauses auch von unterwegs aus steuern lassen.

REALITY-TEST FÜR APPS

Auf Grundlage der Telekom Datenschutzanforderung für die App-Entwicklung erstellten die Tester eine umfangreiche Liste von Prüfanforderungen. In einem Self-Assessment gaben die zuständigen Produktmanager Auskunft zum Status quo ihrer Apps. Die Antworten unterzogen die Prüfer dann einem Reality-Test. Unter anderem klärten sie ab, wie und wann die Apps die geforderten Datenschutzhinweise bereitstellen: Kann sich der Kunde bereits im Store – also noch vor dem Download der Software – ausreichend informieren? Wie detailliert sind die Datenschutzhinweise? Wie viele Klicks erfordert es, sie aufzufinden? Setzt die App das Privacy Icon der Telekom ein, um dem Kunden die Suche zu erleichtern?

Die Datensicherheitsprüfung erfolgte auf Basis der Sicherheitsanforderungen, welche die Telekom für eine sichere iOS- und Android-Programmierung aufgestellt hat. Hierbei kamen sowohl statische als auch dynamische Analyseverfahren zum Einsatz. In dynamischen Analyseverfahren wird die App unter kontrollierten Bedingungen ausgeführt, sodass sich ihr tatsächliches Verhalten bewerten lässt, zum Beispiel bei den Themen Verschlüsselung und Netzwerkverkehr. Demgegenüber konzentrieren sich statische Analysen auf den Programmcode und die Berechtigungen der Apps. Zudem wird eine Schwachstellenprüfung der Backend-Server durchgeführt.

Die Tester waren insgesamt zufrieden mit dem Ergebnis, konnten aber durchaus auch Verbesserungsmöglichkeiten ermitteln. Interessanterweise konnte auch festgestellt werden, dass die Ergebnisse zum Teil auch von Betriebssystem zu Betriebssystem – also von Android zu iOS – variierten. Beispielsweise gab es Apps, die in der iOS-Version relativ gut abschnitten, dann jedoch Mängel in der Android-Version aufwiesen.

DATENSPARSAMKEIT UND ZWECKBINDUNG

Häufigster Kritikpunkt der Tester waren Schwächen bei den Datenschutzhinweisen. Diese betrafen teilweise die inhaltliche Gestaltung, aber ebenso die Auffindbarkeit innerhalb der App. Leider verwendeten auch noch nicht alle Apps das Privacy Icon der Telekom. Dabei handelt es sich um ein von der Telekom entwickeltes Datenschutzsymbol, das den Nutzer auf Privacy-by-Design-Funktionen hinweisen soll. Besonders hervorzuheben ist, dass es beim Prüfpunkt Datensparsamkeit und Zweckbindung gute Ergebnisse gab. Somit steht fest, dass die Apps keine persönlichen Daten der Nutzer speichern oder verwenden, welche nicht für die Funktionsfähigkeit der jeweiligen App benötigt werden.

Auch beim Schutzniveau bezüglich Datensicherheit zeigte sich noch Optimierungspotenzial. Um darüber hinaus die aktuellsten Gefährdungen mit auf dem Radar zu haben, banden die Sicherheitsexperten der Telekom das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) für die Schwachstellenanalyse mit ein. Diese stellten eine Prüfsoftware bereit zur Überprüfung kritischer potenzieller Sicherheitslücken, die von Angreifern bevorzugt genutzt werden. Ihre Ergebnisse spiegelten die Prüfer den Produktverantwortlichen detailliert wider zur Abarbeitung der festgestellten Schwächen.

TÜV-DATENSCHUTZSIEGEL FÜR DIE ABRECHNUNG

TELEFONRECHNUNGEN SIND VERTRAUENSSACHE. 2015 ZERTIFIZIERTE DER TÜVIT ERNEUT DIE ABRECHNUNGSPROZESSE BEI DER TELEKOM DEUTSCHLAND. DATENSCHUTZ UND DATENSICHERHEIT STANDEN IM FOKUS DER PRÜFER.

Monat für Monat erstellt die Telekom allein im Privatkundensegment in Deutschland etwa 27 Millionen Telefonrechnungen. Für jeden Kunden gilt es dabei Hunderte, oft sogar Tausende von Verkehrsdaten zeitgenau abzurechnen. Die Kunden erwarten einen ebenso korrekten wie sensiblen Umgang mit ihren Daten. Eine alles andere als triviale Aufgabe. Sie beginnt mit dem Erheben und Vorverarbeiten der Daten und reicht über die eigentliche Rechnungslegung bis zum Schreiben, Ausliefern und Archivieren der Dokumente. Entlang dieser Prozesskette arbeitet eine Vielzahl unterschiedlicher IT-Lösungen zusammen. 2015 hat der TÜViT sämtliche Prozessschritte und die darin eingebundenen IT-Systeme auditiert. Hierbei bewerteten die Prüfer sowohl den Datenschutz als auch die IT-Sicherheit. Mit dem TÜV-Siegel bescheinigen sie der Telekom den gesetzeskonformen und sicheren Umgang mit den Daten ihrer Kunden.

DATENSCHUTZ IN DER CLOUD

DAS KOMPETENZZENTRUM TRUSTED CLOUD HAT PRÜFKRITERIEN ENTWICKELT, MIT DENEN SICH DAS DATENSCHUTZNIVEAU VON CLOUD-DIENSTEN UMFASSEND BEURTEILEN LÄSST. DER TÜV INFORMATIONSTECHNIK (TÜVIT) TESTET DAS NEUE VORGEHEN NUN AUF PRAXISTAUGLICHKEIT.

Mit dem Programm Trusted Cloud fördert das Bundesministerium für Wirtschaft und Energie (BMWi) die Entwicklung und Erprobung innovativer, sicherer und rechtskonformer Cloud-Lösungen. Der neue Datenschutz-Prüfkatalog setzt auf den ISO / IEC-Normen der 2700x-Familie auf – den meistgebräuchlichen internationalen Zertifizierungsstandards. In Teilen gehen die Anforderungen des Bundesdatenschutzgesetzes jedoch darüber hinaus. Wo genau dies der Fall ist, spiegelt sich in den Prüfkriterien wider, die das BMWi im Frühjahr 2015 vorgestellt hat. Für die Erstellung des Prüfkatalogs hatte das Kompetenzzentrum Trusted Cloud Vertreter der Datenschutzbehörden und Experten aus Wissenschaft, Anwaltschaft und Wirtschaft an einen gemeinsamen Tisch geholt. Darunter waren auch Datenschützer der Telekom, die insbesondere Praxiswissen zur Definition der Schutzbedarfsklassen beisteuerten.

Die neuen Prüfgrundlagen sind der letzte Baustein eines umfassenden Zertifizierungsrahmens für den deutschen Rechtsraum. Im Auftrag des Kompetenzzentrums führt der TÜViT sechs Pilotzertifizierungen durch, die bis zur CeBIT 2016 abgeschlossen sein sollen. Die Telekom ist mit einem Software-as-a-Service(SaaS)-Angebot vertreten, das es Unternehmen erlaubt, ihre Finanzbuchhaltung in einer geschützten Internetumgebung zu führen. Hierbei prüft der TÜViT sowohl die eingesetzte Softwarelösung als auch das Datenhaltungskonzept.

DIGITALISIERUNG UND DATEN-SCHUTZ IM GESUNDHEITSWESEN

BEI DER DIGITALISIERUNG HINKT DAS GESUNDHEITSWESEN IM VERGLEICH ZU ANDEREN BRANCHEN DER ENTWICKLUNG DEUTLICH HINTERHER. DABEI VERBESSERN DIGITALE PROZESSE NICHT NUR DIE VERSORGUNG, SONDERN AUCH DEN DATENSCHUTZ.

Was viele vor wenigen Jahren noch müde belächelten, ist mittlerweile ein Trend – Quantified Self. Immer mehr Menschen – vor allem jüngere – messen ihre Körperdaten und werten sie aus: Gewicht, Puls, Blutzucker, Schlafphasen, Adrenalinspiegel oder Lungenfunktion. Ob das Messen medizinisch Sinn macht oder nicht, sei dahingestellt. Bemerkenswert ist, dass die Fans der Quantified-Self-Bewegung selbst sensibelste Daten ins Netz stellen, um sich beispielsweise mit Gleichgesinnten auszutauschen und ihre Werte zu vergleichen. Zu Fragen des Datenschutzes und der Privatsphäre haben sie eine ganz eigene Haltung: Die Generation Y, die Facebook von der ersten Stunde an nutzte, möchte ganz bewusst auch persönliche Körperdaten mit anderen teilen.

DIGITALISIERUNG BIETET VIELE VORTEILE

Wir leben in einer vernetzten Welt und die Vorteile sind für uns nahezu selbstverständlich. Die Vernetzung macht das Leben komfortabler und einfacher – auch im Gesundheitswesen. Die Telekom stattet zum Beispiel Krankenhäuser mit digitalen Informationssystemen und Ärzte-Tablets aus. Die Geräte helfen, Kosten zu reduzieren, erleichtern Ärzten und Pflegekräften die Arbeit und steigern die Qualität der Pflege. Ein anderes Beispiel ist die Telemedizin. In vielen Regionen Deutschlands – West wie Ost – herrscht Ärztemangel. Mit Telemedizin haben wir die Möglichkeit, die Versorgung zu verbessern, indem wir auch Patienten erstklassig versorgen, die sonst weite Wege zu ihren Ärzten auf sich nehmen müssten.

Oder die Telematikinfrastruktur, welche die elektronische Gesundheitskarte erst ihrem eigentlichen Bestimmungszweck zuführt: dem hochsicheren Austausch von Gesundheitsdaten. Viele Praxen und Krankenhäuser nutzen bereits digitale Daten, aber beim Austausch mit anderen Ärzten oder Kliniken greifen sie noch zum (unsicheren) Faxgerät. Deutschland ist im westlichen Europa das einzige Land, das im Gesundheitswesen auf einen sicheren Onlineaustausch von Daten verzichtet. Dabei bietet die digitale Vernetzung nicht nur schnellere Kommunikation und wirtschaftliche Effizienz, sie beschert uns auch einen handfesten medizinischen Nutzen. Mit elektronischen, jederzeit abrufbaren Notfalldaten stehen dem Arzt wichtige Informationen sofort zur Verfügung. Oder: In Deutschland sterben mehr Menschen an unerwünschten Arzneimittelwirkungen als im Straßenverkehr. Eine simple digitale Übersicht in Verbindung mit einem Onlineabgleich würde Menschenleben retten.

PATIENTENDATEN MÜSSEN BESTMÖGLICH GESCHÜTZT WERDEN

Die Haltung des Quantified Self ist bis auf Weiteres für die medizinische Kernversorgung irrelevant. Die Patienten fordern maximale Sicherheit für ihre Patientendaten. Wir bei der Telekom verstehen dies als Auftrag: Safety first bei der Digitalisierung im Gesundheitswesen! Deshalb werden bei der Telekom sensible Daten stets verschlüsselt versendet und die Daten entsprechend den Vorgaben in hochsicheren Rechenzentren der Telekom in Deutschland gespeichert. Zudem hat sich die Telekom erfolgreich als Auftragsdatenverarbeiter und IT-Dienstleister im Bereich medizinische Bildarchivierung zertifizieren lassen. Das Argument, dass Daten auch in einer aufwendig abgesicherten IT-Umgebung missbraucht werden könnten, ist kein Argument, sich der Digitalisierung im Gesundheitswesen zu entziehen. Die digitale Kommunikation definiert klare Rechte, protokolliert Zugriffe, erfüllt höchste Sicherheitsstandards und verschlüsselt Daten. Werden grundlegende Rechte missachtet, drohen strafrechtliche Konsequenzen. Die Einführung solcher Prozesse stellt für den Datenschutz und damit auch für die Patienten eine enorme Verbesserung dar. In diesem Sinne bewirkt die Digitalisierung keinen schlechteren Datenschutz im Gesundheitswesen, sondern sorgt für einen besseren.

Dr. Axel Wehmeier

ist Geschäftsführer der Telekom Healthcare Solutions. Nach seinem Studium der Volkswirtschaftslehre und Betriebswirtschaftslehre an der University of Texas und an der Kölner Universität arbeitete Axel Wehmeier, Jahrgang 1966, als wissenschaftlicher Mitarbeiter. 1998 promovierte er und setzte seine berufliche Laufbahn als Referent Pricing bei der Deutschen Telekom AG fort. Nach mehreren Stationen bei der Telekom leitet er seit 2010 das Konzerngeschäftsfeld Gesundheit.

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

DATENSCHUTZSIEGEL FÜR BILDARCHIVIERUNG

BEIM UMGANG MIT MEDIZINISCHEN DATEN HABEN DATENSCHUTZ UND DATENSICHERHEIT HÖCHSTE PRIORITÄT. DIE DATENSCHUTZ ZERTIFIZIERUNGS-GESELLSCHAFT (DSZ) HAT DIE MEDIZINISCHE BILD-ARCHIVIERUNGSLÖSUNG DER TELEKOM HEALTHCARE SOLUTIONS, EIN TOCHTERUNTERNEHMEN DER DEUTSCHEN TELEKOM, ZERTIFIZIERT.

In dem Auditverfahren haben die Prüfer der Datenschutz Zertifizierungsgesellschaft mbH (DSZ) Verwaltungs- und Datenverarbeitungsprozesse der „Study-based Archiving Service“ untersucht. Damit archivieren Kliniken und Arztpraxen sicher medizinische Bilddaten und können diese auch anderen Ärzten und Krankenhäusern in digitaler Form zur Verfügung stellen. Dies vermeidet teure Doppelaufnahmen und macht medizinisch notwendige Informationen schnell zugänglich. In Deutschland müssen die Aufnahmen bis zu 30 Jahre lang aufbewahrt werden. Die Zertifizierung garantiert Ärzten und Krankenhäusern, aber auch den betroffenen Patienten, dass die Telekom die hohen Anforderungen bei der Verarbeitung von personenbezogenen Daten zu hundert Prozent erfüllt.

Die Telekom Healthcare Solutions ist das erste Unternehmen aus der Gesundheitsbranche, welches das Datenschutzsiegel nach dem Standard DS-BvD-GDD-01 erhält. „Wir waren positiv überrascht, welch hohe Priorität das Thema Datenschutz bei der Telekom genießt und welch exzellentes Know-how bei dem Unternehmen vorhanden ist, sodass wir die Zertifizierung entsprechend schnell und problemlos vornehmen konnten“, betont Dr. Niels Lepperhoff, Geschäftsführer der DSZ.

Der Standard DS-BvD-GDD-01 wurde von den beiden führenden Datenschutzfachverbänden entwickelt – dem Berufsverband der Datenschutzbeauftragten (BvD) sowie der Gesellschaft für Datenschutz und Datensicherheit (GDD). Das Siegel und der Zertifizierungsablauf erfüllen alle Vorgaben der zuständigen Datenschutzaufsichtsbehörden und gewährleisten damit eine hohe Verlässlichkeit. Durch die Zertifizierung sind sowohl die erforderliche Kompetenz in den fachlichen Grundlagen des Datenschutzes als auch die offizielle Anerkennung der gesetzeskonformen Umsetzung sichergestellt. Neben der medizinischen Bildarchivierung will die Telekom weitere Produkte aus dem Gesundheitssektor zertifizieren lassen.

MOBILFUNKDATEN DATENSCHUTZKONFORM ANONYMISIEREN UND ANALYSIEREN

DIE ANALYSE VON PERSONENBEZOGENEN DATEN IST AUS DATENSCHUTZRECHTLICHEN GRÜNDEN KRITISCH. DIE TELEKOM HAT EIN ANONYMISIERUNGSVERFAHREN FÜR MOBILFUNKDATEN ENTWICKELT, DAS DIE BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT (BFDI) ALS RECHTLICH ZULÄSSIG BEWERTET HAT. ZUSÄTZLICH KONTROLLIEREN UND ZERTIFIZIEREN EXTERNE PRÜFSTELLEN FÜR DATENSCHUTZ DIE VERFAHREN.

Die Motionlogic GmbH, ein 100-prozentiges Tochterunternehmen der Telekom, nutzt das Anonymisierungsverfahren für die Analyse von Verkehrs- und Bewegungsströmen. Sie basieren auf Signalisierungsdaten aus dem Mobilfunk- Netz. Diese Daten fallen immer an, wenn jemand mit dem Handy telefoniert oder eine SMS schickt. Dann werden diese Daten zum Zweck des Netzmanagements an der Mobilfunkzelle gezählt. Weiterhin meldet sich ein Handy in längeren Zeitabständen automatisch im Mobilfunknetz an, wodurch weitere Daten in Bewegungsstromanalysen einfließen können. Zusätzlich lassen sich ausgewählte soziodemografische Merkmale – Altersgruppe in Zehnjahresschritten, Geschlecht, Bundesland oder Wohnort – der Mobilfunknutzer in ebenfalls anonymisierter Form mit den Signalisierungsdaten verbinden.

Bevor die Daten analysiert werden, löscht das Anonymisierungsverfahren personenbezogene Informationen, so dass keine individuellen Bewegungsprofile erstellt werden, sondern lediglich anonyme Bewegungsströme, die keinen Rückschluss auf eine einzelne Person zulassen. Darüber hinaus werden bei der Analyse ausschließlich Gruppen mit einer Mindestgröße von 30 Personen pro Erfassungszeitraum betrachtet. Die Prozessschritte zur Anonymisierung finden in einem Hochsicherheitsrechenzentrum der Deutschen Telekom statt, auf das Motionlogic selbst keinen Zugriff hat.

Die Analysen erlauben es, tagesaktuell anonyme Aussagen über Verkehrs- und Bewegungsströme zu treffen, zum Beispiel über die Fließgeschwindigkeit des Verkehrs, Quell-Ziel-Analysen von Verkehrsströmen und welche Verkehrsträger die anonymen Personengruppen nutzen. Die Lösungsplattform Motionlogic eröffnet so Möglichkeiten, um beispielsweise den öffentlichen Nahverkehr – etwa zu Stoßzeiten – besser takten zu können.

Hilfreich sind Verkehrsanalysen auch für Planer von Verkehrsinfrastrukturen. Das Wissen über Verkehrsflüsse hilft etwa im öffentlichen Nahverkehr, neue Strecken anhand der Nachfrage zu planen oder den Fahrzeugeinsatz nach dem tatsächlichen Bedarf auszurichten. Aus Verkehrsanalysen gewonnene zuverlässige Daten können zudem helfen, Staus zu vermindern und sogar zu vermeiden. Bisher haben Planer für Verkehrsanalysen unter anderem manuelle Zählungen, Sensordaten oder Befragungen eingesetzt. Doch der Aufwand, solche Daten zu erheben, ist hoch – und der Erkenntnisgewinn eher gering.

Ein weiteres Anwendungsfeld ist die Verbesserung der Planungsgrundlage bei der Suche nach neuen Standorten im Einzelhandel. Durch die Analyse der anonymen Verkehrsströme und deren Herkunft lässt sich die Suche nach Versorgungslücken schneller und effizienter gestalten.

TUE GUTES UND REDE DARÜBER

Die Deutsche Telekom hat ein sehr hohes Datenschutz- und Datensicherheitsniveau erreicht. Dies bestätigen auch unabhängige Prüfinstitutionen. Die organisatorischen und technischen Maßnahmen gehen teilweise über die vom Gesetzgeber vorgeschriebenen Vorgehensweisen hinaus. Bei den Verbrauchern schlägt sich das positiv nieder: Laut dem Sicherheitsreport, einer repräsentativen Befragung der Bevölkerung, vertrauen die Menschen der Telekom deutlich mehr als dem Wettbewerb.

Bisher mangelte es in puncto Datenschutz jedoch noch an der Außendarstellung. Das soll sich ändern: 2016 wird der Bereich Datenschutz stärker in die Öffentlichkeit gehen und sich selbstbewusster als bisher präsentieren. Los geht es mit einem neuen Datenschutzportal, in dem die Telekom in Zukunft sehr detailliert zeigen wird, wie Datenschutz konkret funktioniert. Weitere Kommunikationsmaßnahmen sind geplant. Ganz nach dem Motto: Tue Gutes und rede darüber.

SCHULUNG ZU DATEN- UND INFORMATIONSSCHUTZ

Im März 2015 startete die Schulung „Daten- und Informationsschutz“ für alle Beschäftigten der Deutschen Telekom. Die Onlineschulung informiert darüber, was gesetzlich erlaubt ist und was unbedingt beachtet werden muss. Sie wird alle zwei Jahre aktualisiert und ist für alle Mitarbeiter in Deutschland verpflichtend. Ein Schwerpunkt sind die Binding Corporate Rules Privacy – die wichtigste interne Datenschutzrichtlinie. Die Schulung umfasst darüber hinaus: nützliche Tipps zum richtigen Umgang mit sensiblen Informationen und Dokumenten. Die Schulung garantiert weltweit einheitliche Datenschutzstandards bei der Verarbeitung von Kunden- und Mitarbeiterdaten innerhalb des Telekom Konzerns.

SEI KEIN DATENSCHLONZ!

FÜR DEN DATENSCHUTZ BIRGT DER BÜROALLTAG VIELE FALLSTRICKE. IN EINEM IDEENWETTBEWERB RIEF DIE TELEKOM IHRE MITARBEITER AUF, DIE RISIKEN ANSCHAULICH DARZUSTELLEN. DIE BESTEN EINSENDUNGEN ERSCHEINEN JETZT ALS KURZE CARTOONS.

Sei kein Datenschlonz! Mit dieser Aufforderung startet jede Folge der neuen Cartoonserie. Sie erweckt damit eine filmische Kunstfigur zu neuem Leben, die die Telekom Anfang 2015 schuf, um das Bewusstsein für den Datenschutz zu schärfen. Der Film um den Datenschlonz, der gedankenlos vertrauliche Daten preisgibt, kam bei den Beschäftigten gut an. So gut, dass die Konzerndatenschützer einen darauf aufbauenden Ideenwettbewerb auslobten. Weltweit riefen sie ihre Kollegen dazu auf, über mögliche Datenschutzverstöße nachzudenken und diese dann anschaulich in Szene zu setzen. Rund 150 Mitarbeiter folgten dem Aufruf und nahmen die Risiken textlich, grafisch und zum Teil sogar filmisch aufs Korn.

Viele Einsendungen lenken das Bewusstsein auf Szenarien außerhalb des eigentlichen Arbeitsplatzes der Beschäftigten. So zum Beispiel auf einen Geschäftsreisenden, der auf seinem Notebook im Zug vertrauliche Informationen aufruft, ohne sich zu kümmern, wer sonst noch auf sein Display schauen kann und das auch tut. Ein Szenario zeigt Mitarbeiter, die sich nach Feierabend an der Bushaltestelle über die Arbeit unterhalten und dabei arglos über vertrauliche Informationen in Bezug auf andere Personen sprechen. Dinge, die jedenfalls für die Ohren der übrigen Fahrgäste nicht bestimmt sind. Nach und nach setzt die Telekom die eingereichten Szenen nun in Cartoons um und bindet diese in ihre weltweite Datenschutz-Awareness-Kampagne ein.

IM FOKUS VERANTWORTUNGSVOLLER INVESTOREN

FÜR DIE DEUTSCHE TELEKOM IST DAS INVESTMENT NACHHALTIG ORIENTIERTER INVESTOREN EIN BAUSTEIN ZUR LANGFRISTIGEN KAPITALSICHERUNG. AUCH DAS ENGAGEMENT DER TELEKOM FÜR DATENSCHUTZ UND DATENSICHERHEIT IST FÜR INVESTOREN EIN WICHTIGER BAUSTEIN IN BEZUG AUF NACHHALTIGES WIRTSCHAFTEN, ERKLÄRT BIRGIT KLESPER, LEITERIN DES BEREICHS GROUP TRANSFORMATIONAL CHANGE AND CORPORATE RESPONSIBILITY.

Frau Klesper, Sie leiten unter anderem den Bereich „Group Corporate Responsibility“. Wo genau ist die Verbindung zum Thema „Datenschutz und Datensicherheit“?
Birgit Klesper: Die Deutsche Telekom bekennt sich zur verantwortungsvollen Unternehmensführung. Wir übernehmen unternehmerische, ökologische und soziale Verantwortung entlang der gesamten Wertschöpfungskette – das heißt sowohl in unseren internen Prozessen als auch gegenüber unseren Kunden, Lieferanten, der Gesellschaft und natürlich auch gegenüber unseren Investoren. Es ist Teil unseres Selbstverständnisses als verantwortungsvolles Unternehmen, unseren Kunden ein hohes Maß an Sicherheit zu gewähren und die Daten sowie Infrastrukturen unserer Nutzer konsequent vor unerlaubtem Zugriff zu schützen. Wie die IKT-Branche mit diesem Thema umgeht, rückt vermehrt in das Blickfeld von Investoren.

Welche Investoren interessieren sich besonders für das Thema „Datenschutz und Datensicherheit“ und warum?
Birgit Klesper: Viele unserer Investoren – insbesondere die nachhaltig orientierten – setzen auf die langfristige Entwicklung und Rendite eines Unternehmens. Wir sprechen auch vom Fachbegriff „SRI“: Socially Responsible Investment. SRI-Anlageprodukte bestehen in der Regel aus Wertpapieren von Unternehmen, die nicht nur eine gute finanzielle Performance erzielen, sondern auch einer Überprüfung nach unternehmerischen, ökologischen und sozialen Kriterien standhalten. SRI-Investoren ist es wichtig, Risiken auszuschließen und Marktchancen zu erkennen, um dann langfristig zu investieren. Diese Kriterien treffen auch auf die Themen „Datenschutz und Datensicherheit“ zu.

Hat die Deutsche Telekom ein besonderes Interesse an diesen nachhaltigen Investoren?
Birgit Klesper: Ja! Für die Deutsche Telekom ist das Investment nachhaltig orientierter Investoren ein Baustein zur langfristigen Kapitalsicherung, da diese Investoren eben „nachhaltige“ – sprich langfristige – Anlageentscheidungen treffen. Derzeit werden 21 Prozent unserer Aktien von Investoren gehalten, die zumindest teilweise ihre Aktien gemäß nachhaltigen Kriterien managen, und 2 Prozent von Investoren, die sogar vorrangig ihre Aktien entsprechend nachhaltigen Kriterien managen. Und der Markt für nachhaltige Investments wächst stetig. In Deutschland haben sich nachhaltige Investments und Mandate seit 2010 mehr als verdoppelt – auf zuletzt fast 53 Milliarden Euro im Jahr 2014 (FNG Marktbericht 2015). Darüber hinaus gibt es auch Studien, die einen Zusammenhang zwischen guten SRI-Ergebnissen und niedrigeren Kapitalkosten belegen.

Mit welchen Argumenten erläutern Sie den nachhaltig orientierten Investoren, dass die Telekom gut für das Thema „Datenschutz und Datensicherheit“ gerüstet ist?
Birgit Klesper: Durch unsere umfangreichen Maßnahmen im Bereich der Datensicherheit – beispielsweise unser Netzwerk aus „Honey Pots“ oder Cyber Security Center – reduzieren wir geschäftsschädigende Risiken wie zum Beispiel Cyberattacken. Investoren sind beeindruckt, wenn sie erfahren, dass die Deutsche Telekom 99 Prozent der Cyberattacken direkt abwehren und die restlichen Angriffe innerhalb kürzester Zeit bewältigen kann. Neben der Risikominderung nehmen wir gleichzeitig unternehmerische Chancen wahr: Wir gewinnen Kunden, die in puncto Datenschutz und Datensicherheit den Produkten und Diensten der Deutschen Telekom vertrauen. Durch die fortschreitende Digitalisierung und die dadurch anfallenden Datenmengen werden diese Aspekte noch weiter an Bedeutung für unsere Kunden und damit für unseren Geschäftserfolg gewinnen. Auch für Kinder und Jugendliche ist Datenschutz und Privatsphäre bereits ein Thema. Auf der Plattform unserer Initiative „Teachtoday“ können Lehrer, Eltern und auch Schüler praxis- und alltagsnahe Tipps und Materialien zum sicheren und verantwortungsvollen Umgang mit IKT finden.

Gute Argumente! Aber wie genau vermitteln Sie diese Informationen an die nachhaltig orientierten Investoren?
Birgit Klesper: Wir setzen hier auf verschiedene Wege. Von öffentlich verfügbarem Reporting bis zum persönlichen Dialog. Inhalte, die mit Blick auf den Kapitalmarkt extern kommuniziert werden, stimmen wir dabei eng mit dem Konzernbereich Investor Relations ab. Der Geschäftsbericht und der CR-Bericht sind die transparente Wissensbasis, aus der Investoren – wie andere relevante Stakeholder auch – bereits umfangreiche Informationen beziehen können. Beide Berichte erfüllen höchste Berichtsstandards und wurden 2015 mit dem ECON Award ausgezeichnet. Auch dieser Bericht zu Datenschutz und Datensicherheit ist eine wichtige Informationsquelle. Darüber hinaus nehmen wir regelmäßig an ausgewählten Nachhaltigkeitsratings teil. Solche Ratings berücksichtigen zumeist öffentlich verfügbare Informationen zum Beispiel aus dem CR-Bericht, fragen bei Bedarf weitere Details direkt bei den Unternehmen ab und verdichten dies dann zu Unternehmensprofilen. Die entsprechenden Profile enthalten eine genaue Bewertung jedes Themas – entweder in Prozent oder auch auf einer Skala von A bis D. Neben den Ratern, die sich auf Nachhaltigkeit spezialisieren, berücksichtigen darüber hinaus traditionelle Rater wie Bloomberg und Thomson Reuters zunehmend Kriterien der nachhaltigen Unternehmensführung. Die bewerteten Unternehmensprofile können Investoren bei den Rating-unternehmen einkaufen. Meist erwerben Investoren Unternehmensprofile verschiedener Ratinganbieter und kombinieren diese mit hausinternen Recherchen in den öffentlich verfügbaren Quellen. Das Thema „Datenschutz und Datensicherheit“ hat in Ratings seit Jahren ein hohes Gewicht. Die Deutsche Telekom schneidet hier regelmäßig hervorragend ab und liegt deutlich über dem Branchendurchschnitt. So erreichten wir zum Beispiel im Rating von RobecoSAM 2015 einen Score von 97 Prozent, bei oekom research erhält das Thema „Data protection and information security“ die Bestnote A+ und der Rater Sustainalytics lobt „very strong data privacy & security programmes“.

Sprechen Sie auch direkt mit den nachhaltig orientierten Investoren?
Birgit Klesper: Unser Reporting und die Teilnahme an Ratings sind nur die Basis. Ergänzt werden sie durch den direkten Dialog mit nachhaltig orientierten Investoren. Direkter Kontakt mit den Investoren läuft federführend über den Konzernbereich Investor Relations. Zusammen mit Simone Schlief von Investor Relations führen wir regelmäßig „SRI Calls“ und „SRI Roadshows“ durch. Dort werden im Gespräch mit Investoren deren konkrete Fragen beantwortet – zunehmend auch mit Mainstream-Investoren.

Eine „SRI Roadshow“ – das hört sich an wie eine Tournee. Wie können sich unsere Leser das vorstellen?
Birgit Klesper: Das ist auch fast wie eine Tournee! Das ist ein sehr intensives Engagement. Zusammen mit Investor Relations besuchen wir etwa zwei- bis dreimal im Jahr an aufeinanderfolgenden Tagen Investoren in verschiedenen europäischen Metropolen. Es gibt Einzelgespräche und „Luncheons“ – dabei sitzen die Investoren zu Tisch, während wir durch unsere Präsentation führen und auf knifflige Fragen der Investoren antworten. Gerade in den Dialogformaten erleben wir derzeit eine deutliche Zunahme des Interesses für die Themen Datenschutz und Datensicherheit.

Lohnt sich denn der ganze Aufwand?
Birgit Klesper: Ja. Eine „Roadshow“ bedeutet zeitlichen Aufwand und vor allem eine gute Vorbereitung. Vor Ort beantworten wir dann mit hoher Konzentration sehr durchdachte und präzise Fragen der Investoren. Nach dem 5. Gespräch wird ein solcher Tag dann schon recht anstrengend – aber es lohnt sich! So erfahren wir aus erster Hand, wo wir als Deutsche Telekom aus Sicht der Investoren schon erfolgreich unterwegs sind und welche Themen besonders im Augenmerk der verschiedenen finanziellen Stakeholder liegen. Das direkte Feedback der Investoren in einer Roadshow nutzen wir wiederum bei der strategischen Ausrichtung unseres CR-Engagements.

Woran merken Sie, dass Sie die Investoren überzeugen konnten?
Birgit Klesper: Unser Ziel ist natürlich, dass die Investoren die T-Aktie als attraktiv bewerten und entsprechend in ihrem Portfolio priorisieren. Anders als bei den Ratings merken wir im direkten Dialog schnell, ob wir die Erwartungen der Investoren erfüllen oder sogar übertreffen können. Es gibt in der Regel nach jeder Roadshow einen kurzen Abschlussbericht des Brokers, der unsere Roadshows organisiert und begleitet.Hinsichtlich unserer Datenschutz- und Datensicherheitsmaßnahmen wird aktuell besonders positiv bewertet, dass die Deutsche Telekom bereits 2008 einen Vorstandsbereich (DRC) auch für Datenschutz und Datensicherheit geschaffen hat. Hervorgehoben werden auch unsere starken und konzernweit implementierten Richtlinien (Policies) sowie die umfassenden regelmäßigen Maßnahmen, Trainings und Audits. Auch die hauseigene Ausbildung von IT-Experten, das führende Engagement der Deutschen Telekom in Branchen-initiativen sowie die Erschließung von Geschäftspotenzialen im Bereich Datenschutz und Datensicherheit finden deutliche Anerkennung.

Die hohe Wertschätzung der Investoren bezüglich des Themas „Datenschutz und Datensicherheit“ geben wir direkt an die Fachkollegen im Konzern weiter. Ich bin stolz, dass wir als Deutsche Telekom zu den Vorreitern in der IKT-Branche zählen.

Birgit Klesper

ist seit 2012 Senior Vice President Group Transformational Change & Corporate Responsibility bei der Deutschen Telekom AG. Vor ihrem Wechsel zur Telekom 2006 verantwortete die Journalistin die Unternehmenskommunikation der Wella AG und von Tchibo.

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

TEACHTODAY
MEDIENKOMPETENZ FÖRDERN

Immer online, immer erreichbar: Für Kinder und Jugendliche gehören Smartphone, Internet und Social Media zum Leben. Laut der der JIM-Studie 2015 – Jugend, Information, (Multi-)Media – des Medienpädagogischen Forschungsverbundes Südwest besitzen heute 92 Prozent der 12- bis 19-Jährige ein Handy und drei Viertel gehen mit einer Flatrate online. Einen eigenen Computer oder Laptop haben rund drei Viertel, über die Hälfte einen eigenen Fernseher (57 %).

Bei den noch jüngeren Kindern sind mehr als die Hälfte der 8-Jährigen (55 %) bereits online, von den 6-Jährigen geht fast ein Drittel ins Internet, und bei den 3-Jährigen ist es schon jedes zehnte Kind, so Ergebnisse der Studie „Kinder in der digitalen Welt“ des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Zwar sehen sich Eltern in der Hauptverantwortung, wenn es darum geht, ihren Kindern einen kompetenten Umgang mit dem Internet zu vermitteln. Doch auch Schulen und Unternehmen müssen ihren Beitrag dazu leisten, Kinder und Jugendliche an die altersgerechte Nutzung der digitalen Medien heranzuführen.

Teachtoday ist eine Initiative der Telekom zur Förderung der sicheren und kompetenten Mediennutzung. Sie unterstützt Kinder und Jugendliche, Eltern und Großeltern sowie pädagogische Fachkräfte online und direkt vor Ort. Auf www.teachtoday.de bietet die Initiative Erwachsenen Tipps sowie eine Vielzahl von Materialien zum verantwortungsvollen Umgang mit neuen Informations- und Kommunikationstechnologien.

Das erste Handy, die Diskussion um angemessene Nutzungszeiten oder der respektvolle Umgang im Internet: Die Angebote von Teachtoday setzen bei konkreten Alltagssituationen an und berücksichtigen die verschiedenen Lebensräume sowie Nutzungsweisen von Kindern und Jugendlichen in Familie, Schule und Freizeit. Eltern, Großeltern und Pädagogen können sie sofort gemeinsam mit Kindern und Jugendlichen umsetzen.

Kindern und Jugendlichen bietet die Initiative auf www.scroller.de ihren eigenen Bereich. Mit „Scroller – dem Medienmagazin für Kinder“ entdecken sie spielerisch, wie sie sich sicher durch die Welt der digitalen Medien bewegen können. Dazu gibt es spannende und lustige Tipps, Rätsel und Geschichten.

WETTBEWERB „MEDIEN, ABER SICHER!“

Überall engagieren sich pädagogische Fachkräfte dafür, digitale Medien gewinnbringend in das Lehren und Lernen einzubinden. Sie entwickeln Medienkompetenzprojekte und erklären den Kindern, wie sichere Mediennutzung aussieht. Vielen innovativen, beispielhaften Projekten fehlt jedoch eine überregionale Sichtbarkeit. Hier kommt der internationale Wettbewerb „Medien, aber sicher!“ ins Spiel. Der Wettbewerb bietet pädagogischen Fachkräften, die erfolgreich Projekte mit digitalen Medien umgesetzt haben, nicht nur Preise, sondern auch eine Plattform, um ihre Projekte und Konzepte vorzustellen und sich auszutauschen.

Aus den eingereichten Beiträgen hat eine Jury sieben Schulen und Einrichtungen ausgewählt und auf dem Summit for Kids in Bonn prämiert. Beim Wettbewerb 2015 wurden Projekte in zwei Kategorien gesucht:

1. Sichere Mediennutzung: Hierzu zählen Projekte und Konzepte, die den sicheren Umgang mit Medien in den Fokus rücken, egal, ob in der Schule, zu Hause oder in der Freizeit.
2. Lernen mit digitalen Medien: Hier waren Konzepte gefragt, die digitale Medien zur Erreichung von Lernzielen und Vermittlung von Lerninhalten gewinnbringend einsetzen.

SUMMIT FOR KIDS

Am 18. November 2015 fand in Bonn der Teachtoday „Summit for Kids“ mit über 150 Kindern statt. Der Aktionstag sensibilisierte Kinder und Jugendliche dafür, verantwortungsvoll mit digitalen Medien umzugehen. Als Ergebnis der Arbeit in den Workshops entstand ein Manifest mit den Wünschen der Kinder und Jugendlichen zur Nutzung digitaler Medien. In vier Gruppen beschäftigten sich die Kinder jeweils mit der Mediennutzung in einer der vier Lebenswelten Familie, Schule, Freizeit und der weiten Welt. Sie diskutierten angeregt über Thesen zur Mediennutzung in der jeweiligen Lebenswelt.

PARCOURS „MEDIEN, ABER SICHER!“

Die Deutsche Telekom macht Kinder fit im Umgang mit digitalen Medien. 2015 besuchte der Mediensicherheitsparcours Schulen in ganz Deutschland. Über 4.900 Kinder zwischen neun und zwölf Jahren lernten, mit dem Parcours Medien nicht nur intuitiv zu nutzen, sondern sich kompetent im Internet zu bewegen.

An fünf verschiedenen Stationen werden in aktionsreichen Übungen und Aufgaben unterschiedliche Bereiche der Mediennutzung aufgegriffen und Themen wie Spielzeiten, Datenschutz und Cybermobbing behandelt. Die Kinder benötigen, ähnlich wie bei einem „Jump and Run“-Computerspiel, Reaktionsschnelligkeit und Geschicklichkeit. Im Vordergrund stehen Themen wie Spielzeiten, Datenschutz und Cybermobbing.

Pädagogen können in vielfältigen (Lern-)Szenarien und Settings in Kinder- und Freizeiteinrichtungen oder Schulen ihren Einrichtungen den Parcours selbst umsetzen. Auf www.teachtoday.de finden sie hierfür Erklärfilme und alle benötigten Materialien. Der Parcours lässt sich als Stationenbetrieb mit allen fünf Bereichen durchführen oder es können einzelne Stationen in eigene Aktionen eingebunden werden.

DATENHACK BEI IT-DIENSTLEISTER VON T-MOBILE USA

IM SEPTEMBER 2015 HAT DER IT-DIENSTLEISTER EXPERIAN EINEN UNAUTORISIERTEN ZUGRIFF AUF SEINE SERVER ENTDECKT. DAVON BETROFFEN WAREN AUCH DATEN, DIE EXPERIAN FÜR T-MOBILE USA SPEICHERT UND VERARBEITET. SYSTEME DER T-MOBILE USA WURDEN NICHT KOMPROMITTIERT.

Nach Untersuchungen von Experian handelte es sich um einen isolierten Hackerangriff über einen Zeitraum von rund zwei Wochen vom 1. bis 16. September 2015. Dabei gab es keinen Zugriff auf Kreditkarten- oder Bankdaten. Die Server enthielten auch persönliche Daten einiger Kunden von T-Mobile USA sowie Daten von Kunden, welche die Finanzierung von Endgeräten in Anspruch genommen haben, was mit einem Kreditcheck verbunden ist. Daten deutscher Kunden waren von dem Vorfall nicht betroffen.

Die vom Hacking betroffenen Informationen enthielten Daten wie Name, Adresse, Sozialversicherungsnummer, Geburtsdatum sowie Ausweisnummern wie zum Beispiel aus Führerscheinen oder Reisepässen sowie zusätzliche Informationen, die T-Mobile im Rahmen einer Bonitätsprüfung speichert. Es gab laut Experian keinen Hinweis darauf, dass Daten von T-Mobile USA zweckwidrig verwendet wurden. Es bleibt aber festzustellen, dass sich für die betroffenen Kunden das Risiko eines Identitätsdiebstahls erhöht hat.

In einem kurz nach Entdeckung des Vorfalls veröffentlichten Statement hat sich John Legere, CEO von T-Mobile USA, zu dem Vorfall geäußert. „Ich bin unglaublich verärgert über diese Datenpanne und wir werden die weitere Zusammenarbeit mit Experian genau überprüfen. Im ersten Schritt richte ich aber mein Hauptaugenmerk darauf, alle Kunden zu unterstützen, die irgendwie von diesem Vorfall betroffen sein könnten. Ich nehme unsere Kunden und den Schutz ihrer Daten sehr ernst. Dies ist für uns also kein kleiner Vorfall. Ich versichere unseren Kunden, dass weder IT-Systeme noch Netzwerke von T-Mobile von diesem Angriff betroffen sind und dass keine Kreditkartennummer oder Informationen zu Bankverbindungen von dem Ereignis bei Experian betroffen sind.“

Experian hat internationale Strafverfolgungsbehörden über den Zwischenfall informiert und kurzfristig zusätzliche Sicherheitsmaßnahmen eingeleitet, um solche Vorfälle zukünftig zu verhindern. Weiterhin versucht Experian die Hacker zu identifizieren und arbeitet dafür eng mit internationalen Strafverfolgungsbehörden zusammen.

SYNTHETISCHE DATEN FÜR DIE ANALYSE

WELCHE DATEN DÜRFEN UNTERNEHMEN WIE AUSWERTEN? UM DIESE FRAGE DREHT SICH IM DATENSCHUTZ FAST ALLES. EINE LÖSUNG KÖNNTEN SYNTHETISCHE DATEN SEIN, DIE ABSOLUT NICHTS ÜBER REAL EXISTIERENDE PERSONEN VERRATEN.

Was nützen unzählige Informationen – zum Beispiel auch Kundendaten –, wenn wir sie nicht verwenden dürfen? Eine Frage, die sich Unternehmen in den USA nicht unbedingt stellen müssen, da dort der Umgang mit personenbezogenen Daten anders gesehen wird. In Deutschland dagegen verbietet das Datenschutzrecht eine Reihe von Analysen, die durchaus gewinnbringend sein könnten. Unternehmen entscheiden sich daher meist für die Verwendung von anonymisierten Daten. Die Produktion von anonymisierten Daten ist jedoch technisch aufwendig. Daher gibt es, abhängig vom eingesetzten Verfahren und von der eingesetzten Technik, teilweise Abweichungen in der Qualität, also dem Grad der Verfremdung des Datums von einer realen Person. Endnutzer und Medien stehen daher solchen Anonymisierungsverfahren, selbst wenn eine entsprechende Zertifizierung vorliegen sollte, nicht uneingeschränkt positiv gegenüber, da Fälle denkbar sind, in denen Spezialisten mit viel Aufwand und Zusatzwissen möglicherweise wieder bei einzelnen Daten den Bezug zu einer bestimmten Person herstellen könnten.

Forscher der T-Labs in Berlin, des zentralen Forschungs- und Innovationsbereichs (F&I) der Telekom, entwickeln stattdessen Analysemethoden, die der Datenschutz erlaubt und keinerlei Rückschluss auf Einzelpersonen zulassen. Die Antwort sind synthetische Daten. Sie basieren zwar auf realen personenbezogenen Daten, über welche die Forscher einen selbst entwickelten mathematischen Algorithmus laufen lassen. Dieses Verfahren abstrahiert persönliche Daten und überführt sie in synthetische Daten.

So erkennt der Algorithmus selbst in großen Datenmengen spezifische Muster und clustert sie in Gruppen: männlich, 30 – 39 Jahre, aus Charlottenburg, fährt morgens um 8 Uhr zur Arbeit. Die so gewonnenen Muster sind vergleichbar mit Schablonen, aus denen die Forscher im nächsten Schritt synthetische Daten erzeugen, die eine ähnliche Qualität wie echte Daten aufweisen. Der wesentliche Unterschied: Sie lassen keinerlei Rückschlüsse auf eine einzelne Person zu.

Noch befindet sich die Herstellung synthetischer Daten in der Forschungsphase, aber es könnten konkrete Produkte aus dem Verfahren entstehen. Das würde es jedem Unternehmen, das neue Erkenntnisse aus sensiblen personalisierten Daten ziehen möchte, erlauben, die Herstellung von synthetischen Daten als Service zu nutzen.

DATENSCHUTZ FÜR VERNETZTE PRODUKTION

DIE DEUTSCHE TELEKOM HAT DATENSCHUTZLEITSÄTZE ZU „INTERNET OF THINGS“ UND „INDUSTRIE 4.0“ FORMULIERT. SIE BESCHREIBEN DIE PRÄMISSEN FÜR DIE GESTALTUNG VON INTERNET OF THINGS-LÖSUNGEN WIE BEISPIELSWEISE IN DEN BEREICHEN CONNECTED CAR ODER SMART HOME.

1. Die Deutsche Telekom bringt die erfolgreiche Entwicklung von neuen Geschäftsmodellen in den Bereichen „Internet of Things“ und „Industrie 4.0“ voran. Dabei geht es auch um die Etablierung eines einheitlich hohen Datenschutzniveaus bei der Vernetzung einer Vielzahl von Geräten und Produktionsprozessen sowie den dahinterstehenden Menschen. Bei allem gilt: Für die Telekom steht das Vertrauen der Menschen in den Schutz ihrer Daten im Vordergrund. Wir entwickeln datenschutzfreundliche Lösungen im Sinne unserer Kunden.

2. Bei „Internet of Things“- und „Industrie 4.0“-Geschäftsmodellen sind oft mehrere Unternehmen in die Datenverarbeitungsprozesse eingebunden. Die Verantwortlichkeiten der mit der Datenverarbeitung befassten Unternehmen müssen dabei über die gesamten Prozessketten transparent und verständlich dargestellt werden. Dafür steht die Deutsche Telekom.

3. Die Deutsche Telekom verarbeitet die ihr anvertrauten personenbezogenen Daten zur Erfüllung ihrer vertraglichen Vereinbarungen mit den Kunden oder zur Erfüllung ihrer Verpflichtungen als Auftragsdatenverarbeiter.

4. Darüber hinaus verwenden wir Daten grundsätzlich anonymisiert oder, wenn ein mittelbarer Personenbezug erhalten bleiben muss, pseudonymisiert. Pseudonymisierung wird beispielsweise durch eine hochwertige Verschlüsselung erreicht und den Kunden transparent gemacht. Soll der Bezug zur Person wiederhergestellt werden, muss dafür die Einwilligung des Betreffenden eingeholt werden. Das verstehen wir unter der Kultur des Einverständnisses.

5. Die Deutsche Telekom wird Daten grundsätzlich nur in der Form weitergeben, dass Dritte selbst keinen Rückschluss auf Personen herstellen können. Daten mit direktem Personenbezug gibt die Telekom nur mit Einwilligung der Kunden weiter oder wenn sie gesetzlich dazu ermächtigt ist.

WILLKOMMEN IN DER ZETTABYTE-ÄRA

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

DIE DIGITALISIERUNG BIETET ENORME CHANCEN FÜR WIRTSCHAFT UND GESELLSCHAFT – BIRGT ABER AUCH RISIKEN. FÜR MEHR SICHERHEIT BRAUCHEN WIR STANDARDS UND KLARE REGELN, DIE ALLERDINGS INNOVATIONEN NICHT SCHON IM KEIM ERSTICKEN.

Wer vor fünf Jahren bei Google nach dem Begriff „Industrie 4.0“ suchte, ist komplett leer ausgegangen. Heute ist dieses Schlagwort der Digitalisierung in aller Munde. Dahinter steckt die Vernetzung von Maschinen, Objekten und Menschen, die mehr Effizienz in der Produktion und eine größere Kundennähe verspricht. In der „Smart Factory“ sind Produktionsanlagen nicht mehr zentral gesteuert; sie steuern sich selbst. Vernetzte Werkstücke und Maschinen tauschen Informationen über IT-Schnittstellen und das Internet aus. Bauteile sind dazu etwa mit RFID-Chips ausgestattet und sagen der Fertigungsmaschine schon auf dem Fließband, wohin sie transportiert und wie sie weiterverarbeitet werden wollen. Individuelle Kundenwünsche lassen sich direkt berücksichtigen.

Von der Produktion über die Lagerung bis zum Transport gehören intelligente Vernetzungsprozesse in deutschen Unternehmen bereits zum Alltag. Sie sparen Zeit und Ressourcen – also bares Geld. Allerdings reden wir hier von Insellösungen für bestimmte Betriebe und Industriezweige. Bei übergreifenden Vernetzungskonzepten hingegen, etwa dem autonomen Fahren, geht es um den Transport und die Verarbeitung wesentlich größerer Datenmengen. Dazu braucht es eine Infrastruktur aus schnellen Netzen, hochverfügbaren Cloud-Plattformen und sicheren Datenanalysetools. Die Telekom bietet genau das aus einer Hand und ist deshalb ein wichtiger Digitalisierungspartner für Wirtschaft und Gesellschaft geworden.

SO VIELE DATEN WIE SANDKÖRNER AUF DER WELT

Mehr als ein Zettabyte Daten – eine Eins mit 21 Nullen – sollen 2016 laut Expertenschätzung durchs Netz fließen. Die Zahl entspricht etwa der Menge aller Sandkörner an allen Stränden der Welt. Die Marktforscher von IDC schätzen, dass in den nächsten fünf Jahren weltweit etwa 30 Milliarden Dinge – vom Traktor bis zum Blumentopf – ihre Daten in Echtzeit über das Netz in die Cloud senden, wo sie unmittelbar analysiert und weiterverarbeitet werden. Je größer dabei die Datenbasis, desto genauer und fehlerfreier die Analysen.

Von der intelligenten Auswertung großer Datenmengen profitiert künftig nicht nur die Industrie, sondern jeder Einzelne. Ohne großes Zutun. Schon heute ist es möglich – übrigens auch aus Datenschutzsicht unbedenklich – anonymisierte Mobilfunkschwarmdaten zu nutzen, um beispielsweise die Einsatzpläne von regionalen Bussen und Bahnen zu optimieren. Vor allem bei Großevents oder spontanen Veranstaltungen wäre das für Verkehrsbetriebe und deren Kunden eine Hilfe. Auch Rettungskräfte könnten Schwarmdaten nutzen, um bei größeren Unfällen die Anzahl möglicher Verletzter besser bestimmen und ebenjene schneller versorgen zu können.

Vielversprechend für die gesamte Bevölkerung ist auch die Auswertung von Medizindaten. Wenn Wissenschaftler die unterschiedlichen Erkenntnisse über Krankheiten, die oft isoliert in Klinikakten lagern, anonymisiert digital auswerten dürften, würde das die Erforschung und Bekämpfung vieler Krankheiten enorm erleichtern. Die Realität sieht allerdings anders aus: Zehntausende Patientenakten aus Papier stapeln sich zurzeit in den Kellern insolvent gegangener, leer stehender Kliniken. Übrigens nicht anonymisiert und nicht ausreichend vor Diebstahl gesichert.

DIGITALISIERUNG DARF KEINE ANGST MACHEN

Es steht außer Frage, dass die Digitalisierung enorme Chancen für Wirtschaft und Gesellschaft bietet. Doch sie birgt auch Gefahren wie Cyberkriminalität. Innovation und Sicherheit müssen daher Hand in Hand gehen. Dafür brauchen wir Standards und klare Regeln, die wiederum Innovationen nicht schon im Keim ersticken. Das gilt vor allem für die Datenverarbeitung.

Wer darf welche Daten wie lange und wofür genau nutzen? Welche Sicherheitsstandards soll es für das Internet der Dinge geben? Auf diese Fragen brauchen wir konkrete Antworten – und wir müssen sie offen und transparent diskutieren. Die Digitalisierung darf für die Bevölkerung keine angstbesetzte Parallelwelt sein. Vielmehr müssen Industrie und IT-Unternehmen die Vorteile greifbar machen und dabei stets Datenschutz und Datensicherheit in den Vordergrund stellen. Ein erster Meilenstein ist mit der Einigung auf die Europäische Datenschutzgrundverordnung gelegt. Nun geht es darum, auf dieser Basis die Weichen für die digitale Welt von morgen zu stellen.

Anette Bronder

leitet seit dem 1. August 2015 als Mitglied der Geschäftsführung der T-Systems International GmbH die Digital Division. Die Wirtschafts- und Sozialwissenschaftlerin startete ihre berufliche Laufbahn in verschiedenen Führungspositionen bei Hewlett Packard. Zwischen September 2010 und Juli 2015 leitete sie zunächst den Bereich Technology Enterprise der Vodafone Deutschland GmbH und übernahm dann die Position des Director Group Enterprise Solutions.

VORSICHT VOR GEFÄLSCHTEN RECHNUNGEN

IMMER WIEDER VERSUCHEN KRIMINELLE, ÜBER GEFÄLSCHTE TELEKOM RECHNUNGEN SCHADCODE AUF RECHNERN ZU VERBREITEN. SEIT FEBRUAR 2015 VERSENDET DIE TELEKOM IHRE ONLINE-RECHNUNGEN MIT ZUSÄTZLICHEN SICHERHEITSMERKMALEN.

Neben der persönlichen Anrede und Buchungskontonummer finden Kunden jetzt zusätzlich Straße und Hausnummer in ihrer Rechnung Online. Die neuen Merkmale stehen sowohl im Betreff der Rechnungsmail als auch im ersten Satz des eigentlichen Mailtextes. Durch das fälschungssichere E-Mail-Siegel können Kunden authentische Online-Rechnungen der Telekom zweifelsfrei erkennen, wenn sie ihre Rechnung Online über den Browser – http://telekom.de/email – oder die mobilen E-Mail-Applikationen der Telekom abrufen.

Das E-Mail-Siegel hat die Form eines blauen @-Zeichens mit einem Haken darin und wird vor dem Absender der Nachricht angezeigt. Angezeigt wird das Siegel darüber hinaus bei GMX, WEB.DE, freenet und 1&1. In E-Mail-Programmen wie Outlook oder Thunderbird kann das E-Mail-Siegel aus technischen Gründen nicht angezeigt werden.

Außerdem wurde eine neue Signatur eingeführt, die nicht sichtbar ist, beim E-Mail-Versand aber von den Internetprovidern ausgelesen wird. Anhand der Signatur können die Provider erkennen, ob die E-Mail von einem vertrauenswürdigen Absender stammt oder ob es sich um gefälschte E-Mails mit Telekom Absender handelt.

Darüber hinaus verwendet die Telekom eine persönliche Anrede und gibt im Festnetzbereich das Buchungskonto und im Mobilfunkbereich das Kundenkonto an. Wer unsicher ist, kann eine korrekte Rechnung jederzeit über das Telekom Kundencenter abrufen. Fehlt die Rechnung dort oder weist sie einen anderen Rechnungsbetrag auf, handelt es sich um eine Fälschung. Ein Grund für eine nähere Prüfung ist auch, wenn ein Kunde der Telekom eine Einzugsermächtigung erteilt hat, aber zu einer Überweisung aufgefordert wird.

Generell sollten sich E-Mail-Empfänger Zeit nehmen, E-Mails mit Rechnungen oder Ähnlichem genau zu prüfen. Wer kein Telekom Kunde ist, sollte die E-Mail ungelesen löschen. Ist der Empfangstermin für die Rechnung ungewöhnlich oder werden unerwartet hohe Beträge genannt, sollten Empfänger die Mail genauer prüfen, ohne Anhänge zu öffnen.

Auch die absendende E-Mail-Adresse bietet Hinweise auf Fälschungen: Im Festnetzbereich lautet die Adresse rechnungonline@telekom.de. Dieser Absender wird als „Telekom Deutschland GmbH {NoReply}“ angezeigt. Die E-Mail-Adresse ist beim Fahren mit der Maus über den Absendernamen bei manchen E-Mail-Programmen komplett sichtbar. Im Mobilfunkbereich lautet die Absenderadresse Kundenservice.Rechnungonline@telekom.de. Geschäftskunden erhalten ihre Rechnung über „servicecenter.gk@telekom.de“. Diese Adressen werden vollständig angezeigt.

MEHR PRÄSENZ AM INTERNETKNOTEN DE-CIX

DIE TELEKOM HAT DIE NUTZUNG DES NETZKNOTENS DE-CIX IN FRANKFURT AM MAIN MASSIV AUSGEBAUT UND KANN JETZT MEHR DATEN MIT ANDEREN PROVIDERN AUSTAUSCHEN.

Über den Knotenpunkt DE-CIX leiten Internetanbieter Datenströme untereinander weiter. Um mehr Sicherheit für Internetnutzer zu gewährleisten, sollten Daten auf möglichst kurzen Strecken vom Sender zum Empfänger gelangen – also ohne Umwege durch andere Rechtsräume. Dies soll sicherstellen, dass innereuropäischer Datenverkehr nicht über außereuropäische Hoheitsgebiete geleitet wird. Eine Selbstverpflichtung möglichst aller Netzbetreiber in Europa würde den unberechtigten Zugriff auf die transportierten Daten von außerhalb des europäischen Rechtsraums deutlich erschweren.

Das Internet der kurzen Wege ist Teil des Zehn-Punkte-Programms für mehr Sicherheit im Netz der Telekom und im Netz der Telekom bereits realisiert. Andere Internetanbieter hatten eine verstärkte Nutzung des DE-CIX-Netzknotens als Voraussetzung für die Realisierung des Internets der kurzen Wege definiert.

VERSCHLÜSSELTE E-MAILS FÜR ALLE

DIE TELEKOM UND DAS FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE SIT BIETEN AB MITTE 2016 MIT DER „VOLKSVERSCHLÜSSELUNG“ EINE EINFACHE MÖGLICHKEIT ZUR VERSCHLÜSSELUNG VON E-MAILS.

„Security by Design“ und „Usability by Design“: zwei Prinzipien, die bisher der breiten Nutzung von verschlüsselten E-Mails entgegenstanden. Nun haben die Telekom und das Fraunhofer-Institut für Sichere Informationstechnologie SIT ein Werkzeug entwickelt, damit die Ende-zu-Ende-Verschlüsselung von E-Mails nicht nur Experten vorbehalten bleibt. Die Volksverschlüsselung ist kostenlos, unkompliziert und transparent – und die Telekom betreibt die Lösung in einem Hochsicherheitsrechenzentrum. Die Volksverschlüsselung soll kryptografische Methoden aus der Forschung für alle zugänglich machen.

Die Volksverschlüsselung ist eine Software, die sowohl die notwendigen Verschlüsselungsinformationen generiert als auch die E-Mail-Programme der Benutzer entsprechend vorkonfiguriert. Für die eigentliche Verschlüsselung brauchen die meisten Nutzer kein neues Programm, denn die meisten E-Mail-Programme verschlüsseln, wenn entsprechende Schlüssel vorhanden sind. Somit können selbst unerfahrene Nutzer verschlüsselte E-Mails verschicken.

Im ersten Schritt steht die Volksverschlüsselung Windows-Nutzern für E-Mail-Programme wie Outlook oder Thunderbird zur Verfügung. In weiteren Schritten sind Versionen für Mac OS X, Linux, iOS und Android geplant. Die Software unterstützt zunächst den S/MIME-Standard, in einem nächsten Schritt wird sie zusätzlich OpenPGP unterstützen. Fraunhofer wird den Quellcode nach Veröffentlichung der Software allgemein zur Verfügung stellen. So können sich Experten selbst davon überzeugen, dass die Volksverschlüsselung keine Hintertüren hat.

Die Volksverschlüsselung erzeugt kryptografische Schlüssel direkt auf dem Endgerät des Nutzers. Diese privaten Schlüssel verbleiben ausschließlich in der Hand des Nutzers und befinden sich zu keiner Zeit in den Händen des Betreibers der Infrastruktur. Zur Nutzung der Verschlüsselung genügen die Installation der Software und eine einfache sichere Identifikation. Im ersten Schritt erfolgt die Authentifizierung über die etablierten Anmeldeverfahren der Telekom oder mithilfe des elektronischen Personalausweises. Später sind weitere Verfahren zur sicheren Identifikation geplant.

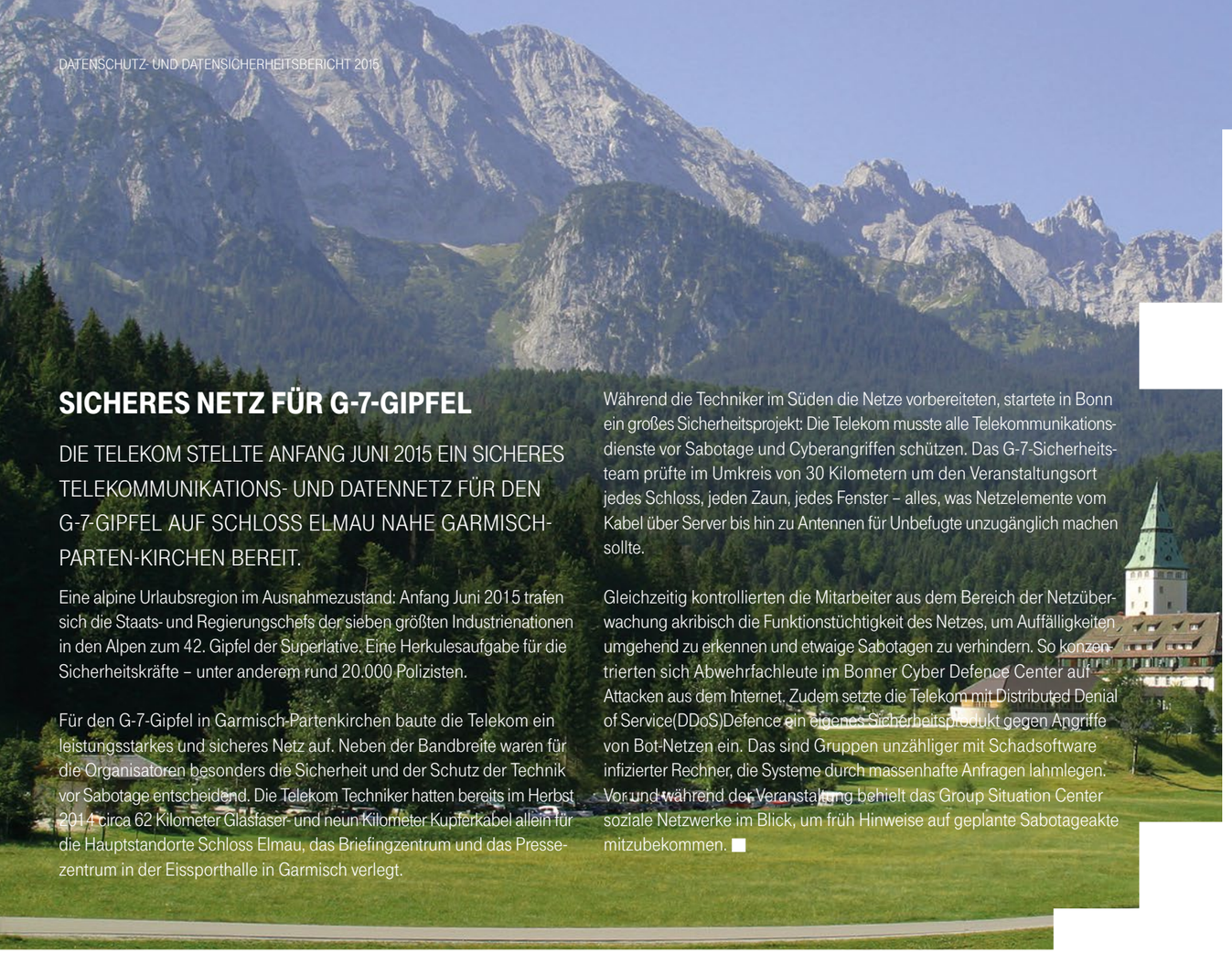
Weitere Informationen zum Thema Volksverschlüsselung und Verschlüsselung allgemein gibt es unter www.telekom.com/verschluesselung oder www.volksverschluesselung.de

SCHUTZ VOR ANDROID-SCHWACHSTELLE

IM SOMMER 2015 HAT EINE SICHERHEITSSCHWACHSTELLE WELTWEIT ANDROID-GERÄTE – UNABHÄNGIG VOM NETZBETREIBER – BEDROHT. SO LIESSEN SICH ÜBER PRÄPARIERTE MMS-NACHRICHTEN ANDROID-SMARTPHONES HEIMLICH KAPERN.

Die Lücke betraf einen Systemteil – Stagefright –, der für das Abspielen von Medien gebraucht wird. Der kriminelle Zugriff konnte über Mediendateien erfolgen, egal, ob diese über MMS, WhatsApp, Hangouts, Facebook, Browsing, Downloads etc. empfangen wurden. Die Schadsoftware konnte so auch Zugriff auf das Adressbuch erlangen und sich darüber weiterverbreiten. Im Fall von MMS-Nachrichten war die Schwachstelle besonders gefährlich: Empfing ein Smartphone eine MMS, lud es sie automatisch vom Server – ohne Zutun des Nutzers. Das bedeutet, dass der Nutzer keine Möglichkeit hatte, nur Botschaften von vertrauenswürdigen Kontakten zu öffnen.

Zum Schutz ihrer Kunden hatte die Telekom daher vorübergehend vom automatischen auf manuellen Download von MMS umgestellt, sodass die Nachrichten nicht mehr automatisch ohne Zutun des Nutzers auf das mobile Endgerät heruntergeladen wurden. Gleichzeitig hat die Telekom neue, netzseitige Schutzmaßnahmen gegen die Stagefright-Lücke ergriffen. Nutzen Dateien Stagefright-Lücke aus, werden sie als solche identifiziert und zum Schutz der Kunden nicht an den Empfänger zugestellt. Nicht betroffene Dateiinhalte werden wie gewohnt versandt. Damit ist es möglich, MMS-Nachrichten mit einer Audio- oder Videodatei auch wieder direkt auf Android-Geräten zu empfangen. Bisher war dies nur für Nutzer von Apple-Endgeräten möglich, da sie von der Schwachstelle nicht betroffen sind.



SICHERES NETZ FÜR G-7-GIPFEL

DIE TELEKOM STELLTE ANFANG JUNI 2015 EIN SICHERES TELEKOMMUNIKATIONS- UND DATENNETZ FÜR DEN G-7-GIPFEL AUF SCHLOSS ELMAU NAHE GARMISCH-PARTEN-KIRCHEN BEREIT.

Eine alpine Urlaubsregion im Ausnahmezustand: Anfang Juni 2015 trafen sich die Staats- und Regierungschefs der sieben größten Industrienationen in den Alpen zum 42. Gipfel der Superlative. Eine Herkulesaufgabe für die Sicherheitskräfte – unter anderem rund 20.000 Polizisten.

Für den G-7-Gipfel in Garmisch-Partenkirchen baute die Telekom ein leistungsstarkes und sicheres Netz auf. Neben der Bandbreite waren für die Organisatoren besonders die Sicherheit und der Schutz der Technik vor Sabotage entscheidend. Die Telekom Techniker hatten bereits im Herbst 2014 circa 62 Kilometer Glasfaser- und neun Kilometer Kupferkabel allein für die Hauptstandorte Schloss Elmau, das Briefingzentrum und das Pressezentrum in der Eissporthalle in Garmisch verlegt.

Während die Techniker im Süden die Netze vorbereiteten, startete in Bonn ein großes Sicherheitsprojekt: Die Telekom musste alle Telekommunikationsdienste vor Sabotage und Cyberangriffen schützen. Das G-7-Sicherheitsteam prüfte im Umkreis von 30 Kilometern um den Veranstaltungsort jedes Schloss, jeden Zaun, jedes Fenster – alles, was Netzelemente vom Kabel über Server bis hin zu Antennen für Unbefugte unzugänglich machen sollte.

Gleichzeitig kontrollierten die Mitarbeiter aus dem Bereich der Netzüberwachung akribisch die Funktionstüchtigkeit des Netzes, um Auffälligkeiten umgehend zu erkennen und etwaige Sabotagen zu verhindern. So konzentrierten sich Abwehrfachleute im Bonner Cyber Defence Center auf Attacken aus dem Internet. Zudem setzte die Telekom mit Distributed Denial of Service(DDoS)Defence ein eigenes Sicherheitsprodukt gegen Angriffe von Bot-Netzen ein. Das sind Gruppen unzähliger mit Schadsoftware infizierter Rechner, die Systeme durch massenhafte Anfragen lahmlegen. Vor und während der Veranstaltung behielt das Group Situation Center soziale Netzwerke im Blick, um früh Hinweise auf geplante Sabotageakte mitzubekommen. ■

DEUTSCHLAND SICHER IM NETZ

DIE TELEKOM HAT IHR ENGAGEMENT IM VEREIN „DEUTSCHLAND SICHER IM NETZ“ (DSIN) VERSTÄRKT. DIE MITGLIEDERVERSAMMLUNG HAT THOMAS KREMER, VORSTAND DATENSCHUTZ, RECHT UND COMPLIANCE BEI DER TELEKOM, ZUM VORSITZENDEN GEWÄHLT.

„Als zentrale Plattform für Verbraucher und Unternehmen stellt DsiN Aufklärungsangebote und Handlungsempfehlungen für einen sicheren Umgang mit der digitalen Welt bereit“, erklärte der neue DsiN-Vorsitzende Kremer. In Zukunft werde DsiN sich noch stärker für aktuelle Themenfelder wie Smart Home, vernetztes Fahren und digitale Bildung öffnen. „Neue Mitglieder, die Schutz und Vertrauen als zentralen Bestandteil der Digitalisierung betrachten, laden wir herzlich ein, bei DsiN mitzumachen.“

DsiN wurde im Rahmen des ersten Nationalen IT-Gipfels vor neun Jahren ins Leben gerufen und steht unter der Schirmherrschaft des Innenministeriums. Der Verein ist Ansprechpartner für Verbraucher und Unternehmen und bietet konkrete Hilfestellungen für mehr Sicherheitsbewusstsein im Netz. In Zusammenarbeit mit seinen Mitgliedern und Partnern entwickelt der Verein neue Strategien und Maßnahmen zum sicheren Umgang mit der digitalen Welt. Die Telekom hat sich beispielsweise für das Sicherheitsbarometer eingesetzt, das über die aktuelle Gefahrenlage im Netz informiert.

Zum zehnjährigen Jubiläum 2016 hat der Verein die Perspektiven seiner Aufklärungsarbeit in der digitalen Welt in einer Publikation „Denn Sicherheit kommt von Verantwortung“ zusammengefasst. Sie beschreibt Handlungsfelder der digitalen Aufklärung von mobiler Sicherheit und E-Government bis zur vernetzten Gesundheitsversorgung. ■

DER TELEKOM SICHERHEITSRATGEBER IM NETZ

CYBERKRIMINELLE, SCHADSOFTWARE UND PHISHING-BETRUG? VIREN UND WÜRMER, DAS ABGREIFEN VON KONTODATEN ODER DER MISSBRAUCH VON PERSÖNLICHEN DATEN SIND RISIKEN, GEGEN DIE SICH JEDER NUTZER SCHÜTZEN SOLLTE.

Informationen dazu gibt es im Internet reichlich, doch sie sind auf Tausende Webseiten verteilt. Die Website www.sicherdigital.de bündelt die Infos und bietet den Besuchern einen explorativen Zugang zu sicherheitsrelevanten Themen, die der Lebenswirklichkeit der Zielgruppen entsprechen. Jugendliche, Erwachsene und Unternehmen finden nützliche Hinweise und konkrete Hilfe rund um die Themen Sicherheit und Datenschutz bei allen Berührungspunkten mit der digitalen Welt. Repräsentiert werden die Zielgruppen über die Jugendlichen Lena und Lukas, die Mutter Sandra mit ihrem Sohn Max, den Unternehmer Matthias und die Senioren Renate und Horst.

Die intuitive Benutzerführung lädt den Besucher ein, sich spielerisch mit diesen Szenarien und den damit verbundenen Sicherheitsrisiken auseinanderzusetzen. Worauf sollte ich achten? Wie kann ich mich effektiv vor Bedrohungen schützen? Zum Beispiel mit den richtigen Grundeinstellungen im Betriebssystem des Smartphones oder mit speziellen Benutzerkonten für Kinder und Jugendliche. Neben informativen Artikeln bietet der Leitfaden eine Reihe von Checklisten, in denen die wichtigsten Tipps zu einem Thema übersichtlich zusammengefasst sind. Der Nutzer kann seine Sicherheit mit interaktiven Fragebogen selbst überprüfen oder sich Filmbeiträge darüber ansehen, wie die unterschiedlichen Charaktere mit dem Thema Sicherheit umgehen.

Zudem bietet der Ratgeber einen zweiten, thematisch strukturierten Zugang zu allen Inhalten. Wer gezielt nach Informationen zu einem bestimmten Thema sucht, wird hier schnell fündig – ganz gleich, ob es um Basisschutz für PC und Laptop, E-Mail-Sicherheit oder Sicherheit beim Onlinebanking geht. Auch die für Smartphones optimierte Version bietet diesen Informationszugang, um wichtige Themen übersichtlich darzustellen.

Die Internetseite www.sicherdigital.de will die fragmentierte Informationslage zur Sicherheit im Internet konsolidieren. Der Nutzer soll hier alles Wesentliche erfahren, was er wissen muss, um sich und seine Daten in der digitalen Welt zu schützen. Als weitere Serviceleistung leiten viele Links aus den Detailbeiträgen zu weiterführenden Informationsangeboten im Netz. ■

SICHERHEIT RÄUMT PREISE AB

BEIM DEUTSCHEN SICHERHEITSTAG 2015 IN BERLIN HAT DIE TELEKOM GLEICH DREI ANERKENNUNGEN FÜR IHRE SICHERHEIT ERHALTEN. AUSGEZEICHNET WURDEN DIE FACEBOOK PRIVACY APP, DAS BEDROHUNGSMANAGEMENT UND DIE SICHERHEITSPARTNERSCHAFT GEGEN METALLDIEBSTAHL.

Die Jury der „Outstanding Security Performance Awards“ (OSPAs) hat entschieden: Die Telekom belegt in Deutschland in der Kategorie „Herausragender Errichter von Sicherheitstechnik“ mit ihrer Facebook Privacy App Platz eins. Die App zeigt ihrem Besitzer, wer seine persönlichen Inhalte sehen kann, wer nach ihm suchen kann und wer auf seiner Chronik posten darf. Er kann seine Privatsphäre-Einstellungen bei Facebook mit nur einem Klick anpassen und seine Privatsphäre besser schützen.

Als „Herausragender Sicherheitsberater“ wurde das Bedrohungsmanagement der Telekom ausgezeichnet. Das Unternehmen sorgt mit dem Bedrohungsmanagement dafür, dass alle Beschäftigten angst- und gewaltfrei arbeiten können. Jeder kann die Kollegen vom Bedrohungsmanagement einschalten bei plötzlichen physischen Annäherungen oder wenn sich jemand verfolgt fühlt, bei Androhung von physischer und psychischer Gewalt oder ungewöhnlichen Beobachtungen, etwa wenn andere Gewaltfantasien äußern. Zertifizierte Bedrohungsmanager haben in mehr als zwei Jahren etwa 200 Kolleginnen und Kollegen geholfen.

Weiterhin würdigte die Jury die SIPAM (Sicherheitspartnerschaft gegen Metalldiebstahl) als „Herausragende Sicherheitspartnerschaft“. Der Zusammenschluss von Verbänden und Unternehmen aus Logistik, Telekommunikation, Bergbau und Energieversorgung wurde 2012 auf Initiative der Telekom, der Deutschen Bahn, der RWE sowie des Verbands Deutscher Metallhändler gegründet. Die meisten Mitglieder betreiben kritische Infrastrukturen, die für Bevölkerung, Wirtschaft und Staat unabdingbar sind.

Juroren der OSPAs waren unter anderem der bisherige Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), Michael Hange, und Dr. Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz (BfV). Die erstmals verliehenen Preise würdigen herausragende Leistungen von Unternehmen und Personen aus der Sicherheitsbranche. Die Awards werden in Zusammenarbeit mit Sicherheitsverbänden und -gruppen in verschiedenen Ländern verliehen. ■

„ES IST VERTRAUENSSACHE!“

DIE HACKTIVISTEN VON ANONYMOUS HABEN IM DEZEMBER 2015 DEN TÜRKISCHEN INTERNETSEKTOR ANGEGRIFFEN. DIE HACKER-GRUPPE „GHOSTSEC“ HAT DEM ISLAMISCHEN STAAT DEN CYBERKRIEG ERKLÄRT. UND DIE BUNDESWEHR BÜNDELT IT-EXPERTEN IN EINER EINHEIT, DIE SICH AUSSCHLIESSLICH UM CYBERABWEHR KÜMMERT. RUND DREI JAHRE NACH DEN ENTHÜLLUNGEN VON EDWARD SNOWDEN SCHEINT SICH DER CYBERWAR ZU EINER ERNSTHAFTEN BEDROHUNG FÜR DIE GESELLSCHAFT ZU ENTWICKELN. WAS SICH VERÄNDERT HAT, ERKLÄRT AXEL PETRI, LEITER GROUP SECURITY GOVERNANCE DER DEUTSCHEN TELEKOM.

Herr Petri, wann löst der Cyberkrieg die konventionelle Kriegsführung ab?
Axel Petri: Fest steht, das Internet ist inzwischen eine Plattform für Staaten oder internationale Organisationen, Computersysteme anderer Nationen zu attackieren oder auszuschalten. Es ist eine fortgeschrittene Form der Kriegsführung. Die Münchner Sicherheitskonferenz diskutierte daher Anfang letzten Jahres schon über das Thema „Hybride Kriegsführung”, also die Kombination von konventionellen und nicht konventionellen Formen der Kriegsführung – unter anderem von Cyberattacken.

Hat Edward Snowden indirekt dazu beigetragen, dass die Zahl der Cyberangriffe explodiert ist?
Axel Petri: Nein, er hat nur offengelegt, was längst Realität ist. Dass Spione spionieren, war nicht wirklich überraschend. Snowden hat uns aber die Augen geöffnet. Auch nach Snowden ist für mich die Existenz von Geheimdiensten nicht infrage gestellt. Eine absolut zentrale Rolle spielt aber die Verhältnismäßigkeit zwischen Sicherheit auf der einen und Privatsphäre auf der anderen Seite. Aus den Snowden-Unterlagen ergeben sich zahlreiche Maßnahmen, die zu weit gehen – ohne das Wissen der Öffentlichkeit und sogar ohne das Wissen der eigenen Regierung.

Welche Rolle spielen Geheimdienste bei Angriffen auf deutsche Ziele?
Axel Petri: In vielen Ländern ist Industriespionage Teil der Aufgabe der Geheimdienste. So spionieren ausländische Geheimdienste Deutschland weiterhin mit hohem organisatorischem und finanziellem Aufwand aus. Warum? Laut dem Bundesamt für Verfassungsschutz interessieren sie sich für uns aus geopolitischen und wirtschaftlichen Gründen. Wir sind Mitglied der NATO und der EU, verfügen über große ökonomische Kraft und innovative Unternehmen. Das sind Gründe genug für Spionage. Dass es im Netz keine Überwachung geben könnte, ist also eine Illusion, allerdings scheint die Verhältnismäßigkeit zum Teil aus den Fugen geraten. Die Menschen verstehen Sicherheitsbehörden zunehmend als Angreifer. Das ist nicht gut. Die staatlichen Institutionen müssen das Vertrauen der Bürger in sie zurückgewinnen. Das geht für mich insbesondere über die Erhöhung von Transparenz über deren generelle Überwachungstätigkeiten. Wir als Telekom tun dafür schon alles Mögliche, zum Beispiel mit unserem Transparenzbericht Lawful Interception / Data Provision. Die Sicherheitsbehörden selbst können da noch deutlich mehr tun.

Welche weiteren Bedrohungen gibt es?
Axel Petri: Wir dürfen bei aller Diskussion um Snowden nicht vergessen, dass die Zahl der konventionellen Cyberkriminellen deutlich zunimmt und deren Professionalität ebenso wächst wie die Verfügbarkeit einfacher, aber effektiver Angriffstools: Es gibt einen regelrechten Markt für Schadsoftware. Wenn Sie bezahlen, bekommen Sie einen top Service rund um die Uhr. Und das tangiert die Verbraucher wie auch die Unternehmen weitaus mehr. Denn jedes große Unternehmen ist heute von Cyberangriffen betroffen. Deswegen dürfen wir nicht nachlassen im Kampf gegen Hacker, sondern müssen uns kontinuierlich verbessern.

Wird sich die Zahl der Cyberangriffe weiterentwickeln?
Axel Petri: Wir müssen davon ausgehen, dass multidimensionale Attacken aus physischen und digitalen Komponenten stetig zunehmen werden. Denn die Bedeutung des Cyberraums steigt kontinuierlich an. Alles, was sich digitalisieren lässt, wird digitalisiert. Alles, was vernetzt werden kann, wird vernetzt. Das bedeutet: Die Zahl der Angriffe wird sich weiter erhöhen. Aber noch kritischer ist: Die Qualität der Angriffe nimmt zu. Dies wird im Vergleich zur Vergangenheit ganz neue Sicherheitsstrategien und -lösungen erfordern.

Das klingt nach Resignation.
Axel Petri: Wer sich zurücklehnt, verliert! Auch wenn es illusorisch ist, eine hundertprozentige Sicherheit in der virtuellen Welt zu erreichen. Wir müssen aber entscheiden, mit welcher digitalen Gesellschaft und welcher Sicherheitskultur wir leben wollen – und was wir dafür tun. Wir führen als Telekom und Sicherheitsexperten die Diskussion aktiv, da wir auch Teil des Spiels sind.

Wie reagieren die Menschen auf die vielen Schlagzeilen über gehackte Unternehmen und Regierungen?
Axel Petri: Die Menschen verlieren zunehmend das Vertrauen in die digitale Welt. Das ist dramatisch. Denn Vertrauen ist ein – wenn nicht sogar der – entscheidender Faktor für den Erfolg des digitalen Zeitalters. Hatten 2011 noch 42 Prozent der Menschen Vertrauen in die Sicherheit ihrer Daten im Internet, waren es ein Jahr später nur noch 29 Prozent und 2013 nur noch 16 Prozent. Das ist erschreckend für eine Gesellschaft, die zunehmend auf Digitalisierung baut. Denn ohne Internet gibt es keinen Fortschritt. Wir brauchen das Internet und wir brauchen Menschen, die ihm vertrauen und die neuen digitalen Möglichkeiten nutzen.

Wie gewinnen wir Vertrauen zurück?
Axel Petri: Zunächst brauchen wir effizientere Sicherheitsprozesse. Wir müssen also auf organisatorischer Ebene physische Sicherheit und Cybersicherheit zusammenbringen. Wenn die Prozesse stehen, geht es nicht ohne technische Innovationen, zum Beispiel ein Cyber Defense Center, das sämtliche Aktivitäten im Netz beobachtet und Gegenmaßnahmen einleitet. Nur so bleiben wir auf Augenhöhe mit den Angreifern und nur so können die Security-Experten der Unternehmen deren Mitarbeiter aufklären und ihnen Werkzeuge mitgeben, mit denen sie Gefahren erkennen. Dabei dürfen wir aber nicht stehen bleiben. Wir müssen die Medienkompetenz hinsichtlich Cybersecurity schon in den Schulen deutlich erhöhen und dürfen auch an den Universitäten nicht aufhören. Die wenigsten der zukünftigen Manager und Unternehmensführer werden IT-spezifische Fächer studieren, daher muss das Thema Cybersicherheit auch in klassischen Studiengängen wie BWL und Jura Eingang finden. Wer Gefahren erkennt, verhält sich automatisch sicherer.

Also kommt den Unternehmen eine wichtige Rolle zu?
Axel Petri: Wir müssen Gefahren transparent machen. Die Telekom macht das beispielsweise mit dem Sicherheitstacho oder indem wir Kunden aktiv auf aktuelle Risiken hinweisen. Und wir brauchen faire Bedingungen für alle: Wer auch immer den europäischen Markt adressiert, muss sich an dessen Regeln und Standards halten. Hard- und Softwarehersteller, ITK-Provider sowie „Over-the-top“-Anbieter – diese kostenlos Text-, Video und Audioinhalte übermitteln, – müssen sich zu Datensicherheit und Datenschutz bekennen, entsprechend transparent agieren und in Gegenmaßnahmen eingebunden sein. Denn nur wenn die komplette Wertschöpfungskette in deren Sicherung einbezogen ist, werden wir die Sicherheit im Netz so steigern können, dass die Kunden den digitalen Produkten und Dienstleistungen (wieder) vertrauen.

Axel Petri

ist Leiter Group Security Governance der Deutschen Telekom und Sicherheitsbeauftragter des Konzerns gem. § 109 TKG. Der Rechtsanwalt gewährleistet als Konzernsicherheitskoordinator den ganzheitlichen konzernweiten Securityansatz. Dies beinhaltet Strategie, Vorgaben und Kontrolle in allen Sicherheitsthemen ebenso wie die Steuerung der konzernweiten Kooperation der Sicherheitseinheiten. Zudem verantwortet er den Informations- und Wirtschaftsschutz ebenso wie den Bereich Ermittlungen und Prävention.

DATENSCHUTZ- UND DATENSICHERHEITSBERICHT 2015

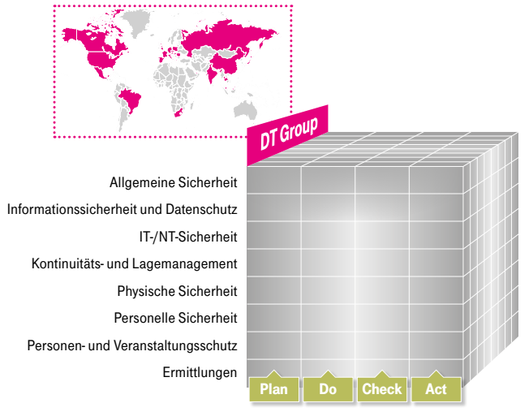
GRENZENLOSE SICHERHEIT

DATENSCHUTZ UND DATENSICHERHEIT ENDEN NICHT AN DER LANDESGRENZE. DIE TELEKOM SORGT WELTWEIT FÜR EINHEITLICHE STANDARDS.

Die gesetzlichen Anforderungen an Datenschutz und Datensicherheit unterscheiden sich von Land zu Land. In Deutschland sind sie besonders hoch, in vielen anderen Ländern vergleichsweise gering. Dennoch ist die Telekom bestrebt, ihren Kunden überall auf der Welt das für sie typische und insbesondere in Deutschland erforderliche hohe Schutz- und Sicherheitsniveau zu bieten. Die Group Security Governance (GSG) sorgt dafür, dass alle Konzernbereiche weltweit die gleichen Standards einhalten. Mittels kontinuierlicher Prüfungen gewährleistet der Bereich GSG, dass alle Unternehmenseinheiten die Sicherheitsrichtlinien des Governance-Modells der Telekom umsetzen. Dazu zählen nicht nur alle internen Bereiche und alle internationalen Landesgesellschaften, sondern auch alle externen Lieferanten, die Daten im Auftrag der Telekom speichern oder verarbeiten.

DAS SECURITY-GOVERNANCE-MODELL DER TELEKOM

Das Governance-Modell definiert die gesamte Organisationsstruktur des Konzerns und beschreibt alle zu ihrer Steuerung und Kontrolle erforderlichen Richtlinien und Maßnahmen. Die darin enthaltenen Konzernrichtlinien gewährleisten das hohe Sicherheits- und Datenschutzniveau der Telekom.



ÜBERALL GESETZESKONFORM UND SICHER

Um diese Aufgabe sinnvoll zu ergänzen, hat die GSG bereits im Jahr 2009 das Gremium „Audit Council“ gegründet, welches alle auditverantwortlichen Bereiche des Konzerns in regelmäßigen Abständen zusammenbringt. Hier werden nationale und internationale Prüfungsergebnisse ausgetauscht und eine gemeinsame Jahresplanung abgestimmt. Diese gemeinsame Vorgehensweise sorgt dafür, dass die richtigen Akzente gesetzt und Synergien erkannt bzw. realisiert werden. Kai Stursberg, einer der Auditoren der Group Security Governance: „Sowohl auf operativer als auch auf strategischer Ebene treffen wir uns mehrmals jährlich. Einerseits besprechen wir die Umsetzung von Normen und Kontrollsystemen, andererseits planen wir, welche sicherheitsrelevanten Themen künftig besonderes Augenmerk erfordern.“ Eines dieser künftig wichtigen Themen ist der grenzüberschreitende Datenverkehr. Am Beispiel Connected Car wird das sehr deutlich. „Stellen Sie sich vor“, erklärt Stursberg, „Sie fahren mit einem vernetzten Auto durch ganz Europa, das auch beim Passieren von Landesgrenzen Daten überträgt und empfängt. Wir werden dafür sorgen, dass diese Daten bei der Telekom überall gesetzeskonform und sicher behandelt werden.“

Seit dem 1. Januar 2015 arbeitet der Bereich GSG noch intensiver mit den Kolleginnen und Kollegen im Ausland zusammen. Die GSG-Spezialisten aus Deutschland besuchen regelmäßig die Landesgesellschaften vor Ort und überprüfen im Rahmen mehrtägiger Governance Checks den Umsetzungsstand der Policies. Mithilfe des Audit Councils konnten sie bereits einige Aktivitäten bündeln und gemeinsam mit anderen Auditeinheiten durchführen.

UNTERSTÜTZUNG FÜR DIE HUMAN FIREWALL

EINE KONZERNWEITE SECURITY-AWARENESS-STRATEGIE ERHÖHT DAS SICHERHEITSBEWUSSTSEIN DER GESAMTEN GRUPPE.

Informationen zählen zu den wichtigsten Faktoren für den betriebswirtschaftlichen Erfolg jedes Unternehmens. Sicherheit und Datenintegrität – insbesondere bei elektronischen Transaktionen – beeinflussen nicht zuletzt die Kundenbindung und das Kaufverhalten. Hier reichen technische Schutzmaßnahmen allein nicht aus. Vielmehr kommt es auf das richtige Zusammenspiel von Technologien, Prozessen und Menschen an. Der Mensch ist ein wichtiger Teil in der Sicherheitskette, um die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität dieser Informationen dauerhaft sicherzustellen. „Unsere Mitarbeiter“, sagt Cordula Tanner aus dem für Kommunikation, Training und Awareness zuständigen Bereich der Group Security Governance (GSG), „bilden eine menschliche Firewall nach außen, deren Widerstandskraft wir kontinuierlich stärken und unterstützen. Erst diese ‚Human Firewall‘ macht Sicherheit komplett.“

DIE WIRKSAMSTE SICHERHEITSMASSNAHME HEISST „SENSIBILISIERUNG“!

Um ihre Mitarbeiter für Datenschutz und Informationssicherheit zu sensibilisieren, investiert die Telekom bereits seit Jahren in Awareness-Kampagnen, -Trainings und -Kommunikationsmaßnahmen. Da weder Normen noch Regelwerke Security Awareness definieren, wurde Anfang 2015 eine konzernweite Security-Awareness-Strategie verabschiedet, um das Sicherheitsbewusstsein weltweit bei allen Beschäftigten methodisch, dauerhaft und nachhaltig zu stärken.

STRENG VERTRAULICH: DIE PRIVATSPHÄRE DES KUNDEN

DAS FERNMELDEGEHEIMNIS, PERSONENBEZOGENE KUNDENDATEN UND DIE VERFÜGBARKEIT DER TELEKOMMUNIKATION STEHEN IN DEUTSCHLAND UNTER EINEM BESONDEREN GESETZLICHEN SCHUTZ.

Netzbetreiber sowie Kommunikationsdiensteanbieter unterliegen den Vorgaben des Telekommunikationsgesetzes (TKG), mit dem der Bund die Schutz- und Sicherheitsanforderungen regelt. Wer öffentlich zugängliche Kommunikation anbietet, muss dafür sorgen, dass Kunden nicht unbefugt abgehört werden können und das Fernmeldegeheimnis gewahrt bleibt. Für diesen Zweck verpflichtet § 109 des TKG Netzbetreiber und Anbieter von Telekommunikationsdiensten, einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen. Das Sicherheitskonzept beschreibt, welche technischen Vorkehrungen und Maßnahmen der Anbieter trifft, um die gesetzlichen Anforderungen an Sicherheit und Datenschutz zu erfüllen. Die Bundesnetzagentur ist auf Behördenseite dafür zuständig, die Einhaltung der Sicherheitsanforderungen zu überprüfen. Für diesen Zweck führt sie regelmäßig Audits bei den Anbietern durch.

ALLE ÜBERPRÜFUNGEN STETS ANSTANDSLOS

Das Team der Group Security Governance der Telekom erstellt und pflegt das Sicherheitskonzept für die Deutsche Telekom AG, die Telekom Deutschland GmbH und die T-Systems International GmbH. Bei jeder organisatorischen oder technologischen Änderung überarbeitet das Team den vertraulichen Inhalt und legt ihn der Bundesnetzagentur vor.

Als größtes Telekommunikationsunternehmen Deutschlands steht die Telekom in engem Austausch mit den Behörden. Umfassende Sicherheitsaudits finden jährlich oder spätestens im Abstand von zwei Jahren statt. Daneben überprüft die Bundesnetzagentur kontinuierlich auf theoretischer Basis, wie die Telekom sicherheitsrelevanten Fragestellungen und Bedrohungsszenarien begegnet. Alle Überprüfungen verlaufen stets ohne Beanstandung und zur vollen Zufriedenheit der Bundesnetzagentur. Dadurch werden das Konzept und die Umsetzung der Sicherheitsmaßnahmen bei der Telekom bestätigt. Und die Group Security Governance sorgt dafür, dass das auch so bleibt.

FÜHRENDER DIENSTLEISTER FÜR IT-SICHERHEIT

ACHT DIENSTLEISTUNGSKATEGORIEN, ACHTMAL IM LEADERQUADRANTEN: DIE EXPERTON GROUP SIEHT DIE DEUTSCHE TELEKOM IM SECURITY VENDOR BENCHMARK 2016 ALS FÜHRENDEN ANBIETER VON SICHERHEITSLÖSUNGEN.

In allen Kategorien gehört die Telekom als „strategischer Taktgeber und Meinungsführer zu den Anbietern mit einem hochattraktiven Serviceangebot sowie einer ausgeprägt starken Markt- und Wettbewerbsposition“, so die Analysten. Auf den Prüfstand kamen bei der Bewertung die Kategorien Database Security, Cloud und Datacenter Security, Backup / Data-Recovery Services, Identity & Access Management, Mobile Security Services, Managed Security Service, Security Consulting, Disaster Recovery Services.

Auch im Securitymarkt setzt sich das Outsourcing immer mehr durch. Laut Benchmark ist die Deutsche Telekom in diesem Markt für Managed Security Services „sowohl hinsichtlich der Portfolioattraktivität als auch der Wettbewerbsstärke das Maß der Dinge“. Für das Securityoutsourcing sprechen insbesondere die geringeren Investitionskosten sowie das stets aktuelle Wissen über die sich ständig ändernden Cyberbedrohungen. Das Telekom-Portfolio deckt zudem die gesamte Bandbreite von Sicherheitsdiensten ab, wodurch der Security-Provider Ende-zu-Ende-Verantwortung bieten kann. „Ein zunehmend stärkeres Argument für die Deutsche Telekom ist die Leistungsbereitstellung aus Deutschland unter den Regeln des deutschen Datenschutzrechts“, betonen die Analysten von Experton.

Die Analysten heben im Benchmark hervor, dass die Telekom für sämtliche internen Sicherheits- und Kundenprojekte eigene Tools wie das PSA (Privacy and Security Assessment) oder ESARIS (Enterprise Security Architecture for Reliable Services) nutze. Mit diesen Tools lassen sich Sicherheitslücken identifizieren und darauf aufbauend lässt sich ein Maßnahmenkatalog entwickeln. Die eingesetzten Securityprodukte werden dann gemeinsam mit den Kunden herstellerunabhängig ausgewählt.

Das Portfolio Mobile Security Services hat die Deutsche Telekom auch 2015 erneut erweitert. Neben Lösungen für das Mobile Device Management (MDM) bietet die Telekom Antiviruslösungen von Symantec und Norton sowie eine eigens entwickelte Unternehmenscontainerlösung „Safe Mobile Business App“. Mit der Mobile Encryption App können Telefonate verschlüsselt werden und jetzt zusätzlich Telefonkonferenzen mit bis zu drei Teilnehmern. Die hochgradig sichere Mobile Encryption App ermöglicht darüber hinaus auch verschlüsseltes Telefonieren und SMS..

Den Bereich Dienstleister für Identity & Access Management deckt die Telekom insbesondere durch „Authentication“ sowie „Identity as a Service“ ab. Hierzu gehören die Zwei-Faktor-Authentifizierung zur Autorisierung von Benutzern per Smartphone, SMS oder Hardware-Token und ein Validierungsdienst für Authentifizierungsverfahren wie etwa mit Smart Card oder Biometrie. Dazu kommen bei der Telekom „Single Sign-on as a Service“ für den Zugriff auf SaaS-Angebote und Webdienste in der Cloud sowie lokale Anwendungen.

Auch im Bereich Security Consulting hält die Telekom im Konzert der großen internationalen Spieler mit. Hier setzen sich die drei Besten etwas von anderen Anbietern im Leaderquadranten ab, da sie bei den Kriterien lokale Marktposition, Vertriebs- und Marketingstärke, Awareness und Kundenzufriedenheit insgesamt etwas stärker sind als die Konkurrenz.

KONTINUIERLICH MESSEN UND VERBESSERN

REGELMÄSSIGE UMFRAGEN DOKUMENTIEREN DEN STATUS VON INFORMATIONSSICHERHEIT UND SICHERHEITSBEWUSSTSEIN IM KONZERN. DIE ERGEBNISSE DIENEN DER STETIGEN VERBESSERUNG.

Einmal pro Jahr führt der Bereich Group Security Governance (GSG) eine konzernweite Online-Awareness-Umfrage durch. Alle Unternehmenseinheiten weltweit, die zehn oder mehr Mitarbeiter beschäftigen, nehmen daran teil. Die Erhebung misst das Sicherheitsbewusstsein der Beschäftigten und erfasst die Effizienz von Awareness-Maßnahmen. Darüber hinaus ermöglicht sie die Analyse zeitlicher Veränderungen im Sicherheitsbewusstsein sowie den Vergleich zwischen Konzerneinheiten. Nicht zuletzt zeigt sie Handlungsbedarf auf.

Das anonymisierte Ergebnis ist eine verdichtete Kennzahl, die das durchschnittliche Sicherheitsbewusstsein der Beschäftigten widerspiegelt. Alle Awareness-Ansprechpartner besprechen diese Ergebnisse und leiten Maßnahmen wie etwa Schulungen daraus ab, um das Sicherheitsbewusstsein der Mitarbeiter gezielt zu verbessern.

IMMER AUF DEM NEUESTEN STAND

Die GSG führt regelmäßig eine weitere Befragung unter den Sicherheitsverantwortlichen aller Unternehmenseinheiten durch. Die Experten messen dabei den Reifegrad der Sicherheit im Konzern auf Basis einer Selbstbewertung, der im „Security Maturity Report“ festgehalten wird. Die Auswertungen erhält jede Einheit in ihrem eigenen Reifegradbericht. Darüber hinaus übergibt die GSG die aggregierten Ergebnisse aller Berichte an die Fachbereiche des Telekom Security Managements. Das ermöglicht den Einheiten wie auch den zentralen Sicherheitsbereichen, eine transparente und vergleichbare Grundlage für die gemeinsame Kommunikation und Weiterentwicklung von Sicherheitsthemen und -maßnahmen zu nutzen. Sämtliche Untersuchungsergebnisse fließen zudem in den jährlichen Erkenntnisbericht „Annual Review of International Security“ ein. Die Führungskräfte nutzen die damit gewonnenen Einsichten, um das Sicherheitsniveau auf hohem Niveau zu halten.

ERFOLGSFAKTOR SICHERHEIT

LÄSTIGE PFLICHT ODER GEWINNBRINGENDE KÜR? DIESE FRAGE STELLT SICH FÜR DIE TELEKOM NICHT. SIE SETZT KONSEQUENT AUF DATENSICHERHEIT UND EINE KONZERNWEITE SICHERHEITSSTRATEGIE

Für die Telekom als führender europäische Telekommunikationsprovider ist Sicherheit einer der Erfolgsfaktoren im Markt. Sie hat dafür eine Sicherheitsstrategie entwickelt, die sich aus drei strategischen Sicherheitsfeldern zusammensetzt und auf der umfassenden Sicherheitsexzellenz im Konzern fußt: „Protect – Enable – Monetize powered by Security Excellence“. Basis der Strategie ist der Schutz des eigenen Unternehmens samt der Netzwerkinfrastruktur, den selbst genutzten IT-Lösungen sowie allen damit verknüpften Daten – insbesondere den Kundendaten.

Der Eigenschutz (Protect) umfasst drei Bereiche: Sicherheitskultur, Sicherheitsbetrieb und Sicherheitscompliance. In der Kultur sind unter anderem die Governance, Verantwortlichkeiten und die einheitlichen Sicherheitsvorgaben geregelt. Im Betrieb werden präventive, abwehrende und reaktive Sicherheitsmaßnahmen eingesetzt. Dazu gehört unter anderem der Einsatz von Abwehrtechnologien oder das Cyber Defence Center. Der Complianceblock gewährleistet die effiziente Beachtung gesetzlicher und regulatorischer Auflagen und Anforderungen und stellt deren Umsetzung im Konzern sicher. Das zweite strategische Sicherheitsfeld (Enable) richtet sich an Telekom-interne Bereiche, die Öffentlichkeit sowie die Kunden. Telekom-intern werden Sicherheitsanforderungen nahtlos in Produkte, Services und Lösungen integriert. Ein bedeutendes Verfahren, Sicherheit und Datenschutz von Grund auf konsequent in Produkte einzubauen, ist das Privacy & Security Assessment (PSA), das alle IT- und Netzwerkentwicklungsprozesse innerhalb der Telekom begleitet.

Die Positionierung als vertrauenswürdiges Unternehmen geschieht über das Engagement in politischen Debatten, Teilnahmen an Gremien oder die transparente Darstellung von Datenschutz- und Datensicherheitsmaßnahmen. Dazu gehört es beispielsweise auch, Sicherheitszertifikate anerkannter Zertifizierungsinstitute und Auditoren nach entsprechender Prüfung zu erhalten. Sie sind Nachweis der Sicherheitsexpertise und der Nutzung sicherheitskonformer Prozesse im Unternehmen.

Das dritte strategische Sicherheitsfeld fokussiert darauf, das vorhandene Sicherheits-Know-how im Konzern in einem eigenen Sicherheitsgeschäftsbereich zu bündeln und einen entsprechend übergreifenden Marktangang zu Sicherheit zu schaffen („Monetize“). Er wird Privat-, Mittelstands- sowie Großkunden künftig Sicherheitsprodukte und -dienstleistungen aus einer Hand anbieten. Das Ziel: führender Anbieter im europäischen Sicherheitsmarkt.

ERFOLGREICHE REZERTIFIZIERUNG

WEITERMACHEN, KORRIGIEREN, VERÄNDERN, VERBESSERN: ALLTAG FÜR DEN BETRIEB EINES INFORMATIONS-SICHERHEITSMANAGEMENTSYSTEMS (ISMS). 2015 HAT DIE DQS DAS ISMS DER TELEKOM ERNEUT ZERTIFIZIERT.

Ein Informationssicherheitsmanagementsystem (ISMS) definiert Verfahren und Regeln, welche die Informationssicherheit in einem Unternehmen dauerhaft steuern, kontrollieren, aufrechterhalten und fortlaufend verbessern. Die Telekom nutzt ein ISMS, mit dem sie die Sicherheitsdienstleistungen für den gesamten Konzern managt und unterstützt. 2015 hat das Zertifizierungsunternehmen DQS das ISMS auditiert und das ISO/IEC 27001:2013 Zertifikat bestätigt.

Die Zertifizierung ist der Nachweis für die kontinuierlich hohe Qualität und zukunftsorientierte Weiterentwicklung der Sicherheitsarbeit bei der Telekom und somit ein wichtiger Baustein für das hohe Vertrauen in das Unternehmen. Doch die Arbeit an dem ISMS endet nicht mit einer Zertifizierung. Als lebendiges und anpassungsfähiges System, wird es mit einem kontinuierlichen Verbesserungsprozess permanent angepasst und erweitert. Nur so lassen sich bestehende Restrisiken systematisch und beständig verringern.

Ein zertifiziertes Sicherheitsmanagementsystem ist auch für immer mehr Unternehmenskunden ein Baustein, auf Services der Telekom zu setzen – zum Beispiel auf Cloud-Lösungen, welche die Telekom in ihren deutschen Rechenzentren betreibt.

SECURITY PROFESSIONAL DEVELOPMENT

SICHERHEIT LÄSST SICH NICHT EINFACH DURCH TECHNISCHE LÖSUNGEN ERZIELEN. UNTERNEHMEN BRAUCHEN GUT AUSGEBILDETE SICHERHEITSEXPERTEN, UM DEN ZUNEHMENDEN ANFORDERUNGEN ZU BEGEGNEN. DIE TELEKOM HAT EINEN WEITERBILDUNGSPLAN ZUR QUALIFIZIERUNG VON SICHERHEITSEXPERTEN AUFGESETZT, DER DEM INTERNATIONALEN INDUSTRIESTANDARD ENTSPRICHT.

Wie in allen Branchen und in allen größeren Betrieben durchlaufen auch Sicherheitsexperten eine entsprechende Qualifizierung. Diese entspricht in der Regel den nationalen Erfordernissen. Aufgrund der weltweiten Zusammenarbeit von über 50 Gesellschaften der Telekom in Sicherheitsbelangen wird ein international breites Wissen verlangt. Das gilt insbesondere für die obersten Sicherheitsverantwortlichen (Chief Security Officer) jeder einzelnen Telekom Gesellschaft, aber auch für Experten von anderen Sicherheitsfunktionen, zum Beispiel die Business Continuity oder Fraud Manager. Entsprechende Lehrgänge werden jährlich gestaffelt in thematischen Wechseln für Präsenztrainings und Onlinetrainings angeboten. 2015 nahmen mehr als 60 Beschäftigte aus Deutschland und den Landesgesellschaften an unterschiedlichen E-Learning-Trainings und Workshops teil.

Ein wichtiges und komplexes Weiterbildungsthema ist das Enterprise Security Risk Management. Hier schulte die Telekom gemeinsam mit einem englischen Partner 24 international tätige Telekom Mitarbeiter pro Lehrgang. Risikomanager analysieren Sicherheitsrisiken für ihr jeweiliges Unternehmen und legen fest, wie damit umgegangen werden soll, um die Risiken zu minimieren. Durch den weltweiten Anstieg der Cyberangriffe kommt dem Thema „Fraud“ – also der Wirtschaftskriminalität – eine zunehmend bedeutendere Rolle zu. Wirtschaftsstraftaten sind für Unternehmen in doppelter Hinsicht gravierend: Sie verursachen konkrete Schäden und können mit Vertrauens- und Reputationsverlust einhergehen. Die Ausbildung rund um das Thema Fraud ist eine entsprechend wichtige Komponente des Weiterbildungsprogramms für Sicherheitsexperten der Telekom. Insgesamt fast 50 Personen nahmen 2015 an den Trainings zum Fraud Manager, dem Training zum International Certified Fraud Investigator und dem Advanced Certified Fraud Investigator teil.

Neben der internen Weiterbildung zu Security Professionals beteiligt sich die Telekom darüber hinaus an vielen unternehmensübergreifenden Netzwerken, in denen sich Sicherheitsexperten und Security Professionals über aktuelle Entwicklungen austauschen. Sie steht zudem mit Forschern in Universitäten in ständigem Austausch und entwickelt beispielsweise mit der Hochschule für Telekommunikation in Leipzig ein „Cyber Security Onlinetraining“ für Nichttechniker.

Zusätzlich baut das Sicherheitsteam aktuell eine auf Sicherheitsthemen fokussierte Bibliothek auf, in der eine breit gefächerte Sammlung von Fachbüchern sowohl als klassisches Buch wie auch online zur Verfügung stehen. Erweitert wird das Ganze durch eine Sammlung an Whitepapers. Denn nur wer sich auskennt, kann sich entsprechend verhalten: Gefahr erkannt – Gefahr gebannt.

MEHR KONTROLLEN, WENIGER RESSOURCEN

NUR MIT REGELMÄSSIGEN KONTROLLEN LASSEN SICH KONZERNWEITE DATENSCHUTZ- UND DATENSICHERHEITSVORGABEN DAUERHAFT EINHALTEN. SEIT 2015 KOOPERIEREN DIE KONTROLLTEAMS DER TELEKOM ABTEILUNGSÜBERGREIFEND.

Vertrauen ist gut, Kontrolle ist besser. Daher sorgten bisher getrennte Teams aus den Datenschutz- und Datensicherheitsabteilungen der Telekom mit regelmäßigen Kontrollbesuchen konzernweit – also auch bei den Landesgesellschaften – für die Einhaltung der Datenschutz- und Datensicherheitsvorschriften. Eine zeitaufwendige Aufgabe für die beiden Kontrollteams, die quer durch Europa sowie Asien und Amerika getrennt unterwegs waren.

Seit 2015 führen die Abteilungen Datenschutz und Datensicherheit immer mehr Kontrollen gemeinsam durch. Dafür stimmen sie ihre Termine eng aufeinander ab und können mit kleineren Teams mehr Kontrollen vornehmen. Dies ist möglich, da es bei Datenschutz- und Datensicherheitskontrollen Schnittmengen gibt. Denn Datenschutz ohne technische Umsetzung kann im digitalen Zeitalter nicht funktionieren.

Die gemeinsamen Termine bedeuten für alle Beteiligten ein Win-win-Situation. Da in den Ländern die Personalressourcen für die Vorbereitung und Begleitung der Kontrollen begrenzt sind, müssen sie nun nur noch einmal die Ressourcen bereitstellen. Die Kontrollteams selbst sind auch kleiner, da es überschneidende Themen gibt. Dies setzt Ressourcen frei, um mehr Kontrollen durchführen beziehungsweise die Umsetzung von vereinbarten Maßnahmen besser begleiten zu können.

SONDEREINSATZ GEGEN BETRÜGER

EIN BEREICHSÜBERGREIFENDES SPEZIALISTENTEAM DER TELEKOM SORGT FÜR SAUBERE GESCHÄFTE BEI DEN VERTRIEBSPARTNERN. DIE PARTNER MÜSSEN SICH AUCH IM HARTEN WETTBEWERB AN DIE SPIELREGELN HALTEN.

In der Vergangenheit haben externe Vertriebspartner mit unerlaubten Mitteln Prämien und Provisionsbetrug betrieben. Dabei ging es zum Beispiel um nicht genehmigte Vermarktungsformen, den Einsatz von nicht autorisierten Subpartnern oder um die Manipulation von Aufträgen (beispielsweise fiktive Kunden).

Die Telekom hat daher den „Round Table Sicherheit in Vertrieb & Service“ zusammengestellt, an dem Mitarbeiter aus unterschiedlichen Bereichen Maßnahmen absprechen, die das unerlaubte Vorgehen im Partnervertrieb verhindern. Seit 2012 ist der Round Table ein etabliertes Beratungsgremium, das alle Aktivitäten rund um die Betrugsbekämpfung bündelt und koordiniert. Alle zwei Wochen tagt die Runde und berichtet ihre Ergebnisse dann an die Geschäftsführung.

Das Team unter der Leitung der Sicherheit besteht daneben aus Vertretern der Bereiche Vertrieb, Risikomanagement, Wirtschaftsstrafrecht, Zivilrecht, Revision, Datenschutz und Compliance. Empfohlene (und dann auch umgesetzte) Maßnahmen waren unter anderem die Kündigung der Zusammenarbeit mit auffälligen Vertriebspartnern, Geltendmachung von Schadensersatz und Anzeigeerstattung. Mehr als 100 Betrugsfälle hat der Round Table inzwischen aufgearbeitet. Dieses konsequente Vorgehen hat dazu geführt, dass die Partner deutlich sauberer arbeiten als in der Vergangenheit.

DIGITALE AUFKLÄRUNG 2.0: MENSCHEN UND UNTERNEHMEN WIRKLICH ERREICHEN!

MENSCHEN IM DIGITALEN ALLTAG KONKRET ZU ERREICHEN UND FÜR EINEN SICHEREN UMGANG MIT DER DIGITALISIERUNG ZU BEGEISTERN – DAS IST DIE TÄGLICHE HERAUSFORDERUNG VON „DEUTSCHLAND SICHER IM NETZ“. DAFÜR ENTWICKELT DER VEREIN FORTLAUFEND STARKE AKTIONEN FÜR VERBRAUCHER UND KLEINERE UNTERNEHMEN. ZUM 10-JÄHRIGEN JUBILÄUM VON „DEUTSCHLAND SICHER IM NETZ“ IM JAHR 2016 WERDEN NEUE PARTNER UND UNTERNEHMEN EINGELADEN.

Die Botschaft des jährlichen DsiN-Sicherheitsindex für Verbraucher 2015 war eindeutig: Während die Verunsicherung im Internet zunimmt, stagniert die Bereitschaft zur Ergreifung von Sicherheitsmaßnahmen im eigenen Umfeld. Dieser Trend beschränkt sich keineswegs auf die Gruppe der sogenannten Fatalisten im Index, sondern umfasst auch die gutgläubigen und außenstehenden Nutzer.

Für das Team von „Deutschland sicher im Netz“ war dieses Ergebnis ein zusätzlicher Ansporn, die Aufklärungsarbeit in Deutschland 2015 weiter voranzutreiben und im Verbund mit seinen Partnern zu professionalisieren. Unter dem Begriff der Digitalen Aufklärung 2.0 standen drei gemeinsame Ansätze im Mittelpunkt:

1. Zielgruppenspezifische Aufklärungsarbeit, die die individuellen Bedürfnisse der Verbraucher stärker in den Fokus nimmt – statt Aufklärung mit der Gießkanne.
2. Bündelung bestehender Initiativen, damit bestehende Initiativen und Angebote für Unternehmen und Verbraucher einfacher gefunden werden sowie
3. Förderung des Dialogs mit Vertretern aus der Wissenschaft, Wirtschaft, Gesellschaft und Politik, um Chancen der Aufklärungsarbeit besser zu verstehen und zu nutzen.

Die Gründung des Aktionsbundes Digitale Sicherheit im Sommer 2015 ist nur ein Beispiel für die Bündelung von Angeboten unter dem Dach von DsiN. In dieser Plattform stellen DsiN-Partner gemeinnützige Initiativen für digitale Aufklärung ein, die von Verbrauchern und Mitarbeitern leicht aufgefunden werden. Der Aktionsbund ist in den ersten Monaten auf 50 Organisationen angewachsen. Der Service kann als iFrame auf jedem Webportal kostenlos eingefügt werden.

Als individualisierbarer Ratgeber für Verbraucher im digitalen Alltag bietet das SiBa – Sicherheitsbaromter seit November 2015 konkrete Sicherheitstipps zu Warnmeldungen. Dazu werden Angebote der Partner wie BKA und BSI, des Banken- und Versicherungsverbands und der DsiN-Mitglieder Deutsche Telekom, Microsoft und Nokia eingebunden. SiBa ist auf Themen wie Smart Home oder Vitaldienste anpassbar und findet großen Anklang: In den ersten Wochen haben bereits 25 000 Verbraucher die App genutzt.

Die lebendige Ansprache und Verbreitung innerhalb der Verbrauchergruppen sind seit jeher ein Bestandteil der Aufklärungsarbeit von DsiN. Mit dem Jugendwettbewerb myDigitalWorld, der 2015 erstmals ausgerichtet wurde, werden vorbildliche Engagements von Jugendlichen und Schülern ausgezeichnet. Die Preisträger konnten „coole Preise“ gewinnen – von Reisen nach London bis zu konkreter Unterstützung für ihr Projekt. Das Bundesministerium des Innern, Förderer des Wettbewerbs, würdigte die Teilnehmer als Vorbilder in ihrer Generation.

Nicht nur bei Verbrauchern, sondern gerade auch in den kleineren Betrieben fehlen oftmals Sicherheitsexpertise sowie die Bereitschaft, sich umfassender mit Sicherheitsaspekten zu befassen. Besondere Aufmerksamkeit der Aufklärungsarbeit bei DsiN galt daher auch 2015 in besonderem Maße wieder den mittleren und kleinen Unternehmen.

- Die Sicherheitsoffensive von DsiN und DIHK in dem Projekt IT-Sicherheit@Mittelstand bietet Entscheidern in kleinen und mittelständischen Unternehmen und IT-Verantwortlichen konkrete Anleitungen für IT-Sicherheit im Unternehmen. Unter der Schirmherrschaft von Bundeswirtschaftsminister Sigmar Gabriel stellt die gemeinsame Initiative unter dem Dach von DsiN für alle IHKs bundesweit Referenten und kostenfreie Unterlagen bereit.
- Für die Sicherheit im Betrieb bieten die DsiN-Leitfäden, die gemeinsam mit dem DsiN-Mitglied DATEV herausgegeben werden, konkrete Anleitungen für digitalen Schutz. Schwerpunkt der Publikationsreihe im vergangenen Jahr waren unterstützende Anleitungen zur Bekämpfung von Social Engineering am Arbeitsplatz. Die Leitfäden können kostenfrei bei DsiN bezogen werden.
- Zur Förderung des Dialogs über IT-Sicherheit liefert der DsiN-Blog seit vier Jahren regelmäßige Fachbeiträge, die bundesweit von zahlreichen mittelständischen Mitarbeitern und Entscheidern gelesen und diskutiert werden. Das Kernteam umfasst 50 Gastautoren aus Wirtschaft, Wissenschaft und der Sicherheitspraxis.

Sämtliche Initiativen von DsiN sind getragen von der Überzeugung des Vereins, dass erst im gemeinsamen Zusammenwirken aller Beteiligten ein nachhaltiger Beitrag für mehr IT-Sicherheit gelingen kann. Der Beschluss der Digitalen Agenda des Bundesregierung, die Aufklärungsarbeit von DsiN für eine breitere Öffentlichkeit zu verstärken, untermauert diesen Anspruch. Dieser Beschluss wurde im vergangenen Jahr mit Leben gefüllt, indem mehrere spannende Aufklärungsprojekte für digitale Sicherheit von DsiN seitens der Bundesregierung erstmals gefördert wurden. Dazu zählen insbesondere

- die Digitale Nachbarschaft zur Unterstützung von ehrenamtlichem Engagement und Vereinen mit Förderung durch das Bundesministerium des Innern,
- der DigitalKompass für digitale Stammtische älterer Generationen im Verbund mit der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) mit Förderung durch das Bundesverbraucherschutzministerium sowie
- IT-Sicherheit für Berufsschüler im Projekt „Bottom up“ für eine Sensibilisierung der Mitarbeiter der Zukunft mit Förderung durch das Bundeswirtschaftsministerium.

In diesem Jahr feiert der Verein sein 10-jähriges Bestehen und ist gut gewappnet, sein Themenspektrum auch in innovativen Themenfeldern wie vernetztes Fahren, digitale Vitaldienste und intelligente Häuser weiter auszubauen und neue Unterstützer zu gewinnen. Für eine erfolgreiche Fortführung der Mission wählte der Verein auf seiner Mitgliederversammlung Herrn Dr. Thomas Kremer, Mitglied des Vorstands der Deutsche Telekom AG, zum neuen Vorsitzenden.

Nach dem erfolgreichen Jahr mit dem starken Engagement der Mitglieder von DsiN, Partner und Unterstützer ist die Vorfreude auf „10 Jahre DsiN“ 2016 gestiegen. Der wachsenden Nachfrage nach IT-Sicherheit und dem enormen Bedürfnis nach Orientierung und Sicherheit soll mit konkreten Projekten, ergänzenden Studien und Veranstaltungen nah bei den Verbrauchern und Unternehmen begegnet werden.

Wir laden Sie herzlich ein, mitzumachen!

Dr. Michael Littger

ist Geschäftsführer des Vereins „Deutschland sicher im Netz“. Zuvor war der promovierte Jurist für die EU-Kommission in Brüssel aktiv und mehrere Jahre im Bundesverband der Deutschen Industrie für die Themenbereiche digitale Wirtschaft, Telekommunikation und Medien tätig.

IMPRESSUM

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Datenschutz,
Recht und Compliance
53262 Bonn, Deutschland
Telefon: 0228 181 4949
Telefax: 0228 181 94004
E-Mail: datenschutz@telekom.de
cert@telekom.de
www.telekom.com/datenschutz
www.telekom.com/sicherheit

www.telekom.com/datenschutz

www.telekom.com/sicherheit

Stand: 2/2016

ERLEBEN, WAS VERBINDET.