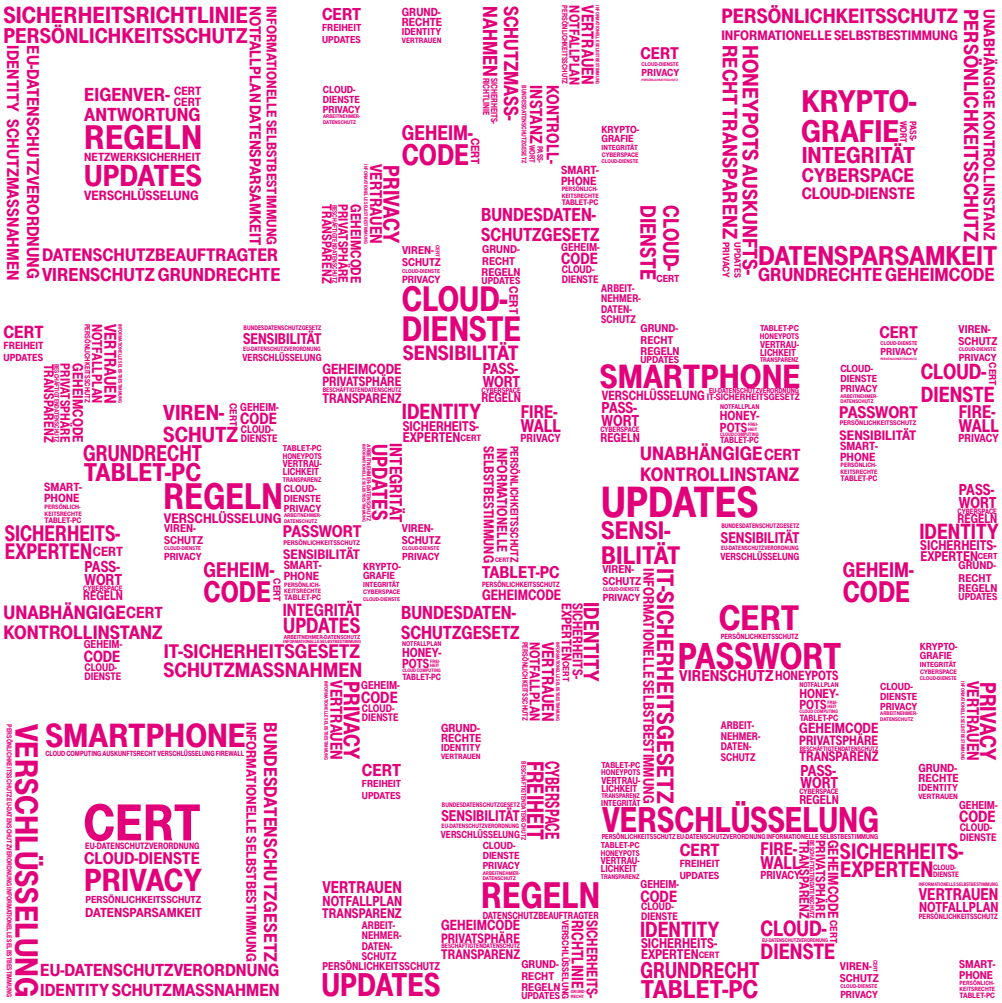


DATENSCHUTZ UND DATENSICHERHEIT

Bericht 2013

ERLEBEN, WAS VERBINDET.

INHALT

„WIR MÜSSEN VERTRAUEN ZURÜCK-GEWINNEN.“

Der Datenschutz im Jahr 2013 stand ganz im Zeichen der Geheimdienstaffären. Bürger und Unternehmen sind verunsichert. Politik, Wirtschaft und Wissenschaft müssen die Vertrauenskrise zum Anlass nehmen, gemeinsam neue Lösungen zu entwickeln, fordert Dr. Thomas Kremer, Vorstand Datenschutz, Recht und Compliance.

Ein Weckruf, ein Paukenschlag, ein Erdbeben. Mögen manche Experten auch sagen, dass sie die Enthüllungen Edward Snowdens nicht überrascht haben. Die breite Medienberichterstattung über die Aktivitäten der NSA und ihrer Verbündeten bedeutete aber zweifellos eine Zäsur in der Debatte um Datenschutz und IT-Sicherheit in Deutschland. Nie zuvor hatten diese Themen so große öffentliche Aufmerksamkeit. Gleichzeitig ist das Vertrauen der Bevölkerung in Telekommunikation und Internet deutlich zurückgegangen.

Aus Sicht der Telekom ist die Balance von Sicherheit und Freiheit aus dem Lot geraten, wenn Geheimdienste persönliche Daten massenweise und anlasslos ausspionieren und speichern. Man kann Freiheit nicht verteidigen, indem man die Persönlichkeitsrechte außer Kraft setzt. Die Telekom hat deshalb klar Position bezogen und sich so viel Kritik eingehandelt. Mit bloßen Aufklärungsappellen an die Politik wollten wir uns aber nicht zufriedengeben. Wir verstehen es als unseren Auftrag, die persönlichen Daten unserer Kunden zu schützen.

Es gibt einiges, was wir konkret tun können, um das Vertrauen der Menschen zurückzugewinnen. Die bessere Verschlüsselung von E-Mails und Handygesprächen ist eine Maßnahme, welche die Telekom sofort umgesetzt hat. Auch der Vorschlag für ein Internet der kurzen Wege lässt sich schnell und einfach realisieren. Warum muss eine E-Mail von Bonn nach Köln über London oder New York geleitet werden?

Natürlich sind wir uns darüber im Klaren, dass durch die Verkehrsführung alleine das Sicherheitsproblem nicht gelöst wird. Die Telekom setzt sich seit Jahren für die europäische Datenschutzgrundverordnung ein. Wir brauchen in Europa einheitliche und hohe Datenschutzstandards, die zudem dann auch für außereuropäische Anbieter gelten, wenn sie ihre Dienste in Europa anbieten möchten. Die Debatte um die Grundverordnung wird uns auch 2014 weiter begleiten. Das Gleiche gilt für die Vorratsdatenspeicherung: Das Bundesverfassungsgericht und jüngst

„Die Enthüllungen von Snowden waren ein Weckruf!“

auch der Europäische Gerichtshof setzen dem Gesetzgeber für die europäische und die deutsche Ebene Grenzen. Das reflektiert die hohe Bedeutung, die dem Schutz der Persönlichkeitsrechte in Europa beigemessen wird. Die Diskussion, auf wie viel Freiheit zugunsten der Sicherheit verzichtet werden soll, ist längst nicht zu Ende geführt. In der Europäischen Union sollten wir zudem vollständig auf die gegenseitige Bespitzelung verzichten. Und wir brauchen ein Safe-Harbor-Abkommen, das diese Bezeichnung verdient. Die USA sind für die Daten europäischer Bürger derzeit alles andere als ein sicherer Hafen. Die Politik wird also nicht aus der Verantwortung genommen werden können, wenn es darum geht, das Vertrauen der Menschen zurückzugewinnen.

Aber auch die Unternehmen können mehr tun: Wir als Deutsche Telekom sind gefordert, Datenschutz und IT-Sicherheit als Wettbewerbsvorteile auszubauen. Dafür müssen hohe Standards von Anfang an in die Entwicklung neuer Produkte und Dienste integriert werden. Ein Beispiel dafür kann die Weiterentwicklung europäischer Cloud-Dienste sein. Zudem stellt sich die Frage, wie wir verantwortlich mit den technischen Möglichkeiten umgehen, welche die Massenauswertung von Daten (Big Data) bietet. Und ganz oben auf der Agenda bleibt weiterhin der gemeinsame Kampf gegen Cyberkriminalität und Wirtschaftsspionage.

Wie können wir vor allem Unternehmen im Mittelstand besser für die Gefahren von Cyberkriminalität sensibilisieren? Und welche konkreten Lösungen bieten wir als Schutz für Geschäfts- und Privatkunden an? Der Dialog zwischen Wirtschaft, Wissenschaft und Politik muss intensiviert werden. Die Telekom wird sich weiterhin für den Austausch einsetzen und beispielsweise mit der Münchner Sicherheitskonferenz den Cyber Security Summit fortsetzen.

Es gibt durchaus die Chance, den Skandal zum Ausgangspunkt einer positiven Entwicklung zu machen. Die Telekom hat damit jedenfalls gute Erfahrungen gemacht. Ja, die Enthüllungen von Edward Snowden waren ein Weckruf. Jetzt geht es darum, nicht wieder einzuschlafen.

ZUR PERSON

Dr. Thomas Kremer
ist seit Juni 2012 Vorstand Datenschutz, Recht und Compliance bei der Deutschen Telekom AG. 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.

„UNSERE REFORM IST EIN MARKTÖFFNER“

Der Innenausschuss des EU-Parlaments hat am 21. Oktober 2013 mit großer Mehrheit den lange umkämpften Entwurf für eine neue Datenschutzgrundverordnung angenommen. Damit ist der Weg frei für die erste umfassende Änderung der europäischen Datenschutzbestimmungen seit 1995.

Wie zufrieden sind Sie mit dem bisherigen Verlauf der Entwicklung der EU-Datenschutzgrundverordnung im Gesetzgebungsverfahren?
Viviane Reding: Die Vorschläge der Europäischen Kommission liegen nun seit zwei Jahren auf dem Tisch. Zu Beginn der Beratungen standen einige Länder auf der Bremse. Seitdem in den vergangenen Monaten ein Datenskandal nach dem anderen ans Licht gekommen ist, sind die Verhandlungen in Schwung gekommen. Diese Skandale waren ein Weckruf. Daher ist es gut, dass unsere Datenschutzreform seit dem EU-Gipfel Ende Oktober zur Chefsache erklärt wurde. Dort haben sich die Staats- und Regierungschefs zu einer „raschen“ Annahme der EU-Datenschutzregeln bekannt. Ich zähle nun darauf, dass die zuständigen nationalen Minister ein starkes gemeinsames Datenschutzrecht für die EU beschließen. Noch vor den Europawahlen im Mai. Die Bürger warten darauf.

Wie sehen Sie die Rolle des Datenschutzes künftig in der digitalen Welt?
Viviane Reding: Datenschutz ist die Grundvoraussetzung dafür, dass sich die digitale Welt weiterentwickelt. Nur wenn Bürger, Unternehmen und andere Nutzer Vertrauen haben, dass ihre Daten stets wirkungsvoll geschützt sind, wird die digitale Welt – auch die digitale Wirtschaft – ihr volles Potenzial erreichen.

Persönliche Daten sind wertvoll: Nach Schätzungen der Boston Consulting Group lag der Wert der Daten von EU-Bürgern 2011 bei 315 Millionen Euro. Bis 2020 könnte er demnach bis auf knapp 1 Trillion Euro steigen. Dieses Potenzial wird die Wirtschaft nur heben können, wenn Nutzer bereit sind, Unternehmen ihre persönlichen Daten anzuvertrauen, etwa wenn sie über das Internet Produkte einkaufen.

Sollten Unternehmen nicht schon längst risikobasierte Ansätze zum Datenschutz entwickelt und implementiert haben?
Viviane Reding: Unternehmen, die mit den Daten ihrer Kunden verantwortungsvoll umgehen, haben eindeutig einen Wettbewerbsvorteil. Deshalb sind starke einheitliche EU-Datenschutzregeln auch im Interesse der europäischen Wirtschaft. Die Skandale des letzten halben Jahres zeigen bereits Wirkung. Eine Umfrage der Cloud Security Alliance ist zu dem Ergebnis gekommen, dass 56 Prozent der Teilnehmer mittlerweile zögern, wenn es darum geht, Cloud-Anbieter zu nutzen, die in den USA ansässig sind. Und der Thinktank „Information Technology and Innovation Foundation“ schätzt, dass die Enthüllungen die US-Cloud-Computing-Branche in den kommenden drei Jahren 22 bis 35 Milliarden Dollar an Umsatz kosten werden. Das birgt eine Riesenchance für unsere europäischen Unternehmen.

Wie haben Sie die Rolle der Länder und der Wirtschaft im Rahmen des bisherigen Gesetzgebungsverfahrens wahrgenommen?
Viviane Reding: Einige Mitgliedsstaaten waren zu Anfang des Gesetzgebungsverfahrens nicht besonders hilfreich. Mit der Enthüllung etlicher Ausspähaktionen vor allem durch die USA und Großbritannien hat sich das Bild aber gewandelt. Viele Politiker haben begriffen, dass die Bürger ein Recht auf hohe Datenschutzstandards haben und dieses Recht auch einfordern. Die Regierungen sind jetzt am Zug.

Auch Teile der Wirtschaft haben eine Zeit lang Sand ins Getriebe gestreut. US-Konzerne haben eine Riesenlobbykampagne in Gang gesetzt, der allerdings mittlerweile die Argumente ausgegangen sind. Der Schuss ging nach hinten los, denn zu viel Lobbyismus hat bewirkt, dass das Europaparlament die Regeln sogar noch verschärft hat.

Dabei ist unsere Reform gut für die Bürger UND die Unternehmen. Warum? Weil wir Bürokratie abbauen und Firmen das Leben erleichtern. Statt 28 nationaler Gesetze müssen Unternehmen künftig nur noch ein europaweites Gesetz einhalten. Ein Kontinent, ein Gesetz. Das spart jedes Jahr rund 2,3 Milliarden Euro. Unsere Reform ist ein Marktöffner.

Ein europäischer Datenschutz schützt aber nicht gegen möglicherweise fehlende Datenschutzregeln außereuropäischer Unternehmen.
Viviane Reding: Und ob. Unsere Reform sorgt dafür, dass sich auch nicht-europäische Unternehmen an europäische Datenschutzregeln halten müssen, wenn sie unseren mehr als 500 Millionen EU-Bürgern Produkte und Dienstleistungen anbieten. Verletzen sie die hohen europäischen Datenschutzstandards, drohen Strafen von bis

ZUR PERSON

Viviane Reding
Die Humanwissenschaftlerin studierte an der Sorbonne in Paris. Ihre berufliche Laufbahn begann sie 1978 als Journalistin beim Luxemburger Wort. Ein Jahr später zog sie als Abgeordnete in das luxemburgische Parlament ein, zehn Jahre später in das Europäische Parlament. 1999 wurde Viviane Reding Mitglied der Europäischen Kommission, zunächst zuständig für Bildung, Kultur, Jugend, Medien und Sport und ab 2004 für Informationsgesellschaft und Medien. Seit Februar 2010 ist die in Esch-sur-Alzette geborene Luxemburgerin Vizepräsidentin der Europäischen Kommission, verantwortlich für Justiz, Grundrechte und Bürgerschaft.

> UNSERE REFORM IST GUT FÜR DIE BÜRGER UND DIE UNTERNEHMEN, WEIL WIR BÜROKRATIE ABBAUEN UND FIRMEN DAS LEBEN ERLEICHTERN.

zu zwei Prozent des weltweiten Jahresumsatzes. Damit schaffen wir gleiche Bedingungen für europäische und nicht-europäische Unternehmen.

Ist die EU-Datenschutzgrundverordnung ein Blueprint für die internationale Zusammenarbeit über die EU hinaus?
Viviane Reding: Starke, einheitliche Datenschutzregeln werden es uns erlauben, auf globaler Ebene Standards zu setzen. Deshalb ist es ja auch so wichtig, dass wir diese Regeln bald bekommen. Wenn wir auf internationaler Ebene mit einer Stimme sprechen, können wir unsere hohen Standards durchsetzen. Das gilt für unser Verhältnis zu den USA, das natürlich derzeit im Blickpunkt steht, aber auch für unsere Beziehungen mit anderen Staaten.

Nur ein einheitlicher, robuster Rahmen wird es uns etwa ermöglichen, der NSA etwas entgegenzusetzen und von den USA dringend notwendige Gesetzesänderungen einzufordern, wie etwa, dass europäische Bürger in den Vereinigten Staaten das Recht bekommen, sich vor Gericht gegen den Missbrauch ihrer persönlichen Daten zu wehren. Umgekehrt können amerikanische Staatsbürger das in der EU schon heute – wie übrigens auch alle anderen Menschen, die hier leben.

Die Verordnung ist ein wichtiger Baustein, um europäische Bürger vor willkürlicher Überwachung und Spionage durch Drittstaaten zu schützen. Welche weiteren Maßnahmen sollten ergriffen werden?
Viviane Reding: Es ist wichtig, dass wir unterscheiden zwischen Regeln für die Arbeit von Geheimdiensten und Regeln zur Wahrung des Datenschutzes. Es sollte niemanden überraschen, dass Geheimdienste im Geheimen handeln. Doch wenn ein Geheimdienst auf dem Territorium eines Mitgliedsstaats operiert, dann sollten die jeweiligen Regierungen sicherstellen, dass die nationalen Regeln eingehalten werden.

Es gibt Dinge, die nicht mit dem Kampf gegen den Terrorismus begründet werden können. Staaten genießen kein unbeschränktes Recht auf geheime Überwachung. Vielmehr gilt es, das richtige Gleichgewicht zu finden zwischen der Bekämpfung des Terrorismus und dem Schutz der persönlichen Daten: Sicherheit und Freiheit sind zwei Seiten einer Medaille. Das ist eine Frage der Verhältnismäßigkeit.

Was die Regeln zur Sicherung des Datenschutzes angeht, da wird unsere Verordnung sicherstellen, dass ausländische Geheimdienste nicht mehr einfach so Daten von Konzernen einfordern oder gar ohne deren Wissen abzapfen können. Das gewährleisten wir dadurch, dass sich jedes in Europa tätige Unternehmen auch an europäische Regeln halten muss. Außerdem sorgen wir für Rechtssicherheit beim Datenverkehr: Daten von EU-Bürgern dürfen nur in genau definierten Ausnahmesituationen und unter gerichtlicher Kontrolle an Strafverfolgungsbehörden außerhalb Europas weitergegeben werden. Es muss dabei einen effektiven Rechtsschutz vor uneingeschränkter internationaler Datenübertragung geben.

Bei Safe Harbor ist bekannt, dass Regelungen nicht konsequent umgesetzt und Zuwiderhandlungen nicht sanktioniert werden. Was wird die Kommission dazu unternehmen?
Viviane Reding: Auf Selbstregulierung und Verhaltenskodizes, die nicht streng kontrolliert werden, wollen wir uns beim Datenschutz nicht mehr verlassen. Angesichts der Enthüllungen der vergangenen Monate hat die Kommission Safe Harbour genau unter die Lupe genommen. Und wir sind zu dem Schluss gekommen, dass die Daten europäischer Bürger, die von amerikanischen Unternehmen unter Safe Harbour in die USA übermittelt werden, in der Tat nicht immer sicher vor Missbrauch sind. Es kommt durchaus vor, dass US-Behörden auf diese Daten zugreifen und sie auf eine Weise nutzen, die nicht mit den Grundlagen von Safe Harbor vereinbar sind. Wir haben Ende November 13 Empfehlungen an die USA gerichtet, um den „Sicheren Hafen“ sicherer zu machen. Jetzt sind die USA am Zug.

DREIKLANG VON FREIHEIT, SICHERHEIT UND WIRTSCHAFT

Von **Dr. Klaus Kinkel**
Bundesminister des Auswärtigen a. D. und Vorsitzender Deutsche Telekom Stiftung

ZUR PERSON

Dr. Klaus Kinkel
Nach Abschluss seines Studiums der Rechtswissenschaften an den Universitäten Tübingen, Bonn und Köln und Promotion zum Dr. jur. begann Dr. Klaus Kinkel 1965 seine Beamtenlaufbahn im Bundesinnenministerium und wechselte 1974 ins Auswärtige Amt. Dort führte er zunächst den Leitungsstab, später den Planungsstab. Von 1979 bis 1982 war er Präsident des Bundesnachrichtendienstes, danach Staatssekretär im Bundesministerium der Justiz, anschließend von 1990 bis 1992 Bundesjustizminister. Von Mai 1992 bis Oktober 1998 war Dr. Klaus Kinkel Bundesminister des Auswärtigen, 1993 bis 1998 zugleich Vizekanzler der Bundesrepublik Deutschland.

Die Digitalisierung unserer Gesellschaft bietet uns einzigartige Chancen. Internationale Zusammenarbeit erreicht durch globalisierte Kommunikation in Echtzeit eine neue Dimension. Neue Formen wirtschaftlicher Zusammenarbeit und Entwicklung sowie des politischen wie privaten Austauschs sind möglich. Die Kehrseite der digitalen Revolution sind jedoch neue Risiken: Das Ausspionieren von Wirtschaftsunternehmen ist bei geringem Risiko und hohen Gewinnen möglich. Weder einzelne Bürger noch Regierungen sind vor Spionage und Überwachung sicher. Kritische Infrastrukturen werden aufgrund zunehmender Vernetzung anfälliger für Cyberangriffe – sei es durch zivile oder militärische Hacker.

Es ist dringlich für die internationale Politik wie für die Wirtschaft, die Herausforderung Cybersicherheit anzugehen. Eine der wichtigsten Aufgaben von Cyberaußenpolitik lautet daher, globale Voraussetzungen für einen sicheren und stabilen Cyberraum zu gewährleisten. Die entscheidende Gestaltungsaufgabe besteht vor allem darin, vorhandene Regeln auf die digitale Welt zu übertragen und wo notwendig neue Regeln zu schaffen.

IMMENSE POTENZIALE NUTZEN, RISIKEN MINDERN

Wie bei jeder Innovation ist es wichtig, eine nüchterne Analyse der Chancen und der Risiken vorzunehmen. Auf der Grundlage der Ergebnisse dieser Analyse muss deutsche Außenpolitik für den Cyberraum dazu beitragen, dessen immensen Potenziale zu nutzen und zu mehren, zugleich aber die erheblichen Risikofaktoren zu mindern. Konkret geht es um einen Dreiklang von Interessen, die in ein Gleichgewicht gebracht werden müssen: Cyberaußenpolitik muss die Freiheit und die freiheitsstiftenden Wirkungen des Internets verantwortungsvoll schützen und nutzen. Sie muss seine wirtschaftlichen Chancen ausbauen. Und sie muss die Sicherheit des Cyberraums sicherstellen – soweit das geht.

Hinsichtlich der wirtschaftlichen Dimension steht deutsche Cyberaußenpolitik vor einer doppelten Herausforderung: Sie muss die Chancen des Internets und neuer Informations- und Kommunikationstechnologien für die deutsche Wirtschaft im Blick haben. Und sie sollte deren Einsatz als Motor globaler Entwicklung berücksichtigen. Die deutsche Außenpolitik kann durch den Einsatz für offene und faire Wettbewerbsbedingungen, eine offene Visapolitik, die Beteiligung an internationalen Forschungsprogrammen und Instrumente der Außenwirtschaftsförderung zum Erfolg der deutschen IT-Industrie beitragen.

ÜBERWACHUNGSTECHNOLOGIEN KÖNNEN DIE FREIHEIT GEFÄHRDEN

Staaten sollten auf die Gefahr eines Cyberangriffs nicht ihrerseits mit einer offensiven Cybersicherheitspolitik reagieren. Wer Sicherheit im Cyberraum durch Abschreckung und Vergeltung herstellen möchte, trifft mit seiner Reaktion möglicherweise den Falschen. Zudem kann die stete Suche nach Angreifern leicht zu einem flächendeckenden Einsatz von Überwachungs- und Kontrolltechnologien im Internet führen und seine Freiheit gefährden.

Demgegenüber setzt eine defensiv ausgerichtete Cybersicherheitsstrategie, wie sie die Bundesregierung und die EU verfolgen, auf Konfliktvermeidung und Stabilität. Sie steht auf zwei Säulen: Zum einen soll mit dem Einsatz von Hochsicherheits-IT die Widerstandsfähigkeit unserer Netze so weit erhöht werden, dass sie auch technologisch anspruchsvollen Angriffen standhalten. Zum anderen initiiert und unterstützt die Bundesregierung internationale Übereinkommen, die im Sinne präventiver Rüstungskontrolle zur Schaffung eines regelbasierten Cyberraums beitragen. Dazu zählen Vereinbarungen über vertrauens- und sicherheitsbildende Maßnahmen, Übereinkommen zur Festlegung internationaler Standards bei der Zulassung von Hard- und Software, Normen verantwortlichen staatlichen Handelns und eine Verständigung bei der Übertragung völkerrechtlicher Regeln auf den Cyberraum.

STAAT, UNTERNEHMEN UND ZIVILGESELLSCHAFT MÜSSEN ZUSAMMENARBEITEN

Wenn wir den Dreiklang von Freiheit, Sicherheit und Wirtschaft in der Cyberaußenpolitik betrachten, geht es um eine Vernetzung dieser Politikbereiche ebenso wie um eine Vernetzung der betroffenen Akteure. Staat, Unternehmen und Zivilgesellschaft müssen zusammenarbeiten, nationale und internationale Maßnahmen miteinander verbunden werden. Nur so können wir Deutschland vor Beeinträchtigungen durch Cyberangriffe schützen und auf ein freies, offenes, stabiles und sicheres Internet hinwirken.

Die Enthüllungen von Edward Snowden haben die Frage nach Datenschutz, Privatsphäre und Sicherheit von Informationen in den Mittelpunkt der Debatte zur Cyberaußenpolitik gerückt. Dabei geht es um Vertrauen, das engste Partner einander entgegenbringen müssen und nicht brechen dürfen. Es geht aber auch um den verantwortungsvollen Umgang mit neuen Technologien: Nicht alles, was für eine Regierung technisch möglich ist, ist ethisch richtig oder politisch klug. Wir brauchen auch in der Cyberaußenpolitik verlässliche Prinzipien, die Werte und Interessen in Einklang bringen. Wir müssen jedoch bei allen Veränderungen eins beachten: Eine zu starke nationalstaatliche Kontrolle des Internets als Antwort auf die NSA-Aktivitäten wäre kein Fortschritt. Eine Fragmentierung des Internets schwächt seine wirtschaftliche Dynamik und spielt autoritären Regimen in die Hände, denen der offene Charakter des Netzes ohnehin ein Dorn im Auge ist. Gleichwohl müssen wir auch über ein Internet der kurzen Wege nachdenken. Lokale Datenströme müssen keine globalen Umwege nehmen.

„IT-SECURITY MADE IN GERMANY“ ALS INTERNATIONALE MARKE AUFBAUEN

Aus meiner Sicht haben daher folgende Maßnahmen Priorität:
Erstens zählen dazu zeitgemäße, dem Zeitalter der Digitalisierung angepasste Vereinbarungen zum Datenschutz. Dafür setzt sich Deutschland gegenwärtig im EU- wie auch im Rahmen der Vereinten Nationen intensiv ein.
Zweitens müssen wir intensive Gespräche mit unseren europäischen Partnern führen. Wir brauchen eine ambitionierte IT-Strategie auf europäischer Ebene, die Europa nicht zuletzt bei Technologien der Datenspeicherung und -verarbeitung unabhängig von chinesischen und amerikanischen Anbietern macht und in die Lage versetzt, auf dem Weltmarkt konkurrenzfähig zu sein.
Drittens gehören dazu Verhandlungen mit den USA. Dabei muss es um die wechselseitige Verpflichtung der USA und der EU gehen, auf politische und Wirtschaftsspionage gegeneinander zu verzichten und die massenhafte Erfassung von Daten europäischer Bürger zu beenden.
Viertens müssen wir die Gespräche zur Internet-Governance mit neuen Gestaltungsmächten wie Indien oder Brasilien ausbauen. Dies bedeutet: Wir müssen eine einseitige Dominanz durch bestimmte Staaten oder Gesellschaften überwinden.
Fünftens zählt dazu eine enge Verständigung zwischen Politik und Wirtschaft zur Sicherheitstechnik. „IT-Security made in Germany“ kann und sollte zu einer Marke mit internationaler Strahlkraft werden.

ZURÜCK ZUM EIGENTLICHEN ZWECK DES DATENSCHUTZES

US-Datenschützer **Martin Abrams** engagiert sich für einen Umgang mit Daten, in dessen Zentrum das Prinzip der Rechenschaft steht: Erst wenn Daten verarbeitende Organisationen voll auskunftspflichtig sind, kann der Datenschutz informationsgetriebene Innovationen fördern und gleichzeitig die Würde des Einzelnen wahren. Darüber hinaus könnte es dann auch möglich sein, eine Interoperabilität zwischen den USA und der Europäischen Union zu erreichen.

Sie kennen sich mit dem Zugang zum Datenschutz auf beiden Seiten des Atlantiks aus. Viele Europäer meinen, dass die Blickrichtung der Amerikaner von der europäischen Sichtweise stark abweicht. Teilen Sie diese Ansicht?

Martin Abrams: Ich sehe einige grundsätzliche Unterschiede, aber auch eine Reihe wichtiger Gemeinsamkeiten. Der größte Unterschied liegt in unserem Verständnis, wo das Gleichgewicht zwischen Datenschutz und freier Meinungsäußerung liegen sollte. In den USA wird das Recht auf freie Meinungsäußerung vom 1. Zusatzartikel der amerikanischen Verfassung garantiert. Die Gründerväter der USA sprachen sich dafür aus, dass der Schutz der freien Meinungsäußerung vor anderen Schutzrechten Vorrang hat. Der Schutz ist daher unglaublich stark. Zur freien Meinungsäußerung gehören etliche Komponenten. Das beginnt mit dem Recht, Verhalten zu beobachten und aufzuzeichnen. In den meisten Fällen ist dieses Recht somit unmittelbar von der Verfassung geschützt.

Wann stößt die Fähigkeit, Verhalten zu beobachten und festzuhalten, auf Grenzen?

Martin Abrams: Solange Sie in der Öffentlichkeit agieren, steht es mir frei, Sie zu beobachten. Dieser öffentliche Bereich schließt den Vorgarten Ihres Hauses und sogar den Hinterhof mit ein, wenn ich ihn beim Überfliegen in Augenschein nehme. Ohne Einladung durch ein Fenster in Ihr Haus zu blicken, ist mir jedoch nicht erlaubt. Es kommt also darauf an, was den öffentlichen Raum einschließt, den man beobachten darf. Das Justizsystem der USA hat Grenzen gesetzt, was wir hier an Privatsphäre erwarten können: Sobald wir unsere Daten mit Dritten tauschen, unterliegen sie nicht mehr dem Schutz der Privatsphäre.

Die amerikanische Verfassung garantiert den Schutz der freien Meinungsäußerung. Das beginnt mit dem Recht, Verhalten zu beobachten und aufzuzeichnen.

Trotz dieser Rechtstradition diskutieren mehr und mehr Amerikaner die Notwendigkeit, die Grenzen der Öffentlichkeit im digitalen Raum enger zu ziehen. Diesen Trend erkennt man an Initiativen wie Do Not Track, welche die Fähigkeit einschränken wollen, das Surfverhalten von Internetnutzern online zu verfolgen.

In Europa brauchen Organisationen eine Rechtsgrundlage, wenn sie Beobachtungen durchführen und digital verarbeiten wollen. Halten Sie diese Verpflichtung für den zentralen Unterschied zwischen beiden Rechtsräumen?

Martin Abrams: Im Zeitalter von Big Data fällt dieser Unterschied sicherlich sehr stark ins Gewicht. Er ist dennoch nicht der einzige. Zusätzlich müssen wir auch die Ebene der Analyse betrachten. In den USA steht es mir frei, Daten zu erforschen. Die Verarbeitung von Beobachtungsdaten wird ebenfalls vom 1. Zusatzartikel der Verfassung garantiert. Hierbei umfasst das Recht auf freie Meinungsäußerung sowohl die Reflexion als auch die Manipulation von Daten. Dieses Verfassungsrecht steht in völligem Gegensatz zur Rechtslage in Europa. Wenn Europäer Daten verwenden wollen, um neue Einsichten zu gewinnen, müssen sie darlegen, dass die Daten mit einem legitimen Forschungszweck übereinstimmen. Außerdem müssen sie feststellen, ob es

ZUR PERSON

Martin Abrams arbeitet als Exekutiv Director und Chefstratege für die Information Accountability Foundation. Zuvor war er Präsident des Center for Information Policy Leadership und Vizepräsident Information Policy bei Experian.

INFORMATION ACCOUNTABILITY FOUNDATION

Unternehmensmitglieder des Global Accountability Project gründeten im Jahr 2012 die Information Accountability Foundation. Ziel der Stiftung ist es, das Prinzip der Rechenschaft in der Unternehmenspraxis, der regulatorischen Aufsicht und der nächsten Generation des Datenschutzrechts zu etablieren. Gemeinsam mit Regierungen, Aufsichtsbehörden, Wirtschaft und Zivilgesellschaft will die Stiftung eine auf das Prinzip der Rechenschaft gestützte Datenführung fördern. Weitere Informationen unter: **http://informationaccountability.org/**

eine entsprechende Rechtsgrundlage gibt, bevor sie mit der Forschung beginnen.

Somit scheint die Lage sehr gespalten. Ungeachtet dessen haben Sie bereits erwähnt, dass es auch Gemeinsamkeiten gibt. Wo beginnen diese?

Martin Abrams: Die Gemeinsamkeiten zwischen dem europäischen und dem amerikanischen System kommen zum Tragen, wenn es um die Nutzung der Daten geht. In den USA darf ich keine Daten für etwas verwenden, was rechtlich ausgeschlossen oder mit dem von mir angegebenen Forschungszweck unvereinbar ist. Ich nenne Ihnen ein Beispiel. Wenn ich Beobachtungsdaten verarbeite und feststelle, dass Frauen zwischen 25 und 35 Jahren ein höheres Kreditrisiko darstellen, darf ich dieses Wissen nicht nutzen. Laut US-Gesetz darf ich keine Entscheidung treffen, die auf Geschlecht oder Lebensalter beruht. Die Einsicht mag ich gewonnen haben, aber ich darf sie nicht anwenden. Somit beginnen die gemeinsamen Interessen zwischen Europa und den Vereinigten Staaten bei der Verwendung der Daten.

Welche Rolle spielt in diesem Zusammenhang das Safe-Harbor-Programm?

Martin Abrams: Perfekt ist es nicht, doch hat das Programm Millionen Europäern echten Schutz gewährt. Denn Safe Harbor ist ein Selbstzertifizierungsprogramm mit Biss. Ein Unternehmensverantwortlicher muss die Integrität des Programms persönlich zertifizieren und darf nach dem False Statements Act strafrechtlich verfolgt werden, wenn seine Dokumente nicht mit den Policies und Umsetzungsprogrammen übereinstimmen. Ohne Safe Harbor fände ein Großteil des Datenverkehrs zwischen Europa und den USA im rechtsfreien Raum statt. Trotz all seiner Schwächen sollte man daher anerkennen, dass Safe Harbor ein wirksames Datenschutzwerkzeug ist.

Martin Abrams: „Ohne Safe Harbor fände ein Großteil des Datenverkehrs zwischen Europa und den USA im rechtsfreien Raum statt."

Sind die Schwächen überwindbar?

Martin Abrams: Die EU-Kommission hat eine Reihe guter Verbesserungsvorschläge gemacht. Beispielsweise regt sie an, dass das US-Department of Commerce seine Kontrollen in Unternehmen ausweitet, die eine Safe-Harbor-Listung beantragen. Zudem schlägt die Kommission Untersuchungen durch die US-Kartellbehörde Federal Trade Commission und die europäischen Datenschutzbehörden vor. Dies sind ausgezeichnete Vorschläge. Doch setzen sie einen entsprechenden Etat voraus. Zurzeit sind die Gebühren für Safe-Harbor-Einträge und -Verlängerungen noch relativ gering. Aus meiner Sicht sollten sie angemessen erhöht werden, um eine wirksame Aufsicht zu finanzieren.

In Ihrem Blog führen Sie Safe Harbor als frühes Beispiel dafür an, wie sich eine Datenschutzbestimmung an den Grundsätzen der Rechenschaft orientieren sollte. Weshalb fällt dem Programm eine solche Vorreiterfunktion zu?

Martin Abrams: Safe Harbor hat die Grundsätze der Rechenschaft umgesetzt, bevor diese überhaupt veröffentlicht wurden. Sieben Grundsätze sind dabei besonders wichtig. Erstens muss eine Organisation interne Ziele verfolgen, die an die Grundsätze einer externen Datenschutzbestimmung anknüpfen. Zweitens soll sie sich öffentlich dazu bekennen, diese Grundsätze einzuhalten. Drittens braucht sie Mechanismen, um die Policies umzusetzen. Viertens soll die Organisation die Einhaltung der Policies überwachen. Fünftens soll sie sicherstellen, dass Verbraucher ihre Rechte ausüben können. Sechstens soll sie einen rechenschaftspflichtigen Verantwortlichen benennen und siebtens zumindest einer Aufsichtsbehörde unterstehen. All diese Erfordernisse entsprechen den Grundsätzen der Rechenschaft, die jeder Big-Data-Akteur unbedingt einhalten sollte.

Warum ist es so wichtig, diese Grundsätze anzuwenden?

Martin Abrams: Derzeit geht es in zu vielen Datenschutzprogrammen darum, bürokratische Aufgaben zu erledigen, also zum Beispiel Forschungszwecke zu formulieren oder Präferenzen zu verwalten. Bei vielen Aufsichtsbehörden sehen wir einen ähnlichen Trend. Dort findet man es einfacher, die Einhaltung einer Bestimmung rein technisch zu messen als sicherzustellen, dass der wahre Zweck des Datenschutzes erfüllt wird. Angesichts dieser Entwicklung sprechen wir uns für eine Rückbesinnung auf den eigentlichen Zweck des Datenschutzes aus. Dieser liegt darin, den Schutz der Menschenwürde zu gewährleisten und die Privatsphäre vor Schäden zu schützen, deren Potenzial permanent zunimmt. Unser digitales Zeitalter benötigt einen Datenschutz, in dessen Rahmen die verantwortlichen Organisationen rechenschaftspflichtig sind – entweder jedem Einzelnen oder den Aufsichtsbehörden gegenüber. Rechenschaft bedeutet, dass sich Organisationen zur Sammlung und Verwendung von Daten bekennen sowie gleichzeitig die Risiken, die sie für den Einzelnen schaffen, verstehen und mildern. Darüber hinaus sollten rechenschaftspflichtige Organisationen den Aufsichtsbehörden offenlegen, wie sie mit den Daten umgehen. Auf diese Weise erhalten Big-Data-Anwender einen Mechanismus, um Daten innovativ zu nutzen und den Schutz des Individuums zu wahren.

AUF UNSERE WERTE BESINNEN

Zunehmende Cyberkriminalität und massive Bespitzelung durch Geheimdienste haben Bürger und Unternehmen stark verunsichert. Doch bei aller berechtigten Angst vor den Risiken dürfen wir die Chancen der digitalen Welt nicht aus den Augen verlieren, sagt Wolfgang Kopf, Leiter Politik und Regulierung bei der Deutschen Telekom.

Die Verwundbarkeit der digitalen Gesellschaft ist spätestens im Jahr 2013 deutlich geworden. So sind nicht nur die Gefahren durch Cyberkriminelle massiv gestiegen, sondern die von Edward Snowden aufgedeckten Geheimdienstaktivitäten haben eine bis dato für unmöglich gehaltene Dimension der Bespitzelung von Einzelpersonen, Wirtschaft und Politik aufgedeckt.

Die Erosion des Vertrauens in die digitale Gesellschaft, ihre Produkte und Dienstleistungen wiegt schwer. Wir müssen uns fragen, ob wir den Bedrohungen aktuell genug entgegensetzen. Vor diesem Hintergrund sind Transparenz und Aufklärung, ein verlässlicher Rechtsrahmen sowie die Entwicklung neuer, einfacher Sicherheitslösungen Voraussetzungen, das Vertrauen der Menschen wiederzugewinnen. Wir müssen Antworten formulieren, wie wir uns gegen Cyberkriminalität und Überwachung zur Wehr setzen können. Nur der informierte Nutzer digitaler Dienste und Produkte kann adäquat reagieren und sich schützen.

SICHERHEIT „MADE IN GERMANY“

In der skizzierten Bedrohung steckt aber auch die Chance für den Standort Deutschland und die gesamte Europäische Union. Datenschutz und Datensicherheit entwickeln sich zu einem wichtigen Differenzierungsmerkmal, Wettbewerbsvorteil und zusätzlichen Verkaufsargument für Unternehmen. Deutschland ist hier sehr gut positioniert. Unsere hohen Datenschutz- und Datensicherheitsstandards entwickeln sich – für viele überraschend – zu einem wertvollen Standortfaktor. Das haben bisher nicht alle Unternehmen so gesehen. Für viele stellten Datenschützer und Sicherheitsbehörden bisher eher die „Verhinderer“ dar, die den Unternehmen im globalen Wettbewerb Steine in den Weg gelegt haben.

Die Entwicklungen der vergangenen Monate sind durchaus ermutigend. Zahlreiche Initiativen in Politik und Wirtschaft befassen sich damit, wie wir uns noch besser gegen die Risiken schützen können und gleichzeitig die Standortvorteile durch Datensicherheits- und Datenschutzkompetenz ausbauen können. Tatsächlich sollten wir die Chance nutzen und „Sicherheit Made in Germany“ zu einer Marke entwickeln. Wo sich deutsche Unternehmen mit ihren Sicherheitsprodukten und -dienstleistungen bisher schwertaten, ist das Interesse gestiegen – insbesondere auch bei ausländischen Unternehmen, die dem Standort Deutschland großes Vertrauen entgegenbringen.

SCHUTZ EUROPÄISCHER BÜRGER

Die Deutsche Telekom entwickelt Lösungen, die mehr Schutz vor dem unbefugten Zugriff auf unsere Daten bieten. Gleichzeitig benötigen wir aber auch gesetzliche Regelungen, die den Schutz europäischer Bürger erhöhen. Hierfür haben wir zum Beispiel den Vorschlag für ein Internet der kurzen Wege, das „Schengen-Routing“ unterbreitet. Wenn sich Sender und Empfänger innerhalb

Sicherheit „Made in Germany“ könnte sich zu einer Qualitätsmarke entwickeln.

des Schengen-Raums befinden, sollte gesetzlich vorgeschrieben werden, dass Daten nicht unnötig über Amerika oder Asien geroutet werden dürfen. In Amerika wird dies längst so gehandhabt. Wenn wir zumindest die Daten schützen, die den eigenen Rechtsraum nicht zwingend verlassen müssen, bedeutet das schon ein Mehr an Sicherheit.

Schon die ersten Gespräche zu No-Spy-Abkommen, Kooperationen in der Cybersicherheitspolitik oder beim grenzüberschreitenden Datenschutz zeigen, wie schwierig es derzeit ist, zu international einvernehmlichen Lösungen zu kommen. Zu unterschiedlich und unvereinbar scheinen die divergierenden Interessen zwischen dem Ziel einer vermeintlich absoluten Sicherheit durch Überwachung und dem Recht auf Privatsphäre und informationelle Selbstbestimmung.

SAFE HARBOR KÜNDIGEN

Europa hat ein anderes Verständnis, wenn es um die Abwägung zwischen Freiheit und Sicherheit seiner Bürger geht. Gleichzeitig hat Europa schon heute das höchste Datenschutzniveau weltweit. Viele dieser Regeln haben in Deutschland ihren Ursprung. Um seine Bürger effektiv zu schützen, müssen diese Regeln auch konsequent umgesetzt werden. Mehrere Studien der EU-Kommission haben gezeigt, dass das Safe-Harbor-Abkommen mit den USA keinen effektiven Schutz europäischer Bürger gewährleistet. Safe Harbor muss deshalb konsequenterweise sofort gekündigt werden.

Auch wenn dieser Schritt vorübergehend zu Spannungen führen kann, so ist er der einzige Weg, eine neue transatlantische Ordnung für Cybersicherheit und Datenschutz zu schaffen. Nur so wird es Europa gelingen, auf Augenhöhe zu verhandeln und damit die Interessen seiner Bürger zu schützen.

ZUR PERSON

Wolfgang Kopf, LL.M. ist seit November 2006 Leiter des Zentralbereichs Politik und Regulierung der Deutschen Telekom. Sein Verantwortungsbereich umfasst neben der nationalen und internationalen politischen Interessenvertretung, Kartellrecht, 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.

DATENSCHUTZ NACH DEM NEED-TO-KNOW-PRINZIP

Für die Deutsche Telekom steht der Datenschutz ganz oben auf der Agenda. Daher verfügt der Konzern als eines der wenigen deutschen Dax-Unternehmen über ein eigenes Vorstandsressort für Datenschutz, Recht und Compliance. Wie verfährt die Telekom mit den Kundendaten? Die wichtigsten Aspekte im Überblick.

Welche Kundendaten speichert und verarbeitet die Deutsche Telekom und zu welchem Zweck?
Bei der Sprachtelefonie werden Vertrags- und Verkehrsdaten gespeichert und verarbeitet. Die Vertragsdaten dienen dazu, die Vertragsverhältnisse zu begründen und die Kundenbeziehung zu pflegen. Hierzu zählen beispielsweise Daten wie Name, Anschrift sowie Informationen über die genutzten Produkte, Dienste und Tarife von Kunden. Mithilfe von Verkehrsdaten werden Telekommunikationsverbindungen hergestellt und gesteuert. Sie werden zur Erzeugung von Rechnungen verarbeitet und zum Leistungsnachweis gespeichert. Auf Wunsch wird daraus ein Einzelverbindungsnachweis für den Kunden erstellt. Details über die Erhebung und Verarbeitung von Kundendaten finden sich in den jeweiligen Datenschutzbestimmungen zu den gewählten Produkten.

Wer muss auf die gespeicherten Daten zugreifen können?
Zur Kundenbetreuung müssen der Kundenservice und die technischen Betriebskräfte auf die gespeicherten Daten zugreifen können, wenn dies für die Bearbeitung erforderlich ist. Der Kundenservice muss auf Kundendaten zugreifen können, um etwa Kundenanfragen zu Rechnungen zu bearbeiten. Technische Betriebskräfte benötigen zur Störungsbeseitigung Zugriff auf Verkehrsdaten. Für andere Zugriffe bedarf es einer expliziten Einwilligung des Kunden oder einer besonderen gesetzlichen Erlaubnis.

Kann der Kunde Auskunft über seine gespeicherten Daten erhalten?
Jeder Betroffene kann nach § 34 des Bundesdatenschutzgesetzes Auskunft verlangen, welche Daten über ihn bei der Deutschen Telekom gespeichert sind. Diesen Auskunftsanspruch hat aber nur der Betroffene höchstpersönlich, also nicht zum Beispiel dessen Ehepartner

Speichert die Deutsche Telekom Vorratsdaten?
Seit der Entscheidung des Bundesverfassungsgerichtes vom 2. März 2010 speichert die Telekom keine Vorratsdaten mehr. Alle bis dahin gespeicherten Vorratsdaten haben wir aufgrund des vom Bundesverfassungsgericht für nichtig erklärten, gesetzlichen Bestimmungen unverzüglich gelöscht.

Was tut die Deutsche Telekom, um Kundendaten bestmöglich zu schützen?
Die Deutsche Telekom hat umfassende interne Regelungen und Maßnahmen getroffen, um Kundendaten bestmöglich zu schützen. Für die Daten verarbeitenden Systeme werden detaillierte Konzepte erstellt, die den Datenschutz, Berechtigungen und die Datensicherheit dokumentieren. Voraussetzung für die Inbetriebnahme eines Systems ist die Bestätigung der Einhaltung der Datenschutz- und Sicherheitsbestimmungen. Erst bei Vorliegen der geforderten Konzepte und einer entsprechenden Freigabe darf im Rahmen der dort definierten Festlegungen mit Kundendaten umgegangen werden. Generell gilt beim Umgang mit Kundendaten ein striktes „Need-to-know"-Prinzip.

Welche Schutzmechanismen gibt es für die gesetzlich vorgeschriebenen Kontaktpunkte für Ermittlungsbehörden?
Als Ansprechpartner für die Ermittlungsbehörden stehen bei der Deutschen Telekom sogenannte „Regionalstellen für Staatliche Auflagen" zur Verfügung. Hier arbeiten besonders qualifizierte und in Datenschutzfragen speziell geschulte Mitarbeiter. Ihr Handeln wird protokolliert und dokumentiert und von der Bundesnetzagentur auf die Einhaltung der gesetzlichen Bestimmungen und Erfüllung der rechtlichen Voraussetzungen überwacht.

Wer überprüft die Sicherheit der Kundendaten und die Einhaltung der Regelungen?
Unter anderem überprüfen die zuständigen Aufsichtsbehörden, also der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die zuständigen Landesbehörden sowie die Bundesnetzagentur, regelmäßig die Einhaltung der Datenschutzanforderungen. Spezifische Systeme, zum Beispiel zur Missbrauchsverhinderung, wurden den Datenschutzbehörden vorgelegt. Weiterhin werden die IT-Sicherheitsvorkehrungen regelmäßig durch interne Überprüfungen sowie von Wirtschaftsprüfern testiert. Die Deutsche Telekom führt jährlich ein konzernweit einheitliches Datenschutzaudit bei den Mitarbeitern durch. Es enthält Fragen zur Umsetzung des personellen, technischen und organisatorischen Datenschutzes.

110 UND 112 – FUNKZELLENÜBERMITTLUNG BEI MOBILEN NOTRUFEN

Seit Dezember 2012 erhalten Feuerwehr und Polizei automatisch die Funkzellendaten der Mobiltelefone, von denen Notrufe an sie abgesetzt werden. Das hierzu erforderliche technische Verfahren wurde unter Federführung der Telekom entwickelt und in allen deutschen Mobilfunknetzen eingeführt.

Bei Notrufen mit dem Handy muss die Deutsche Telekom Standortdaten der Funkzelle übermitteln.

Feuerwehr oder Polizei kommen und helfen mir – im Grundsatz können sich Notrufende darauf verlassen. In der Praxis müssen die Leitstellen allerdings wissen, wohin sie die Rettungskräfte schicken sollen. Doch nicht jeder Notrufende weiß, wo er sich gerade befindet, wenn er denn überhaupt noch sprechen kann. Um im Falle eines Falles unverzüglich für Klarheit zu sorgen, sind alle Mobilfunknetzbetreiber in Deutschland dazu verpflichtet, den zuständigen Rettungsdiensten die Funkzellendaten der Notrufenden automatisch mitzuliefern. Rechtsgrundlage ist § 108 des Telekommunikationsgesetzes, der in der Notrufverordnung konkretisiert wird. Um die Verordnung in die Praxis umzusetzen, hat die Bundesnetzagentur im Juni 2011 die Technische Richtlinie Notruf erlassen. An deren Ausgestaltung nahmen alle in Deutschland aktiven Mobilfunknetzbetreiber teil: In enger Abstimmung mit der Deutschen Telekom, E-Plus, Telefónica und Vodafone legte die Bundesnetzagentur verbindlich fest, wie ein Notruf aus einem Mobilfunknetz zu den Festnetzanschlüssen von Feuerwehr und Polizei zu übertragen ist.

Da jeder Netzbetreiber seine Funkzellen unternehmensspezifisch kennzeichnet, galt es vier Formate in das einheitliche Rettungsstellenformat zu übertragen. Den erforderlichen Übersetzungsdienst übernimmt die Telekom. In der Praxis erhält sie in ihrem Mobilfunknetz die mobilen Notrufe aus allen vier Mobilfunknetzen, bereitet deren Funkzellenkennung leitstellenkonform auf, wandelt anschließend die Daten festnetzkonform um und stellt die Notrufe dann über ihr Festnetz der Polizei und den Rettungsdiensten zu. Bei Notrufen aus ihrem eigenen Mobilfunknetz liefert die Telekom auch automatisch Informationen mit, die den Versorgungsbereich der Funkzelle erkennen lassen. In allen übrigen Fällen nutzen die Leitstellen die übermittelten Funkzellenkennungen, um den Versorgungsbereich in Onlinedatenbanken von E-Plus, Telefónica und Vodafone zu ermitteln.

KLARE SPIELREGELN FÜR AUSLÄNDISCHE SICHERHEITSBEHÖRDEN

Für den Fall, dass ausländische Sicherheitsbehörden Daten aus Deutschland benötigen, gibt es klare Spielregeln: Die Behörden müssen sich mit einem Rechtshilfeersuchen an eine deutsche Behörde wenden. Diese prüft dann die Zulässigkeit der Anordnung nach deutschem Recht, insbesondere das Vorliegen einer Rechtsgrundlage. Anschließend stellt die deutsche Behörde das Ersuchen der Telekom zu. Sind die rechtlichen Voraussetzungen erfüllt, teilt die Telekom der deutschen Behörde die angeordneten Daten verpflichtungsgemäß mit.

VERKEHRSDATEN FÜR DEUTSCHE SICHERHEITSBEHÖRDEN

Da es in Deutschland derzeit keine gesetzliche Regelung zur Vorratsdatenspeicherung gibt, speichert die Telekom keine Verkehrsdaten speziell für Behördenanfragen. Grundsätzlich dürfen deutsche Sicherheitsbehörden aber diejenigen Verkehrsdaten abfragen, die das Unternehmen für seine Geschäftsabläufe benötigt und deswegen vorhält. Für solche Abfragen ist grundsätzlich ein richterlicher Beschluss nötig. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft erfolgen, bedarf dann aber einer richterlichen Bestätigung. Auskunft über Kundenbestandsdaten erhalten die berechtigten Stellen – bei Vorliegen der rechtlichen Voraussetzungen – entweder automatisiert über die Bundesnetzagentur oder auf Anfrage beim jeweiligen Telekommunikationsunternehmen. Maßnahmen der Telekommunikationsüberwachung, also die Ausleitung von Telekommunikationsinhalten an eine berechtigte Stelle, können im Rahmen der Strafverfolgung oder der Gefahrenabwehr stattfinden und bedürfen im Regelfall eines richterlichen Beschlusses. Die Telekommunikationsüberwachung durch Verfassungsschutzbehörden, den Militärischen Abschirmdienst und den Bundesnachrichtendienst (BND) unterliegt besonderen rechtlichen Restriktionen: Nach dem Artikel-10-Gesetz sind diese Behörden unter engen Voraussetzungen befugt, Überwachungsmaßnahmen zu beantragen. Der BND kann nach dem Gesetz bis zu 20 Prozent der Daten überwachen. Diese Berechtigung bezieht sich jedoch nur auf Auslandsverkehr. Konkrete Maßnahmen der „Strategischen Fernmeldeüberwachung“ werden durch die sogenannte G-10-Kommission angeordnet und beaufsichtigt. Zusätzlich gibt es ein parlamentarisches Kontrollgremium der Nachrichtendienste.

WELTWEIT EINHEITLICHE DATENSCHUTZRICHTLINIEN

Die Telekom hat neue bindende Datenschutzrichtlinien für alle Tochtergesellschaften des Konzerns weltweit entwickelt. Mit den „Binding Corporate Rules Privacy“ (BCRP) bietet die Telekom ihren Kunden und Mitarbeitern in jedem Land der Welt das gleiche hohe Datenschutzniveau.

Die Binding Corporate Rules Privacy der Telekom garantieren ein weltweit gleich hohes Datenschutzniveau.

Die BCRP sind eine Weiterentwicklung des bereits für viele Landesgesellschaften der Telekom geltenden Privacy Code of Conduct (PCoC). Sie lösen den PCoC ab, berücksichtigen aktuelle Gesetzesänderungen und gelten für alle Tochterunternehmen der Telekom Gruppe weltweit. Die Telekom hat diese Richtlinien in Einklang mit dem Bundesdatenschutzgesetz (BDSG) und europäischen sowie internationalen Datenschutzrichtlinien entwickelt. In einzelnen Punkten geht die Telekom jedoch über die gesetzlich vorgegebenen Mindeststandards hinaus.

Jede Landesgesellschaft unterzeichnet die Richtlinien, die in Deutschland unter der „Konzernrichtlinie Datenschutz“ geführt werden und in allen übrigen Regionen der Welt inhaltlich identisch sind. Mit Unterzeichnung verpflichtet sich jede Gesellschaft unabhängig von den im jeweiligen Land geltenden Datenschutzbestimmungen dazu, den gleichen hohen Maßstab bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten anzulegen. In den seltenen Fällen, in denen in einem Land striktere Datenschutzvorgaben gelten als in den BCRP, tritt das geltende Recht an die Stelle der Telekom Richtlinie. Im umgekehrten Fall, etwa in Brasilien, wo es kein Datenschutzgesetz gibt, gelten die BCRP in vollem Umfang.

Die Telekom hat ihre Konzernrichtlinie bereits mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) abgestimmt. Anschließend hat sie die BCRP zur Prüfung an internationale Aufsichtsbehörden geschickt. Sobald Österreich und Polen dem Entwurf zustimmen, wird der Vorstand der Telekom die Richtlinie verabschieden und ihren internationalen Rollout beauftragen, der bis Ende 2014 abgeschlossen sein soll.

NEUES GOVERNANCEMODELL FÜR ALLE LÄNDER

Das internationale Governancemodell der Telekom definiert die Aufgabenbereiche der Datenschutzbeauftragten und die Verantwortlichkeiten des Vorstands jeder Telekom Gesellschaft weltweit.

Die Datenschutzspezialisten der Telekom haben ein internationales Governancemodell erarbeitet, das auf der Datenschutzrichtlinie des Konzerns basiert. In kompakter Form als modular aufgebautes Handbuch legt das Modell verbindlich fest, über welches Profil der Datenschutzbeauftragte einer Landesgesellschaft verfügen muss und welche Aufgaben er zu erfüllen hat. Darüber hinaus richtet sich das Governancemodell auch direkt an die Geschäftsführung der Landesgesellschaften und legt deren Verantwortlichkeiten fest.

Mit diesem Modell stellt die Telekom sicher, dass jeder Datenschutzbeauftragte eines Telekom Unternehmens die nötige Unterstützung erhält, um die hohen Ansprüche an den Umgang mit personenbezogenen Daten zu erfüllen – auch wenn die Behörden den Datenschutz in den meisten Ländern weniger stark regulieren als in Deutschland. Der Konzern überprüft jährlich die

Internationales Governancemodell der Telekom basiert auf Konzern-Datenschutzrichtlinie.

Einhaltung der Datenschutzrichtlinien im Rahmen des „International Basic Privacy Audit“. Dabei füllt der Datenschutzbeauftragte einer Landesgesellschaft zunächst einen Fragebogen aus, um den Prüfern in der Zentrale einen Überblick über die Situation in seiner Gesellschaft zu geben. Zeitgleich nehmen etwa 30 Prozent der Mitarbeiter an einer Onlinebefragung teil. Auf Basis der Ergebnisse beider Befragungen erfolgt eine Prüfung vor Ort. Dabei auditieren die Experten aus der Zentrale sowohl physikalische Schutzmaßnahmen als auch die Situation für den Datenschutzbeauftragten vor Ort.

GEMEINSAME LINIE

Die ausländischen Standorte der Telekom weisen ein hohes Datenschutzniveau auf. Dies belegen regelmäßige Vor-Ort-Audits des Konzerndatenschutzes.

Die Deutsche Telekom ist in rund 50 Ländern vertreten. Im Ausland trifft der Konzerndatenschutz auf eine Fülle von Auffassungen, worauf im Umgang mit personenbezogenen Daten zu achten ist. Unterschiede zeigen sich sowohl in rechtlicher als auch in kultureller Hinsicht. Um ein weltweit einheitliches Schutzniveau zu erreichen, hat die Telekom bereits 2004 eine konzernweite Leitlinie eingeführt und seither kontinuierlich weiterentwickelt (siehe Seite 15: Weltweit einheitliche Datenschutzrichtlinien). Mit kontinuierlichen Vor-Ort-Audits untersuchen die Mitarbeiter des Konzerndatenschutzes, in welchem Maße die ausländischen Töchter und Beteiligungen den Bestimmungen des PCoC nachkommen.

2013 konzentrierten sich die Audits auf Südafrika, Malaysia, Russland, Spanien, Ungarn, Griechenland und die Schweiz. Das Spektrum der geprüften Standorte reichte von der Verwaltung über die Produktion (Engl.: Point of Production) bis zum Rechenzentrum. Im Fokus der Audits steht die Frage, wie die jeweiligen Konzerngesellschaften die Anforderungen des Datenschutzes in ihre Arbeitsabläufe einbetten. Neben zahlreichen technischen und organisatorischen Maßnahmen prüfen die Auditoren die Rolle des lokalen Datenschutzbeauftragten: Ist er fachlich geeignet? Kann er die Belange des Datenschutzes gegebenenfalls auch gegen den Widerstand des Managements durchsetzen? Stehen ihm genügend personelle und finanzielle Ressourcen zur Verfügung? Fördern die Prüfer Defizite zutage, so setzen sie gemeinsam mit den Verantwortlichen vor Ort Maßnahmen auf, die sie in Folgeaudits überprüfen. 2013 stellten die Auditoren in 13 internationalen Prüfungen fest, dass sich der konzernweite Datenschutz auf einem hohen Niveau stabilisiert hat.

KARTIERTE RISIKEN

Die Datenschützer der Deutschen Telekom haben eine Landkarte entworfen, auf der sie die Datenschutzrisiken der Konzerngesellschaften kennzeichnen. Die Risikolandkarte hilft den Experten, die Standorte und Systeme zu ermitteln, in denen der höchste Auditbedarf herrscht.

Wie entscheidet der Konzerndatenschutz, welche IT-Systeme und Tochtergesellschaften er auditiert, um den Umgang mit personenbezogenen Daten zu prüfen? Mitte 2013 hat die Telekom ein Planungswerkzeug erstellt, das konzernweit mehr Transparenz schafft. Ziel dieser sogenannten Risikolandkarte ist es, die Auditauswahl zu formalisieren und für alle Beteiligten nachvollziehbarer zu machen.

Die Landkarte verarbeitet 26 Risikofaktoren. Grundlegend gibt sie darüber Auskunft, wie sensibel die Daten sind, die verarbeitet werden. Die Sensibilität bemisst sich nach den Schutzklassen der Daten, nach ihrer Relevanz für das Fernmeldegeheimnis sowie dem Detaillierungsgrad der eventuell angelegten Persönlichkeitsprofile. Zudem geht die Gesamtzahl der verarbeiteten Datensätze in die Kartierung mit ein. Ebenso vermerken die Datenschützer, ob Data-Warehouse-Systeme im Einsatz sind und wie viele Schnittstellen es zu anderen IT- und Telekommunikationssystemen gibt.

Ein zusätzliches Augenmerk liegt auf den Verarbeitungsrisiken, die aus Unternehmensbeteiligungen entstehen. Unter anderem untersuchen die Kartografen die Kritikalität des Geschäftsmodells der Beteiligungen und das allgemeine Datenschutzniveau im jeweiligen Land. Weitere Faktoren sind Auffälligkeiten und offene Maßnahmen aus vorangegangenen Audits. Darüber hinaus bezieht die Risikolandkarte Informationen aus dem laufenden Incident Reporting mit ein. Aus all diesen Faktoren errechnet sich ein Gesamtwert für das gegenwärtige Datenschutzrisiko. Anhand dieser Auswertung entscheiden die Mitarbeiter des Konzerndatenschutzes, an welchen Standorten sie welche Art von Audit durchführen werden.

AUFWÄRTSTREND HÄLT AN

Das Basisdatenschutzaudit gibt detailliert Auskunft darüber, wie ausgeprägt das Wissen der Telekom Mitarbeiter in puncto Datenschutz ist und wie intensiv sie dieses Know-how im Tagesgeschäft umsetzen. 2013 legten die Kennzahlen noch einmal deutlich zu.

Wissen Sie, wie sich E-Mails sicher verschlüsseln lassen? Kennen Sie den Meldeweg für Datenschutzvorfälle? Mit praxisbezogenen Fragen wie diesen ermittelt das Basisdatenschutzaudit, inwieweit die Belange des Datenschutzes im Tagesgeschäft der Beschäftigten angekommen sind. Um die Kompetenzentwicklung langfristig einschätzen zu können, führt der Konzerndatenschutz die Befragung jährlich durch. 2013 nahmen 36.000 repräsentativ ausgewählte Mitarbeiter aus 33 Landesgesellschaften teil.

Die Ergebnisse zeigen für alle Landesgesellschaften, dass das Datenschutzniveau noch einmal signifikant angestiegen ist. Dies belegt die sogenannte Hauptkennzahl, mit der die Prüfer die zahlreichen Einzelergebnisse des Audits in einem einzigen Wert zusammenfassen. Während die Hauptkennzahl in Deutschland im Jahresvergleich von 9,1 auf 9,7 zulegte, fiel das internationale Wachstum sogar doppelt so stark aus: Nach 6,5 im Jahr 2012 kamen die Landesgesellschaften 2013 auf einen neuen Spitzenwert von 7,6.

Mitarbeiter öffnen ihre Schulungsräume per Mausklick.

VIRTUELLE SCHULE

Seit diesem Jahr steht den Telekom Mitarbeitern ein webbasiertes Schulungshaus für den Datenschutz offen. Im Intranet ist das neue Schulungswerkzeug rund um die Uhr erreichbar. Nutzer erhalten Informationen zu allen Fragen des betrieblichen Datenschutzes.

Das Schulungshaus führt die Mitarbeiter durch die Wissensangebote des Konzerndatenschutzes. Auf drei Etagen erhalten sie Zugang zu sämtlichen Schulungsmodulen. Per Mausklick öffnen sie das Angebot, das sie aktuell nutzen wollen. Im Erdgeschoss finden sie die Grundlagenschulung, zu der jeder Telekom Beschäftigte verpflichtet ist. Der erste Stock bietet Platz für Aufbauschulungen, in denen die Inhalte des Erdgeschosses vertieft werden. In der Dachetage befinden sich Spezialistenschulungen zu ausgewählten Datenschutzthemen, die sich gezielt an einzelne Arbeitsbereiche wenden – so etwa an die Mitarbeiter des Marketings, der Personalabteilung oder des Rechnungswesens. Wie die Angebote des Schulungshauses bei der Belegschaft ankommen, messen die Datenschützer über die Klickraten, die anonymisiert erhoben werden.

MEHR PRAXISBEZUG

Die Deutschen Telekom setzt auf eine webbasierte Grundlagenschulung, um alle Mitarbeiter im Umgang mit personenbezogenen Daten fit zu machen. 2013 wurde die Schulung aktualisiert. Dabei wurde vor allem der Praxisbezug noch einmal signifikant gestärkt.

Alle Telekom Angehörigen sind konzernweit zu einer Grundlagenschulung im Daten- und Informationsschutz verpflichtet. Damit die Verpflichtung nicht zur reinen Pflichtübung wird, hat der Konzerndatenschutz ein interaktives Schulungsformat konzipiert, das die Mitarbeiter in ihrem Tagesgeschäft abholt und praxisorientiert mit den Anforderungen des Datenschutzes vertraut macht. Um die Bezüge zu den Arbeitsabläufen noch deutlicher werden zu lassen, erhielt die Onlineschulung im April 2013 ein neues Gesicht. Seither erscheinen die Inhalte ausschließlich aus der Perspektive der Mitarbeiter. Ganz gleich, ob es um Allgemeinwissen im Datenschutz, den Umgang mit Mitarbeiter- und Kundendaten oder das Melden von Vorfällen geht. Stets haben sich die Schulungsverantwortlichen die Frage gestellt, wie sich die zu vermittelnden Themen auf die Arbeit der Kollegen auswirken. Und um wirklich jeden zu erreichen, wurde zusätzlich auch an eine Verbesserung der Barrierefreiheit gedacht.

DATENSCHUTZ ON TOUR

2013 hat Dr. Claus-Dieter Ulmer, Konzernbeauftragter für den Datenschutz, mehrere Telekom Landesgesellschaften besucht und sich mit dem Management zum Thema Datenschutz ausgetauscht.

Auch wenn das Datenschutzniveau bei der Deutschen Telekom insgesamt hoch ist, zeigen die jährlichen Audits Unterschiede im Umgang mit dem Thema Datenschutz auf. Daher hat sich der Konzerndatenschutz in Abstimmung mit dem Datenschutzbeirat auf die Reise begeben, um gemeinsam mit den jeweiligen Datenschutzbeauftragten das Management vor Ort über die offenen Punkte zu informieren und mögliche Lücken zu schließen. Das Ziel der Reise: dem Thema Datenschutz mehr Aufmerksamkeit schenken und ein einheitliches Verständnis für den Datenschutz aufbauen.

Wichtig für ein konzernweites einheitliches Datenschutzniveau sei, dass das örtliche Management verstehe, dass es den Datenschutz in der jeweiligen Landesgesellschaft verantworte, erklärt Claus-Dieter Ulmer. „In einigen Ländern standen etwa zu wenige Ressourcen für den Datenschutz zur Verfügung. „Den Datenschutzbeauftragten vor Ort müssen aber immer die notwendigen Ressourcen bereitstehen, damit sie ein angemessenes Datenschutzniveau herstellen und halten können“, unterstreicht Ulmer. Auch der Umgang mit den Kundendaten stand auf dem Programm. So ist in den Datenschutzrichtlinien des Konzerns klar definiert, nur diejenigen Kunden mit Werbung zu kontaktieren, die dafür ihr Einverständnis gegeben haben. Denn Kunden sollten selbst über ihre Daten entscheiden können. Das wird in einigen Ländern weniger kritisch gesehen und lässt sich teilweise auf unterschiedliches Datenschutzverständnis in den jeweiligen Kulturen zurückführen. So gibt es in China bis heute kein eigenes Wort für Privatheit. „Ich bin überall auf offene Türen, Ohren und Herzen gestoßen“, sagt Ulmer. „Meinen Gastgebern konnte ich verdeutlichen, warum manche internationale Regelung, die wir in Bonn festlegen, unumgänglich ist für den vertrauensvollen Umgang mit unseren Kunden und Mitarbeitern und damit auch für das Wohl des Konzerns.“

Einige Stationen der Datenschutz on Tour:
Niederlande, China, Polen, Slowakei, Tschechien und Dänemark.

ENTSCHEIDER-INFORMATIONSSYSTEM GESTOPPT

Bei der Migration eines IT-Systems für das Personalmanagement stellte sich heraus: Statt ausschließlich anonymisierter Daten enthält es auch personenbezogene Informationen von Mitarbeitern. Das System wurde gestoppt, der Betriebsrat informiert.

Mitarbeiterzahlen, Altersstruktur, mögliche Engpässe in der Personalplanung – die Software SAP Business Warehouse EIS (Entscheider Information System) generiert solche statistischen Kennzahlen für Geschäftsberichte und Einsatzplanungen. Dafür werden nur anonymisierte Daten benötigt, die nicht auf bestimmte Mitarbeiter zurückzuführen sind. Durch eine vom Datenschutz durchgeführte Prüfung hat sich jedoch herausgestellt, dass es trotzdem seit 2002 personenbezogene Daten der Mitarbeiter in Deutschland enthält. Nach Bekanntwerden des Vorfalls wurden alle Reports gesperrt und das System EIS von anderen Systemen isoliert.

Grundsätzlich darf ein Unternehmen personenbezogene Daten der Mitarbeiter verarbeiten, wenn es die datenschutzrechtlichen Vorgaben einhält und die Daten für einen legitimierten Zweck verwendet, etwa für die Gehaltsabrechnung. Da diese datenschutzrechtliche Klärung beim System EIS offensichtlich nicht vorgenommen worden war, hätten die personenbezogenen Daten anonymisiert werden müssen. Auch wenn im System selbst nur ein begrenzter Kreis von Mitarbeitern Zugriff auf die personalisierten Daten hatte.

Der Vorstand hat sich bei den Arbeitnehmern entschuldigt und die Aufsichtsbehörden, den Datenschutzbeirat und den Prüfungsausschuss des Aufsichtsrats informiert. Weiterhin hat der Vorstand unmittelbar nach Bekanntwerden des Fehlers drei Projekte zur Aufarbeitung des Vorfalls beschlossen. Eine unabhängige, externe Wirtschaftsprüfungsgesellschaft prüft, wie es zu der Verarbeitung personalisierter Daten kommen konnte. Dazu analysieren die Prüfer, welche Daten die Software zu welchem Zweck ausgewertet hat und ob es während der langen Laufzeit des Systems EIS Auffälligkeiten gegeben hat, die auf die Verarbeitung nicht anonymisierter Daten hingewiesen haben. Weiterhin wird das System so umgebaut, dass es aus datenschutz- und mitbestimmungsrechtlicher Sicht nutzbar ist, so dass die für das Unternehmen notwendigen Reports wieder erstellt werden können. Im dritten Projekt nimmt ein Team nochmals alle HR-Systeme auf Übereinstimmung mit den gesetzlichen Rahmenbedingungen unter die Lupe.

DATENSCHUTZ IN DER SCHULE

Wie sich Kinder und Jugendliche sicher im Netz bewegen können und worauf sie beim Surfen achten sollten.

Bösartige Kommentare über Lehrer und Mitschüler auf Facebook. Fotos vom letzten Trinkgelage am Wochenende auf Instagram. Saftige Rechnungen für das Downloaden von teuren Apps. In der digitalen Welt lauern Fallstricke unterschiedlichster Art, und das Internet vergisst nichts.

Wenn eine Schule ihre Schüler vor den Gefahren im Internet warnen will, kann sie einen Datenschützer der Telekom kostenlos buchen. Unter anderem erklärt Claus-Dieter Ulmer, Konzernbeauftragter für den Datenschutz der Deutschen Telekom, was die Schüler beim Surfen lieber lassen sollten und wie sie sich sicher im Netz bewegen können. Das Angebot richtet sich an sämtliche Schulformen. Weitere Informationen können Schulen anfordern per E-Mail an: datenschutz@telekom.de.

HFGWLU STATT MÜLLER

Die Telekom hat ein eigenes Anonymisierungstool entwickelt, das nicht nachvollziehbare, jedoch eindeutig zugeordnete Pseudonyme aus Echtdaten erstellt.

Die Deutsche Telekom verarbeitet in Kundendatenbanken Millionen von personenbezogenen Informationen. Dazu kommen Verbindungsdaten aus Telefonie und Internetnutzung. Führt sie neue Software ein, zum Beispiel für das Kundenmanagement oder die Rechnungserstellung, müssen die IT-Experten des Konzerns die Funktionen zunächst mit möglichst realitätsnahen Daten testen. Laut Datenschutzgesetzgebung dürfen sie dafür keine echten Daten aus den Altsystemen verwenden. Bisher erstellten sie daher fiktive Datensätze, die jedoch die Wirklichkeit nur unzureichend widerspiegeln.

Eine Alternative ist, echte Daten zu anonymisieren, in dem sie etwa reale Namen oder Adressen austauschen. So wird aus Müller ein Meier, der nicht in der Burgstraße 17 sondern in der Holzgasse 11 wohnt. Dieses Verfahren ist sehr aufwendig. Es ist zudem nicht genau nachvollziehbar, wie die Sicherheitsmechanismen der dafür eingesetzten kommerziellen Software-Lösungen genau funktionieren.

Mit dem neuen Anonymisierungstool werden aus Namen kryptische Buchstabenkombinationen wie Hsjxut oder Pdhiwuhf sowie aus Rufnummern quasi zufällige Zahlenfolgen. Die Nutzung von pseudonymisierten und dann anonymisierten Echtdaten verbessert die Testqualität – zum Vorteil für Kunden und Telekom –, und sie

erfüllt die gesetzlichen Vorgaben des Datenschutzes. Denn der Übergang vom Pseudonym zum Anonym erfolgt erst dann, wenn der für den Pseudonymisierungsschritt erforderliche Schlüssel vollständig gelöscht ist. Danach ist es nicht mehr möglich, an die Originaldaten zu gelangen.

DATENSCHUTZ UND DATENSICHERHEIT IM KOALITIONSVERTRAG

Der Koalitionsvertrag enthält klare Aussagen zu den Zielen der neuen Bundesregierung für mehr Datenschutz und Datensicherheit. Die Telekom unterstützt diese Vorhaben und setzt sich für die Stärkung der informationellen Selbstbestimmung der Nutzer in digitalen Netzen ein.

Besonders zu begrüßen ist, dass sich die neue Regierung dafür einsetzen will, die EU-Datenschutzgrundverordnung schnell zu verabschieden. Im Koalitionsvertrag heißt es dazu: „Die EU-Datenschutzgrundverordnung muss zügig weiter verhandelt und schnell verabschiedet werden, um europaweit ein einheitliches Schutzniveau beim Datenschutz zu garantieren. Die strengen deutschen Standards beim Datenschutz, gerade auch beim Datenaustausch zwischen Bürgern und Behörden wollen wir bewahren. Europa braucht ein einheitliches Datenschutzrecht für die Wirtschaft, in dem alle Anbieter, die in Europa ihre Dienste anbieten, dem europäischen Datenschutzrecht unterliegen."

Außerdem begrüßt es die Deutsche Telekom, dass sich auch die neue Bundesregierung dem Ziel verschrieben hat, ein Gesetz zur Regelung

des Beschäftigtendateschutzes zu verabschieden. Klare Regelungen in diesem Bereich sind überfällig. Die Telekom selbst strebt in diesem Zusammenhang bereits heute den Abschluss einer Konzernbetriebsvereinbarung zum Beschäftigtendatenschutz mit dem Sozialpartner an.

„Wir werden die EU-Richtlinie über den Abruf und die Nutzung von Telekommunikationsverbindungsdaten umsetzen", heißt es darüber hinaus im Vertrag zwischen CDU, CSU und SPD. „Die Speicherung der deutschen Telekommunikationsverbindungsdaten, die abgerufen und genutzt werden sollen, haben die Telekommunikationsunternehmen auf Servern in Deutschland vorzunehmen. Auf EU-Ebene werden wir auf eine Verkürzung der Speicherfrist auf drei Monate hinwirken."

Sollte die Regierung während der 18. Legislaturperiode unter Berücksichtigung der ausstehenden Entscheidung des Europäischen Gerichtshofes ein Gesetz zur Vorratsdatenspeicherung umsetzen, wird die Telekom an diese gesetzlichen Anforderungen gebunden sein. Wichtig sind dabei klare und nachvollziehbare Vorgaben ohne Rechtsunsicherheiten für die Telekommunikationsanbieter. Für die Telekom besonders bedeutend ist die durchgehende Umsetzung des Richtervorbehaltes für alle Daten – insbesondere auch für IP-Adressen –, so, wie es der Koalitionsvertrag vorsieht. „Dabei soll ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten, zur Abwehr akuter Gefahren für Leib oder Leben" und unter Vorbehalt einer richterlichen Anordnung erfolgen dürfen.

NUTZERFREUNDLICHE DATENSCHUTZHINWEISE

Die Telekom hat sich als Konzernziel unter anderem „Einfachheit" auf die Fahne geschrieben. Dies gilt für Produkte und Lösungen – und auch für Datenschutzhinweise.

Sie sind zu lang, zu unübersichtlich oder sie sind für Nichtjuristen kaum zu verstehen: Datenschutzhinweise bleiben für viele Verbraucher oft ein Buch mit sieben Siegeln. Dabei schreibt das Telekommunikationsgesetz in § 93 vor: „Diensteanbieter haben ihre Teilnehmer bei Vertragsabschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten so zu unterrichten, dass die Teilnehmer in allgemein verständlicher Form Kenntnis von den grundlegenden Verarbeitungstatbeständen der Daten erhalten."

Mit dem vom Datenschutzbereich entwickelten Icon erkennen Kunden auf einen Blick, wann der Kauf eines Produkts oder der Abschluss eines Vertrags datenschutzrelevant ist.

Daher hat die Telekom 2013 damit begonnen, ihre Datenschutzhinweise übersichtlicher und verständlicher zu gestalten. Sie hat die Texte zum einen in Form eines Fragenkatalogs aufgearbeitet, so dass der Leser nun schnell und unkompliziert genau die Informationen findet, die er sucht.

Die Telekom hat zum anderen die Formulierungen erheblich vereinfacht, was das Verständnis deutlich erleichtert. Für die Auftragsbestätigung bei Bestellung eines Telefonanschlusses hat der Datenschutzbereich zudem eine Kurzfassung der Datenschutzhinweise entwickelt.

Auch die internen Prozesse wurden verbessert. Konnte es bisher vorkommen, dass im Konzern unterschiedliche Datenschutzhinweise für die gleichen Angebote verwendet wurden, stellt ein neues Verfahren sicher, dass die Datenschutzhinweise immer in einheitlicher und aktueller Version verfügbar sind. Zudem gibt es für Privat- und Geschäftskunden bei Abschluss eines Vertrags dieselbe Fassung der Datenschutzhinweise. Und sie entfallen ganz, wenn sie gar nicht erforderlich sind, zum Beispiel beim Barkauf eines Endgeräts.

FLUCH ODER SEGEN?

Die Debatten und Spekulationen um PRISM und Tempora haben den Blick auf Big-Data-Technologien getrübt. Bringen das Sammeln und Auswerten von riesigen Datenmengen wirklich Vorteile für den Bürger? Oder zieht auf Kosten des Datenschutzes allein die Wirtschaft einen Nutzen aus Big Data? Eine Diskussion mit dem unabhängigen Konzernbeauftragten für den Datenschutz der Deutschen Telekom, **Dr. Claus-Dieter Ulmer**, und Telekom Vorstand **Reinhard Clemens,** der als Chef von T-Systems seinen Geschäftskunden Big-Data-Lösungen verkauft.

Wer Big-Data-Analysen durchführt, sollte seine Kunden entscheiden lassen, ob sie ihre personenbezogenen Daten zur Verfügung stellen wollen.

Herr Dr. Ulmer, Ihnen müsste doch angesichts der Möglichkeiten von Big Data Angst und Bange werden. Werden Sie bei Telekom Big Data verhindern?
Dr. Claus-Dieter Ulmer: Ich lehne Big Data nicht pauschal ab. Dafür gibt es zu viele positive Anwendungsszenarien, die nicht nur Unternehmen einen Nutzen bringen, sondern genauso den Menschen. Dazu gehört beispielsweise die Auswertung von Verkehrsdaten in Echtzeit, um Staus zu verringern. Aber wir Datenschützer begleiten die Big-Data-Aktivitäten im Konzern mit wachem Auge. Wir schauen genau hin, was wir mit den Daten unserer Kunden machen, aber auch was T-Systems Geschäftskunden als Big-Data-Lösungen anbietet.

Worin besteht denn aus Sicht des Datenschutzes die grundlegende Problematik von Big Data?
Dr. Claus-Dieter Ulmer: Lassen wir die Daten aus der Machine-to-Machine-Kommunikation außen vor, dann bestehen Big-Data-Modelle grundsätzlich in der Verarbeitung von Informationen, die personenbezogen oder personenbeziehbar sind. Dementsprechend muss für die Verarbeitung eine Rechtsgrundlage gegeben sein. Diese kann sich im Gesetz finden oder gegebenenfalls aus der Einwilligung des Betreffenden herleiten. Daneben ist es möglich, Datenbestände zu anonymisieren. Dann unterliegen sie nicht mehr dem Datenschutzrecht und deren Verarbeitung bedarf dann keiner Rechtsgrundlage mehr.

Herr Clemens, diese Auslegung des Datenschutzes engt den Rahmen von Big-Data-Lösungen stark ein. Wie oft haben Sie sich schon über die Datenschützer geärgert?
Reinhard Clemens: Noch nie! Wir sind gar nicht auseinander in unserer Einschätzung von Big Data. Ohne die Akzeptanz der Bürgerinnen und Bürger wird sich die neue Technologie nicht durchsetzen. Dafür brauchen wir auch einen strengen Datenschutz. Wir haben vergangenes Jahr mit dem Handelsblatt Research Institute eine Studie zu Big Data durchgeführt. Die Ergebnisse zeigen, dass nach den Geheimdienstaffären bei den Menschen große Skepsis und Unsicherheit bestehen, was mit ihren Daten passiert. Dies nehmen wir sehr ernst und prüfen mit den Datenschützern ganz genau, welche Lösungen wir auf den Markt bringen.

Ist das Kind aber durch die NSA-Affäre nicht längst in den Brunnen gefallen?
Reinhard Clemens: Es gibt einen sehr großen Vertrauensverlust in der Bevölkerung. Dies ist auch vollkommen nachvollziehbar. Aber wir dürfen nicht vergessen, dass hier ein illegaler Zugriff auf persönliche Daten vermutet wird. Das ist ja nicht Big Data. Denn Big Data ist die Verarbeitung, Verknüpfung und Auswertung von nicht personenbezogenen Daten jeglicher Art, zum Beispiel die Auswertung regionalisierter Wetterdaten mit dem Einkaufverhalten. Dagegen ist die Auswertung von Daten einer konkreten Person aus verschiedensten Quellen in Deutschland nicht erlaubt. Allerdings wird das in der Öffentlichkeit noch nicht differenziert. Unsere Aufgabe als Unternehmen ist es deshalb, das Vertrauen für unsere Sache zu gewinnen. Dies gilt insbesondere bei allem, was mit personenbezogenen Daten zu tun hat. Die Telekom hat sich daher eigene Leitsätze für Big Data gegeben, deren wichtigster Punkt Transparenz ist. Verbraucher müssen wissen, was mit ihren personenbezogenen Daten passiert.

Es gibt Big-Data-Lösungen, welche die Telekom ihren Kunden anbietet. Wie sieht es aber mit den eigenen Kundendaten aus? Es müsste doch jeden Marketingverantwortlichen kitzeln, diese Daten auszuwerten.
Dr. Claus-Dieter Ulmer: Wir unterliegen in hohem Maße dem zu Recht sehr strengen Telekommunikationsgesetz. Standortdaten, also Verkehrsdaten, dürfen wir lediglich zu Vertrags-

erfüllungszwecken, zu Zwecken der Abrechnung oder zu anderen im Telekommunikationsgesetz genannten Vorhaben verwenden. Für die Auswertung von Daten im Rahmen von Big-Data-Modellen findet sich keine explizite Rechtsgrundlage im Telekommunikationsgesetz. Für den Bereich des direkten Marketings oder der Werbung reichen die Rechtsgrundlagen nicht. Damit können sie auch nicht für Lösungen wie Big-Data-Auswertungen herangezogen werden. Und daran halten wir uns.

Unternehmen können das umgehen, indem sie die Einwilligung ihrer Kunden einholen.

Dr. Claus-Dieter Ulmer: Es ist richtig, dass Big-Data-Anwendungen durch die Einwilligung der Betreffenden zum Einsatz kommen. Eine wirksame Einwilligung setzt zwingend voraus, dass der Betreffende transparent über den Zweck der Datenverarbeitung und die daraus ableitbaren Ergebnisse für ihn nachvollziehbar informiert wird. Er muss für sich selbst eine Risikoabwägung vornehmen können, wie sich die Verarbeitung auf ihn und seine persönliche Situation auswirken kann. Die Art und Weise, wie und was ausgewertet werden soll, sollte den Betreffenden bekannt sein.

Reinhard Clemens: Unsere Studie bestätigt: Wenn die Kunden einen klaren Nutzen erkennen, stehen sie einer Auswertung positiv gegenüber. Eine deutliche Mehrheit lehnt es ab, dass bei Online-Einkäufen die Anbieter die Eingabe von Adresse, Bankverbindungen und sonstiger persönlicher Angaben nur für den schnelleren Einkauf fordern. Dagegen akzeptiert es mehr als die Hälfte der Bevölkerung, dass Pharmafirmen Beiträge in Diskussionsforen auswerten, um bislang unbekannte Nebenwirkungen eines Medikaments herauszufinden.

Drei von vier Verbrauchern sagen jedoch, dass Unternehmen ihre Kunden nicht ausreichend darüber informieren, ob sie die Daten speichern und wofür sie diese verwenden.

Dr. Claus-Dieter Ulmer: Es gibt sicher eine Reihe von Firmen, die datenschutzrelevante Aspekte in den Verträgen und allgemeinen Geschäftsbedingungen (AGB) irgendwo versteckt aufführen. Das darf nicht sein. Wir legen deshalb Wert darauf, unsere Kunden möglichst klar und deutlich zu informieren. Allerdings sind auch unsere Kunden gefordert, sich über Datenschutzaspekte zu informieren. So ist es bedenklich, wenn eine deutliche Mehrheit der Verbraucher zugibt, sie würden nie oder nur ab und zu die AGB lesen, wenn sie eine App auf ihr Smartphone laden. Genau hier aber könnten sie die schwarzen Schafe des Datenschutzes erkennen und sich selbst vor Missbrauch schützen.

Reinhard Clemens: Ich will deutlich unterstreichen, dass die Verbraucher wissen müssen, welche Vorteile sie haben, wenn Unternehmen anonymisierte Daten nutzen, um zum Beispiel Produkte und Services zu verbessern. Dafür müssen wir erklären, dass ein großer Teil der Big-Data-Analysen nicht auf personenbezogenen Daten beruht, für die das Datenschutzrecht greift, sondern auf anonymisierten Daten. Auch unsere Big-Data-Leitsätze sollen hier klar und transparent weiterhelfen. Wir brauchen unbedingt einen aufgeklärten und verantwortungsbewussten Umgang mit Daten – eine Kultur des Einverständnisses.

DIE BIG-DATA-LEITSÄTZE DER DEUTSCHEN TELEKOM

1. Die Deutsche Telekom ist sich ihrer gesellschaftlichen Verantwortung bewusst und wird Big-Data-Lösungen mit der notwendigen Sensibilität entwickeln.
2. Die Deutsche Telekom ist transparent über ihre Planungen und Lösungen im Bereich Big Data und sucht den Austausch mit Aufsichtsbehörden, Politik, staatlichen und nicht staatlichen Institutionen sowie Kunden und Bürgern.
3. Die Deutsche Telekom verarbeitet Daten für Big-Data-Lösungen grundsätzlich in anonymisierter Form, so dass eine Rückführung auf einzelne Personen ausgeschlossen ist. Die Anonymisierung erfolgt an der Quelle oder so quellnah wie möglich.
4. Die Deutsche Telekom bekennt sich zur Kultur des Einverständnisses und wird, soweit die Verwendung von personenbezogenen Informationen notwendig wird, diese nur mit Einwilligung des Betreffenden in Big-Data-Lösungen einbringen.
5. Die Deutsche Telekom wird verschiedene anonymisierte Datenbestände nur so zusammenführen, dass auch eine mittelbare Rückführung auf einzelne Personen ausgeschlossen ist.
6. Die Deutsche Telekom wird Informationen über Gruppen von Personen nur auswerten, wenn sichergestellt ist, dass eine Gruppe, auf die sich Ergebnisse beziehen, dadurch nicht einem Diskriminierungsrisiko ausgesetzt wird.
7. Die Deutsche Telekom stellt Dritten keine Kundendaten zur Verfügung, sondern lediglich die Ergebnisse eigener, interner Auswertungen.
8. Die Deutsche Telekom wird über etwaige Änderungen dieser Leitsätze transparent informieren.

ZU DEN PERSONEN

Reinhard Clemens
ist seit 2007 Vorstandsmitglied der Deutschen Telekom AG und CEO von T-Systems. Zuvor verantwortete der studierte Elektrotechniker bei EDS in Deutschland als Vorsitzender der Geschäftsführung die Bereiche Vertrieb, Business Operations und Strategie in Zentraleuropa.

Dr. Claus-Dieter Ulmer
ist seit 2002 Konzernbeauftragter für den Datenschutz der Deutschen Telekom AG. Zuvor leitete der promovierte Jurist den Datenschutz von T-Systems International und war als Rechtsanwalt mit Schwerpunkt Arbeitsrecht tätig.

CLOUD-COMPUTING IST VERTRAUENSSACHE

IT-Experte Peter Franck gehört dem Datenschutzbeirat der Deutschen Telekom an. Beim Cloud-Computing sieht er spezifische Risiken für Architektur, Anwendungen und Nutzergruppen der unterschiedlichen Angebote.

ZUR PERSON

Peter Franck gehört dem Chaos Computer Club seit etwa 30 Jahren an. Sein beruflicher Schwerpunkt ist die Entwicklung von Elektronik, Software und Verfahren. Zudem arbeitete er mehrere Jahre als technischer Gutachter. In den vergangenen zehn Jahren ist Peter Franck hauptsächlich im Bereich Datenrettung tätig.

Die Bandbreite der Cloud-Services reicht von der Infrastrukturebene bis zur Anwendungsebene. Dabei geschieht die gesamte Verarbeitung und Datenhaltung für den Anwender unsichtbar im Hintergrund. Der Anwender nimmt nur die Präsentationsschicht – meist in Form einer Weboberfläche oder App – wahr. Daten werden in der Cloud in aller Regel unverschlüsselt verarbeitet. Somit besteht die Möglichkeit des administrativen Zugriffs durch den Betreiber oder Bedarfsträger, derer sich der Betreiber nicht erwehren kann. Um abzuschätzen, welche Instanzen dafür in frage kommen, ist primär relevant, wo sich die Rechenzentren physisch befinden und von welchen Jurisdiktionen der Betreiber abhängig ist. Das ist umso wichtiger, wenn es darum geht, personenbezogene Daten zu speichern oder zu verarbeiten. Letztlich ist die Auswahl eines Cloud-Anbieters – neben Gesetzen und Vereinbarungen – eine Frage des Vertrauens in den Betreiber und die eingesetzte Technik.

RISIKEN AUF BETREIBERSEITE

Die Möglichkeit des unbefugten Zugriffs auf die Administrationsebene der Cloud ist für jede Cloud sicherheitsmäßig ein Totalschaden, weil dadurch schlimmstenfalls alle Prozesse und Daten kompromittiert sind. Dass es sich dabei nicht nur um eine theoretische Gefahr handelt, haben in der Vergangenheit erfolgreiche Angriffe auf Schwachstellen in praktisch allen Hypervisoren, also den Virtualisierungssystemen selbst, die zur Verwaltung und Isolation der virtuellen Systeme untereinander dienen, gezeigt. Allerdings sind seriöse Cloud-Betreiber auf allerlei Schwachstellen sicher besser vorbereitet als die meisten kleinen und mittleren Unternehmen, weshalb eine Verlagerung von Anwendungen in die Cloud durchaus einen Sicherheitsgewinn bedeuten kann.

Eine interessante Entwicklung stellt in diesem Zusammenhang die sogenannte „homomorphe Verschlüsselung“ dar. Damit bezeichnet man Verschlüsselungsverfahren, die eine Verarbeitung verschlüsselter Daten ohne Kenntnis deren Inhalts erlauben. Der Klartext wäre also in der Cloud zu keinem Zeitpunkt vorhanden und die Schlüssel verblieben beim Anwender. Bis zur kommerziellen Verfügbarkeit dieses Verfahrens wird es aber vermutlich noch einige Zeit dauern.

Das Risiko eines Datenverlusts ist zwar recht gering, aber dennoch real, da viele Cloud-Dienste keine Mechanismen für Back-up und Restore der Anwenderdaten außerhalb der Cloud bereitstellen. Auch ist jeder Cloud-Service grundsätzlich von der Verfügbarkeit des Netzes und der Verfügbarkeit der Infrastruktur abhängig. Ein praktisches Beispiel für diese Risiken haben wir beim Ausfall der Amazon EC2 im April 2011 bereits erlebt.

TENDENZ ZUR ENTEIGNUNG DER NUTZER

Im privaten Bereich, wo Cloud-Anwendungen besonders durch den Smartphone-Boom getrieben werden, scheint mir neben meist mangelhaftem Umgang mit personenbezogenen Daten eine Tendenz zur Enteignung der Nutzer an den von ihnen erzeugten Inhalten um sich zu greifen. Immer mehr Apps sammeln Daten der Benutzer, die sie nicht nur zuweilen zweckfremd einsetzen, sondern auch in Summe nicht wieder an den erfassenden Nutzer herausgeben, wodurch dieser vom jeweiligen Anbieter abhängig wird. Eine Trennung vom Anbieter – oder die Einstellung des Dienstes – führt dann unweigerlich zum vollständigen Verlust dieser Inhalte.

Ein Modetrend scheint mir auch die Kopplung von Geräten an eine Cloud-Anwendung zu sein. Hier verliert man in einem solchen Fall nicht nur die mühsam gesammelten Informationen, sondern das Gerät ist plötzlich nutzlos, obwohl es technisch einwandfrei funktioniert. Die Enteignung erstreckt sich nun also schon auf die genutzten Gerätschaften. Aus dieser Erkenntnis heraus sind im Open-Source-Bereich Projekte wie Owncloud entstanden, die es ermöglichen, Cloud-Dienste auf eigener Hardware unter eigener Kontrolle zu hosten und der Abhängigkeit von Anbietern zu entgehen.

Eine sinnvolle Anwendung ist die Sicherung wichtiger Daten in der Cloud, da die Daten hier vor Elementargefahren geschützt sind. Voraussetzung ist allerdings die vorherige Verschlüsselung auf Anwenderseite mit verifizierbar guten Verschlüsselungsverfahren und geheimen Schlüsseln, die nur der Anwender hält. Die meisten Cloud-Speicher-Dienste erfüllen diese Voraussetzung nicht. Immerhin kann man sich mit einer separaten Verschlüsselung vor dem Hochladen behelfen.

MAXIMALE TRANSPARENZ

Der Business Marketplace der Telekom bündelt Cloud-Anwendungen verschiedener Anbieter in einem Portal. Insbesondere kleine und mittelständische Kunden können hier Software nutzen, ohne sie auf eigenen Rechnern installieren und betreiben zu müssen. Wie es um den Datenschutz im Cloud-Computing-Portal steht, erklärt Dr. Claus-Dieter Ulmer, Konzernbeauftragter für den Datenschutz bei der Deutschen Telekom.

Der Business Marketplace bietet qualitätsgeprüfte Software aus der Cloud.

Nicht erst seit den Enthüllungen von Edward Snowden fürchten insbesondere kleine und mittlere Unternehmen die Risiken des Cloud-Computings. Laut einer Studie aus dem Frühjahr 2013 – also einige Wochen vor der NSA-Affäre – stehen aufgrund von Sicherheitsbedenken drei Viertel der IT-Verantwortlichen, die bis dato noch keine Cloud-Lösungen eingesetzt haben, diesen Themen skeptisch gegenüber. Trotzdem hält laut einer weiteren Umfrage des Information Technology Observatory (EITO) mehr als jede zweite Firma die Einführung oder Weiterentwicklung von Cloud-Computing für wichtig oder sehr wichtig. Für den Hightechverband BITKOM hat Cloud-Computing sogar Vorteile unter Sicherheitsaspekten, da nur wenige Unternehmen ihre Daten annähernd so gut sichern könnten, wie ein spezialisierter Cloud-Anbieter.

VERTRAUEN IN DIE CLOUD STÄRKEN

Die Cloud-Anbieter haben die wichtige Aufgabe, die Nutzer ausführlich und transparent über Datensicherheit und Datenschutz zu informieren. Auffallend ist aber, dass in der Diskussion um Cloud-Computing die Themen Datenschutz und Datensicherheit gern in einen Topf geworfen werden. Auch wenn die beiden Seiten der Risikomedaille zusammenspielen, birgt der Blick auf den Datenschutz im Cloud-Computing andere Facetten. Während Datensicherheit sehr stark auf Sicherheitstechnik fußt, beruht der Datenschutz auf dem Umgang mit den Daten und den jeweiligen Datenschutzgesetzen in den Ländern der Cloud-Betreiber und Software-as-a-Service-Anbieter. Diese Gesetzgebung ist unterschiedlich streng – selbst innerhalb der Europäischen Union.

Ein wichtiges Ziel des Anbieters von Cloud-Computing-Lösungen besteht im Aufbau von Vertrauen gegenüber dem Nutzer – sowohl bei Endkunden als auch bei Firmen. Oftmals sind die Vertragsbedingungen und Gesetzesgrundlagen jedoch für Nichtjuristen kaum zu durchschauen. Gerade für kleinere Firmen ohne Rechtsabteilung geht die Bewertung der Datenschutzaspekte eines Cloud-Angebots mit hohem Aufwand einher.

Die Telekom ermöglicht insbesondere kleinen und mittelständischen Unternehmen im Business Marketplace den Zugang zu einer Vielzahl von Geschäftsanwendungen aus der Cloud. Um den Interessenten der einzelnen Anwendungen der Telekom Partner maximale Transparenz in Bezug auf Datenschutzfragen zu bieten, stehen Informationen über den Datenschutz neben der Kurzbeschreibung der Lösung offen zur Verfügung. Die Datenschutzaspekte sind einfach und verständlich beschrieben und durch besondere Symbole gekennzeichnet.

DEUTSCHE DATENSCHUTZSTANDARDS

Zu jeder Applikation ist genau angegeben, in welchem Land der Anbieter die Daten speichert und wer die Software betreibt. So unterscheidet die Telekom bezüglich der Datenspeicherung zwischen den Standorten Deutschland, Europäische Union und Schweiz sowie außerhalb der Europäischen Union und der Schweiz. Der Betrieb der Software erfolgt je nach Angebot in einem deutschen Rechenzentrum der Telekom und unterliegt damit den hohen Sicherheitsstandards der Telekom. Oder der Anbieter betreibt die Software selbst, nutzt dafür aber die Infrastruktur der Telekom, für die dann wiederum die Telekom Standards gelten. Schließlich kann es auch sein, dass der Anbieter selbst die Software im eigenen Rechenzentrum betreibt. Dann überprüft die Telekom die Sicherheitsstandards regelmäßig auf Grundlage der vereinbarten Anforderungen.

Zusätzlich bestehen zum Datenschutz unterschiedliche Verträge mit den Partnern, die im Wesentlichen von deren Firmenstandort abhängen. So müssen die Anbieter mit deutschem Standort vertraglich eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz (BDSG) garantieren. Verarbeitet die Lösung eines Partners keine personenbezogenen Daten, besteht auch kein spezifischer Vertrag zur Auftragsdatenverarbeitung.

KONTROLLRECHTE FÜR NUTZER

Weiterhin kommen bei einigen Anbietern außerdem sogenannte Standardvertragsklauseln zum Einsatz, die von der europäischen Kommission freigegeben sind. Nutzer einzelner Cloud-Software im Business Marketplace haben auch Kontrollrechte, die es ihnen grundsätzlich erlauben, Kontrollen zur Einhaltung der Vereinbarungen selbst durchzuführen oder durch Dritte ausführen zu lassen. Kontrollen sind nur dann nicht erforderlich, wenn keine personenbezogenen Daten verarbeitet werden.

Mit den umfangreichen und möglichst einfach beschriebenen Datenschutz- und Datensicherheitsinformationen im Business Marketplace zeigt die Telekom, wie man über Transparenz Vertrauen gegenüber Cloud-Computing aufbauen kann. Diese Transparenz ist Teil des offensiven Umgangs mit allen datenschutzrechtlichen Aspekten des Produkt- und Serviceangebots im Konzern.

NEUAUFLAGE DATEN-SCHUTZRATGEBER

Die Telekom Datenschützer haben ihren Ratgeber für sicheres Surfen im Internet aktualisiert und neu herausgegeben.

Überall lauern Gefahren in der digitalen Welt. Oftmals tappen Nutzer ohne es zu wissen in Fallen. Dabei lassen sich schon mit ein paar Sicherheitsvorkehrungen viele Risiken in den Griff bekommen. Wie das geht, zeigt der Ratgeber „Surfen in der digitalen Welt“, der sich unter www.telekom.com/datenschutz als pdf-Dokument kostenlos runterladen lässt.

Der Ratgeber zeigt, wie man Passwörter richtig gestalten sollte, damit sie nicht zu knacken sind. Auch ungesicherte WLAN-Router sind Einfallstore für Betrüger. Im Vorbeifahren auf der Straße scannen sie, welche privaten WLANs nicht richtig abgesichert sind und laden dann über die drahtlose Verbindung verbotene Dateien aus dem Netz. Das kann Ärger mit dem Gesetzgeber geben, denn der verpflichtet Besitzer von WLAN-Zugängen dazu, sie mit Passwörtern zu schützen.

Mit Phishing versuchen Kriminelle an Passwörter oder PIN- und TAN-Daten zu kommen. Dafür schicken sie gefälschte E-Mails an tausende von Empfängern oder manipulieren Internetseiten. Geben Online-Banking-Nutzer auf solchen gefälschten Seiten ihre Kontodaten samt Passwort ein, können die Betrüger unter Umständen Geld an unbekannte Kontoinhaber überweisen oder Überweisungen unbemerkt umleiten. Der Ratgeber gibt Tipps, wie man sich gegen solche Phishing-Angriffe schützen kann.

Auch Smartphones stellen ein Sicherheitsrisiko dar. Wer sicher mobil im Netz surfen will, sollte seine Software regelmäßig updaten und den Zugriff auf das Smartphone mit einem Passwort schützen. Gefahr lauert auch durch permanent aktivierte Bluetooth- und WLAN-Verbindungen. Kriminelle können sich so in das System einhacken. Wer sein Smartphone beruflich nutzt, sollte auch keine sensiblen Daten auf seinem Gerät speichern.

STATUS-REPORT DATENSCHUTZ

Auch 2013 hat die Deutsche Telekom wieder eine Reihe von Datenschutzmaßnahmen konkret umgesetzt.

TECHNISCHER FEHLER

Im Internetvertriebsportal für Geschäftskunden wurde durch einen Kundenhinweis ein technischer Fehler an einem Link entdeckt. Dieser Fehler konnte dazu führen, dass den Kunden bei Abschluss eines Neukundenvertrages die Vertragsunterlagen eines anderen Geschäftskunden angezeigt wurden. Betroffen waren dabei unter anderem die Kontoverbindungen der Firmen und persönliche Daten der Firmeninhaber wie Geburtsdatum und Ausweisnummer.

Der Fehler trat nur unter bestimmten Bedingungen auf und kam nur bei Kunden zum Tragen, die ihre Auftragsbestätigung per Link abgerufen und nicht die parallel per Mail verschickte, korrekte Bestätigung genutzt haben. Daher ist nicht feststellbar, wie viele Kunden tatsächlich betroffen waren. Vorsorglich hat die Deutsche Telekom alle 2.107 möglichen Betroffenen angeschrieben. Darüber hinaus informierte die Telekom die Aufsichtsbehörden.

FALSCHE ZUGANGSDATEN

Die Telekom hat bei einer Systemumstellung rund 120 Geschäftskunden versehentlich für ein Administrationsportal einen falschen Aktivierungslink per E-Mail zugestellt. Die Plattform, über die die Anwender Internet-Domains verwalten, wurde daher vorsorglich kurzzeitig vom Netz genommen, bis der Fehler behoben war. Die Telekom informierte die betroffenen Kunden.

28 Anwender des neuen Administrationsportals haben den falschen Aktivierungslink tatsächlich genutzt. In den anderen Fällen wurde dieser also nicht verwendet. Der Fehler wurde innerhalb von wenigen Stunden bemerkt, worauf die Telekom die Plattform vorübergehend gesperrt hat, um eine missbräuchliche Nutzung zu verhindern. Ein Schaden ist nicht entstanden. Der Datenfehler wurde identifiziert und umgehend behoben.

Auslöser waren durch einen Systemfehler falsch zugeordnete E-Mails. Bereits vor der Systemumstellung hatte die Telekom die Portalnutzer gebeten, E-Mail-Adressen zu hinterlegen bzw. diese zu verifizieren um sicherzustellen, dass nur die berechtigten Anwender die Aktivierungsmail erhalten. Bei der dazu erforderlichen Übertragung der E-Mail-Adressen wurden durch einen Systemfehler beim Datenexport indes Daten vertauscht.

FEHLER BEI IT-MIGRATION

Bei der Vorbereitung der Migration eines IT-Systems stellte sich heraus: Statt ausschließlich anonymisierter Daten enthält es auch personenbezogene Informationen von Mitarbeitern. Das System wurde gestoppt, der Betriebsrat informiert. Die Mitarbeiter wurden am 26. August 2013 informiert.

AUFTRÄGE AUF PAKETEN

Im Juni 2013 wurden in einem Telekom Partner Shop Kundenaufträge an Hardwareverpackungen im Ladengeschäft befestigt, um diese für die Kunden zu reservieren. Der Bearbeitungsfehler wurde umgehend behoben und die Partner erneut über den Datenschutz geschult.

Weitere Infos unter:
http://www.telekom.com/verantwortung/datenschutz/42942

KONTROLLE GEWÜNSCHT

Aufsichtsrat Dr. Bernhard Walter leitet die Arbeit der Prüfungsausschüsse von Telekom und Daimler. Der ehemalige Sprecher des Vorstands der Dresdner Bank erklärt, welche Aufgaben das Gremium erfüllt und warum Datenschutz und Datensicherheit dabei eine besondere Rolle spielen.

Der Prüfungsausschuss der Telekom überwacht die Wirksamkeit der internen Kontroll-, Risikomanagement- und Revisionssysteme.

Viele denken allein an Themen der Rechnungslegung, wenn es um die Arbeit des Prüfungsausschusses geht. Weshalb stehen aber auch der Datenschutz und die Datensicherheit auf Ihrer Agenda?
Dr. Bernhard Walter: Ohne Zweifel beinhaltet ein Kernbereich unserer Arbeit, die Prozesse der Rechnungslegung zu überwachen und das Vorgehen bei der Abschlussprüfung im Auge zu haben. Da die Aufgaben eine hohe Außenwirkung besitzen, ist es durchaus verständlich, dass manch einer die Arbeit des Prüfungsausschusses damit gleichsetzt. Tatsächlich reichen unsere Aufgaben aber viel weiter. Insbesondere überwachen wir die Wirksamkeit der internen Kontroll-, Risikomanagement- und Revisionssysteme. Mit der Prüfarbeit kontrollieren wir, ob die Telekom alle relevanten rechtlichen Vorschriften und internen Richtlinien einhält. Bei diesen Compliancechecks spielen die Bestimmungen des Datenschutzes und der Datensicherheit eine wesentliche Rolle.

Aus welchem Grund?
Dr. Bernhard Walter: Datenschutz und Datensicherheit sind unmittelbar mit dem Geschäftsmodell der Deutschen Telekom verbunden. Weltweit vertrauen uns Millionen von Kunden ihre Daten an. Vielfach haben wir es dabei mit hochsensiblen Inhalten zu tun – sowohl im Privat- als auch im Geschäftskundenbereich. Hinzu kommen die nicht minder schützenswerten Daten unserer 230.000 Mitarbeiterinnen und Mitarbeiter. Um das Vertrauen zu rechtfertigen, das Kunden und Mitarbeiter in uns setzen, behandeln wir Themen des Datenschutzes und der Datensicherheit als Teil der Compliance und des Risikomanagements.

Was kann der Prüfungsausschuss bei diesen Aufgaben leisten?
Dr. Bernhard Walter: Die Themen Datenschutz und Datensicherheit werden regelmäßig im Prüfungsausschuss berichtet. Unsere Sitzungen finden quartalsweise statt. In einer zusätzlichen Sondersitzung beschäftigen wir uns intensiv mit den Risikokontrollsystemen des Konzerns und untersuchen dabei, ob die Anforderungen aus Datenschutz und Datensicherheit angemessen Berücksichtigung finden.

Sie gehören dem Aufsichtsrat seit 1999 an und leiten die Arbeit des Prüfungsausschusses seit fünf Jahren. Sicherlich können Sie sich noch gut an den Datenschutzskandal erinnern. Was hat sich aus Ihrer Sicht seither geändert?
Dr. Bernhard Walter: Da der Prüfungsausschuss die Aufarbeitung intensiv begleitet hat, sind mir die Vorfälle tatsächlich noch sehr präsent. Im Vergleich zur damaligen Situation hat sich die Stellung des Datenschutzes im Unternehmen deutlich verbessert. Seit 2008 gibt es ein eigenes Vorstandsressort für Datenschutz, Recht und Compliance. Zur Durchsetzung seiner Strategien und Policies ist es mit umfassenden Informations- und Kontrollrechten ausgestattet. Zudem wurde ein umfangreiches Maßnahmenpaket für einen verbesserten Datenschutz und eine erhöhte Datensicherheit realisiert. Darüber hinaus haben wir mit dem Datenschutzbeirat ein externes Gremium eingesetzt, in dem Experten aus Forschung, Politik, Wirtschaft und Gesellschaft die Telekom beraten. Das hat sich hervorragend bewährt. Zusätzliche Transparenz schaffen wir durch die Kooperation mit Behörden und nicht zuletzt auch durch den jährlichen Bericht zu Datenschutz und Datensicherheit.

ZUR PERSON

Dr. h. c. Bernhard Walter
(1942) gehörte seit 1987 dem Vorstand der Dresdner Bank an, von 1998 bis Mai 2000 als dessen Sprecher. Dr. Walter bekleidet mehrere Aufsichtsratsmandate bei namhaften deutschen Unternehmen, darunter die Deutsche Telekom AG, sowie weitere Mandate, und ist Vorsitzender des Stiftungsrates der Stiftung Frauenkirche Dresden.

KRITISCHE BEGLEITER

Der Datenschutzbeirat der Deutschen Telekom berät den Vorstand und fördert den Austausch mit führenden Experten und Persönlichkeiten aus Politik, Lehre, Wirtschaft sowie Nichtregierungsorganisationen zu aktuellen, datenschutz- und datensicherheitsrelevanten Herausforderungen. Das Themenfeld des Datenschutzbeirats ist umfangreich. Er befasst sich mit Geschäftsmodellen und -prozessen im Hinblick auf den Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit ergriffener Maßnahmen. Weitere Themen betreffen internationale Aspekte des Datenschutzes sowie die Implikationen neuer gesetzlicher Regelungen.

Auch die Beurteilung von allgemeinen Datenschutz- und Datensicherheitsmaßnahmen bei der Telekom sowie die Erarbeitung von Vorschlägen und Empfehlungen an Vorstand und Aufsichtsrat zu entsprechenden Fragen gehören zu den Aufgaben des Beirats. Der Vorstand kann den Datenschutzbeirat zudem um die Bewertung von datenschutzrelevanten Prozessen im Konzern bitten. Weiterhin greift der Beirat eigenständig Datenschutz- und Datensicherheitsthemen auf und erarbeitet passende Vorschläge oder Empfehlungen für den Vorstand der Telekom.

Im Jahr 2013 kam der Datenschutzbeirat zu fünf Sitzungen zusammen. Wichtige Themen umfassten die Bewertung von Datenschutz- und Datensicherheitsaspekten neuer Cloud-Anwendungen ebenso wie die Entwicklung neuer Sicherheitsprodukte des Konzerns. Der Beirat befasste sich zudem mit mobilen Bezahldiensten und Lösungen zum elektronischen Fahrtenbuch.

Ferner beriet der Beirat über Big Data und informierte sich über die Ergebnisse des Basisdatenschutzaudits und das erreichte Datenschutzniveau im Konzern.

DIE AKTUELLEN MITGLIEDER DES DATENSCHUTZBEIRATS:

Wolfgang Bosbach
CDU, MdB und Vorsitzender des Innenausschusses des Deutschen Bundestages

Peter Franck
Mitglied des Vorstands Chaos Computer Club (CCC)

Professor Dr. Hansjörg Geiger
Honorarprofessor für Verfassungsrecht an der Goethe-Universität in Frankfurt am Main, von 1998 bis 2005 Staatssekretär im Bundesjustizministerium, Präsident des Bundesamts für Verfassungsschutz und des Bundesnachrichtendienstes a. D.

Professor Peter Gola
Ehrenvorsitzender 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 (TUM)

Dr. Konstantin von Notz,
Bündnis 90/Die Grünen, MdB, stellvertretender Fraktionsvorsitzender, Sprecher für Netzpolitik, Mitglied des Innenausschusses

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)

Dr. Gerhard Schäfer
Vorsitzender Richter am Bundesgerichtshof (BGH) i. R.

Lothar Schröder
Vorsitzender des Datenschutzbeirats, Mitglied des ver.di-Bundesvorstands und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom AG, Mitglied der Enquetekommission „Internet und digitale Gesellschaft“

Halina Wawzyniak
DIE LINKE, MdB, Obfrau im Ausschuss für Recht und Verbraucherschutz

Professor Dr. Peter Wedde
Professor für Arbeitsrecht und Recht in der Informationsgesellschaft an der Fachhochschule Frankfurt am Main, Direktor der Europäischen Akademie der Arbeit in der Universität Frankfurt am Main

EXPERTENAUSTAUSCH ÜBER DATENSCHUTZ

Klaus-Dieter Hommel, Vorsitzender des Datenschutzbeirats der Deutschen Bahn, und Lothar Schröder, Vorsitzender des Datenschutzbeirats und stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom, hatten die Idee: Einen Tag lang informierten sich Datenschutz- und Datensicherheitsvertreter der beiden Unternehmen gegenseitig über ihre Arbeit. Dabei hoben während des ganztägigen Austauschs in Berlin Gerd Becht als Vorstand Compliance, Datenschutz, Recht und Konzernsicherheit der Deutschen Bahn sowie Dr. Thomas Kremer als Vorstand Datenschutz, Recht und Compliance der Deutschen Telekom die Bedeutung der Datenschutzbeiräte hervor. Als unabhängige Gremien beraten sie den Vorstand in datenschutzrelevanten Fragen. Darüber hinaus geben die Beiräte Empfehlungen zur zukunftsfähigen Weiterentwicklung des Datenschutzes. Dabei bringen sie wichtige Impulse für die Arbeit der beiden Konzerne ein. Die Deutsche Bahn stellte in Berlin unter anderem eine Management-Selbstauditierungslösung vor und diskutierte über die Videoüberwachung in Bahnhöfen. Die Deutsche Telekom informierte über die datenschutz- und datensicherheitskonforme Entwicklung von internationalen Cloud-Computing-Lösungen sowie ihren jährlichen Transparenzbericht, den Bericht zu Datenschutz und Datensicherheit.

DRANBLEIBEN, VERTRAUEN AUSBAUEN

Das Verhalten der Geheimdienste hat an den Fundamenten des demokratischen Gemeinwesens gerüttelt, sagt Lothar Schröder, stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom. Dies hat auch die Integrität der Telekommunikation und der digitalen Medien infrage gestellt.

2013 war für den Datenschutz ein belastendes Jahr. Der Skandal rund um die Abhörpraktiken der NSA sowie des britischen Geheimdienstes GCHQ hat grundlegende Fragen zum Fundament unseres demokratischen Gemeinwesens aufgeworfen – und nicht zuletzt die Integrität der Telekommunikation und der digitalen Medien infrage gestellt. Denn das Big-Brother-Verhalten von einigen Sicherheitsbehörden konterkariert jede Anstrengung der Telekommunikationsunternehmen, die ihnen zugänglichen persönlichen Daten vertraulich zu behandeln. Wenn wir befürchten müssen, dass immer jemand mithört und ausspäht, leidet die Vertrauenswürdigkeit massiv.

DEUTLICHE SIGNALE AUSSENDEN

Führen Geheimdienste unsere Arbeit ad absurdum? Die zwölf Mitglieder des Datenschutzbeirats der Telekom setzen sich seit Jahren erfolgreich für den Schutz der Kunden- und Mitarbeiterdaten ein. Für sie ist das von anderen Staaten legitimierte Abgreifen von Kommunikationsdaten jeglicher Art bis hin zum Abhören der Handyverbindungen von politischen Verbündeten nicht hinnehmbar und da weiß sich der Datenschutzbeirat mit dem Vorstand der Telekom einig.

Das Abgreifen schafft ein Misstrauensklima, gegen das wir uns mit aller Macht wehren müssen. Deswegen müssen wir deutliche Signale aussenden, dass wir uns dies nicht bieten lassen wollen. Dafür bleibt die Arbeit eines Datenschutzbeirats bedeutsam – als starkes Zeichen dafür, wie mächtig die Persönlichkeitsrechte für die Deutsche Telekom sind.

René Obermann hat die gesellschaftsverändernde Wirkung des flächendeckenden Eingriffs in die Kommunikation ganz im Sinne des Datenschutzbeirats in bemerkenswerter Weise öffentlich problematisiert. Das braucht kontinuierliche Unterstützung. Wir dürfen das Thema Persönlichkeitsrechte nicht so behandeln wie das Thema „eigene Gesundheit“. Da merken wir meist erst dann, wenn sie nicht vorhanden ist, welche Bedeutung sie besitzt.

ZU FEHLERN STEHEN UND HANDELN

Wie gewichtig konsequentes Handeln in Sachen Datenschutz für einen Konzern sein kann, hat 2013 ein Regelverstoß bei der Verarbeitung von Mitarbeiterdaten gezeigt. Der unabhängige Konzerndatenschutz konnte einen schwerwiegenden Fehler in dem zentralen Personalverarbeitungssystem aufdecken. Der Vorstand hat daraufhin schnell und entschieden reagiert. Wurden solche Verstöße in früheren Jahren von den Unternehmen gern unter den Teppich gekehrt, hat der Telekom Vorstand den Vorfall öffentlich gemacht und sich bei den Beschäftigten entschuldigt.

Auf Initiative des Vorstands und der Mitarbeitervertretung wurde mit Unterstützung durch den Datenschutzbeirat eine externe Untersuchung des Vorfalls veranlasst. Diese Untersuchung soll herausfinden, wer welche Daten dieses Systems in welcher Form widerrechtlich verarbeitet hat, wie es zu dem Vorfall kommen konnte und wer dafür Verantwortung trägt. Nur mit schonungsloser Aufklärung können solche Vorgänge in der Zukunft vermieden werden. Die Art des Regelverstoßes zeigt, dass die Bedeutung des Themas Datenschutz noch nicht bis in die letzten Bereiche vorgedrungen ist, wenngleich die Prozesse der Selbstheilung zu funktionieren scheinen.

Trotzdem brauchen wir in Deutschland ein eigenständiges Datenschutzgesetz. Denn viele allgemeine Bedingungen des Datenschutzes sind nicht auf den Beschäftigtendatenschutz anwendbar und ein um den Beschäftigtendatenschutz erweitertes allgemeines Datenschutzgesetz würde das Gesetz zu kompliziert machen.

EINFACH UND DURCHSCHAUBAR

Wir brauchen ein durchschaubares Beschäftigtendatenschutzgesetz, welches das besondere Abhängigkeitsverhältnis der Arbeitnehmer zu den Arbeitgebern berücksichtigt und Sanktionsmechanismen enthält. Betriebe, die nicht sensibel mit den Daten ihrer Belegschaft umgehen, müssen sanktioniert werden können. Wir brauchen zudem noch mehr Mitbestimmungsrechte der Datenschutzbeauftragten und Betriebsräte sowie Immunitätsschutz für die Funktionsträger im Datenschutz und der Betriebsverfassung.

Zum Kerngeschäft der Telekom gehört es, vertrauliche persönliche Kommunikation zu ermöglichen. Wenn dieses Kernelement verletzt wird, entweder durch eigenes oder fremdes Handeln, dann hat der Konzern ein Problem. Die Telekom hat aus den Fehlern der Vergangenheit gelernt und sich einen Vertrauensvorsprung gegenüber den Wettbewerbern erarbeitet. Dies gilt es nun in den kommenden Jahren auszubauen.

ZUR PERSON

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)“.

„WIR BRAUCHEN WELTWEIT EINHEITLICHE, HOHE DATENSCHUTZSTANDARDS“

Staatlich verordnete Datenspionage unter Partnern ist indiskutabel. Darüber sind sich **Wolfgang Ischinger**, Vorsitzender der Münchner Sicherheitskonferenz, und **Timotheus Höttges**, Vorstandsvorsitzender der Deutschen Telekom, einig. Die größere Gefahr in der digitalen Gesellschaft geht von professionellen Cyberkriminellen aus.

Herr Ischinger, wie hat sich aus Ihrer Sicht als Vorsitzender der Münchner Sicherheitskonferenz das Thema Cybersicherheit 2013 entwickelt?
Wolfgang Ischinger: Wir haben 2011 erstmals das Thema in München auf die Agenda genommen. 2012 folgte dann der erste Cyber Security Summit in Bonn, da das Thema rasant Fahrt aufgenommen hatte. Und mittlerweile gehört Cybersicherheit zu einem der wichtigsten Themen in der internationalen sicherheitspolitischen Debatte.

Wobei die NSA-Affäre dazu einen großen Beitrag geleistet hat.
Wolfgang Ischinger: Ich denke, dass nun jeder verstanden hat, wie zentral das Thema Cyber- und Datensicherheit für uns alle ist. Aber die Bedrohungen waren auch schon vor der NSA-Affäre exponentiell gestiegen. Nur haben es viele Unternehmen und Regierungen noch nicht so ganz ernst genommen. Insofern haben uns PRISM und Tempora sogar einen Gefallen getan: Die Aufmerksamkeit für unser Interesse an Chancen und Risiken der digitalen Welt ist deutlich gestiegen. Dies spielt eine ganz wichtige Rolle.

Timotheus Höttges: Wobei ich ergänzen will, dass wir nicht zwei unterschiedliche Bedrohungsszenarien in einen Topf werfen dürfen. Da ist mir nach den Enthüllungen zu viel vermischt worden. Was wir über die Praktiken der Geheimdienste erfahren haben, lässt sich nicht direkt vergleichen mit den Aktivitäten der professionellen Cyberkriminellen. Die Geheimdienste haben uns mit ihren Abhörmaßnahmen bewusst gemacht, wie wichtig Datenschutz für jeden von uns ist: ob als Privatperson, in der Wirtschaft oder als Politiker. Den amerikanischen Diensten geht es primär darum, mehr Sicherheit zu erreichen. Ob hier die Balance stimmt – in der Abwägung mit dem Recht auf Privatsphäre – ist Gegenstand der aktuellen Debatte. Bei Cyberkriminellen geht es nicht um Balance. Sie wollen direkten Schaden verursachen. Wie wir inzwischen wissen, mit großem Erfolg.

Wolfgang Ischinger, Leiter der Münchner Sicherheitskonferenz.

ZU DEN PERSONEN

Wolfgang Ischinger
ist Generalbevollmächtigter der Allianz SE und hat im Mai 2008 den Vorsitz der Münchner Sicherheitskonferenz übernommen. Der Jurist und Völkerrechtler war zuvor von 1975 bis 2008 im Auswärtigen Amt der Bundesrepublik Deutschland tätig. Unter anderem war Ischinger deutscher Botschafter in Washington, D.C., und London sowie zuvor Staatssekretär des Auswärtigen Amtes. Er leitete die deutschen Delegationen bei den Bosnien-Friedensverhandlungen in Dayton und war zudem Repräsentant der Europäischen Union in den Troikaverhandlungen über den Status des Kosovo.

> „BEI CYBERKRIMINELLEN GEHT ES NICHT UM BALANCE. SIE WOLLEN DIREKTEN SCHADEN VERURSACHEN.“

Timotheus Höttges, Vorstandsvorsitzender der Deutschen Telekom.

Welche Folgen hat denn die offensichtlich übergründliche Arbeit der Geheimdienste?
Wolfgang Ischinger: Ein erheblicher Vertrauensverlust, großes Misstrauen gegenüber dem Staat, aber auch gegenüber vielen Unternehmen. Die Menschen fragen, wem und was sie noch im digitalen Wilden Westen trauen können. Dem Internet, der eigenen Regierung, der Wirtschaft? Jeder scheint machen zu können, was er will. Und dies über alle Grenzen hinweg und recht hemmungslos. Daher ist es eine eminent wichtige Aufgabe, das verloren gegangene Vertrauen wiederzugewinnen. Die digitale Welt bietet auch großartige Chancen.

Wie soll das in einer global vernetzten Welt funktionieren, wenn einzelne Staaten oder Unternehmen nur ihre eigenen Interessen verfolgen?
Wolfgang Ischinger: Es gibt Beispiele, dass sich die Staatengemeinschaft auch bei komplizierten Themen auf gemeinsame Regeln verständigen kann. Das ist sicher kein einfacher Prozess, aber wir brauchen dringend weltweite, staatenübergreifende Regelwerke und vertrauensbildende Maßnahmen. Beispielsweise könnte ein transatlantisches No-Spy-Abkommen vertrauensbildend wirken, wobei ein europäisches No-Spy-Abkommen ein wichtiger Schritt davor wäre. Dieser EU-Standard könnte dann Ausgangsbasis sein für den Dialog mit Washington und anderen Partnern. Hier hätten wir sicher auch Verbündete in großen US-Firmen, deren Geschäftsmodell nahezu vollständig auf dem Internet beruht und deren Erfolg auf dem Spiel steht. Hier hat durch die NSA ein Umdenken der Konsumenten begonnen. Eine entsprechende Kampagne wurde ja jüngst von sehr namhaften US-Unternehmen lanciert.

Aber schon die Ratifizierung der EU-Datenschutzgrundverordnung zieht sich mittlerweile über Jahre hin. Das macht nicht gerade Hoffnung.
Wolfgang Ischinger: Die Datenschutzgrundverordnung wird

Timotheus Höttges
ist seit dem 1. Januar 2014 Vorstandsvorsitzender der Deutschen Telekom AG. Zuvor war der studierte Betriebswirt seit 2009 Vorstand Finanzen und Controlling. Von Dezember 2006 bis 2009 leitete er im Konzernvorstand den Bereich T-Home. In dieser Funktion zeichnete er für das Festnetz- und Breitbandgeschäft sowie den integrierten Vertrieb und Service in Deutschland verantwortlich. Seine berufliche Laufbahn bei der Telekom begann 2000 als Geschäftsführer Finanzen und Controlling und später Vorsitzender der Geschäftsführung T-Mobile Deutschland. 2005 war Höttges im Vorstand der T-Mobile International für das Europageschäft zuständig.

durch die NSA-Affäre den letzten Schub erhalten. Denn nur auf der Grundlage einer klaren EU-Linie ist ein sinnvoller transatlantischer oder globaler Dialog über eine Art „Code of Conduct“ vorstellbar.

Wenn sich die Politik einigt, hätte dies nicht unbedingt Auswirkungen auf die Wirtschaft?
Timotheus Höttges: Datenschutz ist nicht nur ein Thema der Politik, sondern auch der Unternehmen. Jeder muss vor der eigenen Haustür kehren. Auch Unternehmen sammeln Daten. Oft ist das notwendig, manchmal ist es fragwürdig. Insgesamt trägt die Wirtschaft Verantwortung dafür, mehr für IT-Sicherheit und Datenschutz zu tun und möglichst alle Hintertürchen zu schließen, um Missbrauch zu verhindern.

Aber Datenaffären in den Unternehmen tragen nicht gerade dazu bei, das Vertrauen in die Wirtschaft zu verbessern.
Timotheus Höttges: Manche angebliche Affäre ist Ausdruck der neuen Transparenz beim Thema Datensicherheit. Diese Transparenz auch unter den Unternehmen ist aber wichtig, um auf Angriffe schneller und effizienter reagieren zu können. Die Telekom hat immer für Offenheit geworben und ich bin froh, dass wir an der Stelle jetzt deutlich weiter sind. Wir haben es mit einer immer professionelleren Cyberkriminalität zu tun, da rollt ein regelrechter Tsunami auf uns zu. Das Bewusstsein für die Wucht, mit der dieses Thema auf uns zurollt, hat in der Wirtschaft insgesamt lange gefehlt. Eine weitere Facette ist natürlich der Umgang der Unternehmen selbst mit den Daten der Kunden. Dafür gibt es in Deutschland klare Regeln, die wir ohne Wenn und Aber einhalten müssen.

Welche Lehren zieht die Deutsche Telekom aus dieser Cyberwar-Gemengelage aus dem Jahr 2013?
Timotheus Höttges: Wir haben nach unserer eigenen Abhöraffäre schon vor mehr als fünf Jahren deutliche Konsequenzen gezogen. Seitdem drehen wir unseren Konzern weltweit durch die Datenschutzmangel. Dafür haben wir nicht nur als erstes deutsches Unternehmen einen eigenen Vorstand für Datenschutz berufen, sondern sukzessive alle Abteilungen, Standorte oder Anwendungen auf Datenschutzaspekte hin geprüft und wo nötig, angepasst. Wir sind heute beim Datenschutz Vorbild für andere. Aber natürlich sind wir nicht unfehlbar. Und auch wir müssen uns ständig neu auf die Bedrohungen aus dem Cyberspace einstellen.

Glauben Sie, dass die Kunden zukünftig Produkte vertrauenswürdiger Unternehmen bevorzugen werden?
Timotheus Höttges: Das Risikobewusstsein der Menschen wächst. Sie werden sich daher zunehmend von Angeboten und Unternehmen abwenden, denen sie nicht vertrauen. So, wie die Menschen bei einem Auto erwarten, dass die Bremsen funktionieren und sie sicher unterwegs sind, erwarten sie von uns, dass wir die uns anvertrauten Daten schützen und sie sich sicher im Netz bewegen können. Die Telekom hat sehr früh die Bedeutung der Sicherheit im Netz erkannt und mit Produkten reagiert, zum Beispiel der Cloud made in Germany. Ich möchte diesen Wettbewerbsvorteil weiter für die Telekom ausbauen.

Sehen Sie die Diskussionen rund um Cybersicherheit und Datenschutz also als Chance für die Telekom?
Timotheus Höttges: Ich sehe sie nicht nur als Chance für die Telekom, sondern auch für den Standort Deutschland und die europäische Wirtschaft. Wir verfügen über große Kompetenz in Cybersicherheitsfragen und können uns als Marktführer für Cybersicherheitstechnologie etablieren. Mit unseren hohen Sicherheitsstandards und unserem Datenschutzverständnis können wir uns mit eigenen High-End-Sicherheitsprodukten im Wettbewerb zu US-amerikanischen und chinesischen Hard- und Softwareprodukten positionieren. Jedenfalls bekommt die Telekom seit dem Sommer 2013 enorm viele Anfragen von Unternehmen, die wissen wollen, was wir für sie in Sachen Cybersicherheit tun können.

Munich Security Conference MSC
Münchner Sicherheitskonferenz

Im Laufe der vergangenen fünf Jahrzehnte hat sich die Münchner Sicherheitskonferenz (MSC) zu einem zentralen jährlichen Treffen der internationalen „strategic community“ entwickelt. Seit ihrer Gründung dient die MSC als unabhängiges Forum, das sich der Förderung friedlicher Konfliktlösung und internationaler Kooperation beim Umgang mit gegenwärtigen und zukünftigen sicherheitspolitischen Herausforderungen widmet. Im Mittelpunkt steht dabei insbesondere die transatlantische Partnerschaft. Weitere Infos:
www.securityconference.de

Sie profitieren von dem Wissen, das wir in den vergangenen Jahren konsequent aufgebaut haben.

Bei allem Verständnis für die Empörung über die Arbeit der Geheimdienste: War das, was Edward Snowden aufgedeckt hat, für Sie eine Überraschung?
Wolfgang Ischinger: Dass man so weit gehen würde, im eigenen Land Regierungschefs von Verbündeten abzuhören, hätte ich nicht für möglich gehalten. Aber einige Reaktionen in Deutschland fand ich auch etwas blauäugig. Es war schon immer so, dass man vertrauliche oder gar geheime Informationen nicht über offene Telefone kommunizieren sollte. Wir sollten also nicht allein die USA einfach an den Pranger stellen, sondern uns fragen, wie wir uns schützen können. Warum nutzen wir diese technischen Möglichkeiten nicht stärker? Warum verschlüsseln wir unsere Kommunikation nicht konsequenter? Warum gehen wir immer noch recht naiv mit den Neuen Medien um? Hier besteht offenbar ein großer Nachhol- und Aufklärungsbedarf.

www.cybersecuritysummit.de/current
Experten aus Wirtschaft, Politik und Wissenschaft diskutieren über Kriminalität, Wirtschaftsspionage und Sabotage im Netz.

FÜR MEHR CYBERSICHERHEIT

Zum zweiten Mal haben die Münchner Sicherheitskonferenz und die Deutsche Telekom den Cyber Security Summit am 11. November 2013 in Bonn ausgerichtet. Damit setzten sie die im Herbst 2012 begonnenen Gipfelgespräche von Topmanagern und Spitzenpolitikern fort.

Neben Keynotes von EU-Kommissarin Neelie Kroes und der damaligen Bundesjustizministerin Sabine Leutheusser-Schnarrenberger konnten die Teilnehmer der hochrangig besetzten Paneldiskussion zum Thema „Cybersecurity, Datenschutz und internationale Beziehungen“ folgen. Redner waren der ehemalige israelische Ministerpräsident Ehud Barak, der frühere Cybersicherheitsberater von US-Präsident Barack Obama, Howard A. Schmidt, Mag. Johanna Mikl-Leitner, österreichische Bundesministerin für Inneres, sowie der stellvertretende Generalsekretär der OECD, Yves Leterme.

2013 konzentrierte sich der Cyber Security Summit auf die Themenfelder Spionage und Sabotage, den Ordnungsrahmen auf nationaler und internationaler Ebene sowie auf konkrete Sicherheitslösungen. In einem Abschlusskommuniqué haben die Teilnehmer Vorschläge zusammengetragen, um die richtigen Weichen für mehr Sicherheit im Cyberraum zu stellen. So gilt es, das öffentliche Bewusstsein für die Gefahren im Cyberraum zu stärken und Unternehmen, Behörden sowie private Endnutzer für die Risiken, die Prävention und für die Chancen der Cybersicherheit zu sensibilisieren.

Cybersicherheitspolitik bedeutet auch Wirtschaftspolitik, denn ein hohes Datenschutz- und Datensicherheitsniveau ist ein Standortvorteil in der globalisierten Welt. Digitale Geschäftsmodelle funktionieren nur, wenn Kunden sich auf die Sicherheit ihrer Daten verlassen können. Die Wirtschaft hat daher ein vitales Eigeninteresse, IT-Systeme durch technische und prozedurale Maßnahmen so sicher wie möglich zu machen. Ein Mehr an Sicherheit ist wichtiges Differenzierungsmerkmal, Wettbewerbsvorteil und Verkaufsargument zugleich. Der weitere Aufbau von Kompetenzen in der Cybersicherheit wird sich auch wirtschaftlich auszahlen, denn er schafft technolgische Souveränität und trägt zur Profilierung als Vertrauensexporteur von High-End-Cybersicherheitsprodukten bei.

Der Cyberraum braucht ein verbindliches, ausgewogenes Rahmenwerk, in dem legitime Sicherheitsbedürfnisse und elementare Grundrechte ausbalanciert sind und in dem der Grundgedanke der Freiheit im Netz erhalten bleibt. Nur eine übergreifende Zusammenarbeit verspricht Erfolg. Ein Bewusstsein für die Risiken setzt eine möglichst umfassende und globale Abbildung von Ursprung, Qualität und Quantität von Angriffen voraus. Ein solches Lagebild müssen Staat, Wirtschaft und Gesellschaft immer wieder aufs Neue durch freiwilligen, internationalen und branchenübergreifenden Austausch erstellen.

Der dritte Cyber Security Summit findet am 3. November 2014 in Bonn statt.

HASE UND IGEL

Die Telekom steckt viel Energie, Aufwand und Personal in den Datenschutz und die Datensicherheit. Dabei kämpft sie gegen eine zunehmende Zahl von Angreifern und Schadprogrammen.

70

Mitarbeiter stellen in der Datenschutzabteilung der Telekom täglich IT-Systeme, Prozesse und neue Produkte auf den Prüfstand.

3

Milliarden Virenangriffe verzeichneten 2013 die Rechner von Kaspersky-Nutzern.

80

Prozent der Internetnutzer in Deutschland hielten Ende November 2013 ihre persönlichen Daten im Internet generell für unsicher.

5

gezielte Angriffe täglich registriert das komplett verschlüsselte deutsche Regierungsnetz.

7.222

Anfragen von Kunden und Mitarbeitern an datenschutz@telekom.de hat der Konzerndatenschutz im Jahr 2013 beantwortet.

250.000

Identitäten haben Hacker beim Onlinebanking laut BSI in nur drei Monaten gestohlen.

70

E-Mails mit Malware gehen laut BSI durchschnittlich pro Stunde im deutschen Regierungsnetz ein.

170

nationale Datenschutzkoordinatoren sorgen an den deutschen Standorten des Telekom Konzerns dafür, dass überall das gleiche Datenschutzniveau besteht.

800.000

Hackerangriffe pro Tag verzeichneten die Honeypots der Telekom in Spitzenzeiten.

100

Datenschutzbeauftragte vertreten in den nationalen und internationalen Telekom Standorten die Interessen des zentralen Konzern-Datenschutzbeauftragten.

42,5 Mio.

Euro schätzt das Bundeskriminalamt den Schaden, den Cyberkriminelle 2012 allein in Deutschland verursacht haben.

70

Prozent der Unternehmen wollten 2013 mehr Geld in ihre IT-Sicherheit investieren und damit ihre Sicherheitsstatus verbessern.

9

Prozent der Internetnutzer in Deutschland nutzten laut BITKOM Ende 2013 für ihre E-Mails eine Verschlüsselungssoftware.

580

Teilnehmer verzeichnete Mitte Dezember 2013 die „Allianz für Cybersicherheit". Dies entspricht einer Verdopplung der Mitgliederzahl innerhalb von sechs Monaten.

42

nationale und internationale Audits führten externe und interne zertifizierte Prüfer innerhalb der Telekom durch.

180

Honeypots der Telekom lockten im Jahr 2013 Hacker an, um aus den Daten neue Erkenntnisse über Cyberangriffe zu gewinnen.

16.762

Mal allein in einer Maiwoche informierte das Abuse-Team die Telekom Kunden über Schadsoftware auf ihren Computern.

1.446

Sicherheitswarnungen und Handlungsempfehlungen veröffentlichte das CERT der Telekom im Jahr 2013 intern.

45

Prozent der Unternehmen haben keinen Notfallplan für IT-Sicherheitsvorfälle.

300

Tage bleibt die Hälfte aller Hackerangriffe auf Unternehmen unbemerkt.

130

Beschäftigte arbeiten bei der Telekom allein in der internen Datensicherheitsabteilung.

200.000

neue Schadprogramme verbreiten Hacker laut Kaspersky Lab pro Tag über das Internet.

WECKRUF FÜR UNTERNEHMEN

Die NSA-Affäre hat für Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), einen positiven Nebeneffekt. Waren die Themen Ausspähung und Spionage bisher in Unternehmen nur schwer zu vermitteln, haben die Geheimdienstaktivitäten zu einem Umdenken geführt.

Die Enthüllungen von Edward Snowden haben das bisher eher auf Expertenebene diskutierte Fachthema IT-Sicherheit in nur wenigen Wochen in den Mittelpunkt des allgemeinen Interesses gerückt. Die Bereitschaft wächst, mehr in IT-Sicherheit zu investieren. Cybersicherheit und der Schutz vor digitaler Wirtschaftsspionage gehören nun zu den regelmäßigen Themen in Vorstands- und Geschäftsführungsrunden. Das ist gut so! Denn Quantität und Qualität von Cyberangriffen haben im Jahr 2013 noch einmal stark zugenommen. Pro Tag entstehen rund 40.000 neue Schadprogrammvarianten. Auch wenn die Betroffenen davon wenig zu wissen scheinen: Die Hälfte aller erfolgreichen Hackerangriffe auf einen privat genutzten PC bleibt mehr als 300 Tage unbemerkt. Es wird also höchste Zeit, sich intensiv mit dem Thema zu beschäftigen und angemessene Schutzmaßnahmen zu treffen.

Trotz der vielen Meldungen über erfolgte und erfolgreiche Cyberangriffe haben wir bis heute kein eindeutiges Lagebild zur Cyberkriminalität. Wir müssen allerdings von einer massiven Bedrohung der Wirtschaft ausgehen. Dies zeigt eine einfache Analyse: Ein gängiges Betriebssystem oder andere vergleichbar komplexe Software besteht in der Regel aus Programmzeilen in zweistelliger Millionenhöhe. Davon sind laut Expertenmeinung etwa zwei Promille fehlerhaft oder verfügen über Sicherheitslücken. Das wären bei zehn Millionen Programmierzeilen 20.000 offene Tore für Hacker.

Cyberkriminalität hat sich zu einem internationalen arbeitsteilig organisierten Markt entwickelt, auf dem professionelle Hacker ihre Dienste anbieten. Sie bauen Werkzeuge auf Bestellung, die kriminelle Vertriebsorganisationen in den Markt bringen und die Käufer illegal einsetzen. Attraktiv sind diese Dienste unter anderem, weil das Entdeckungsrisiko sehr gering ist. Strafbar ist nur der Einsatz der Werkzeuge. Entwickler und Vermarkter dürfen ihre Services unter den Augen der Polizei offen im Internet oder auf Messen anbieten. Hinzu kommt, dass Hacking ein lukratives Geschäft darstellt. Mit überschaubarem finanziellen Einsatz lassen sich viele Ziele gleichzeitig angreifen.

GRENZÜBERSCHREITENDER DIALOG

Wichtig ist jedoch, angesichts dieser Entwicklungen nicht in blinden Aktionismus zu verfallen. Schon wenige strukturierte Maßnahmen können das Risiko eines erfolgreichen Hackerangriffs verringern. Das fängt bei der Prävention an, die sich über Firewall und Virenscanner hinaus deutlich verbessern lässt. Dabei spielt es eine entscheidende Rolle, IT-Sicherheit nicht nur einmalig zur Chefsache zu machen, sondern in nachhaltige Prozesse umzusetzen. IT-Sicherheit beschreibt eine dauerhafte Führungsaufgabe, an deren Anfang ein Konzept steht, in dem die „Kronjuwelen“ der eigenen Firma definiert sind, sowie die Methoden, mit denen sich diese schützen lassen. Das BSI stellt hierfür eine breite Palette von Empfehlungen und Angeboten zur Hilfestellung zur Verfügung und zertifiziert dazu nicht nur Produkte, sondern auch vertrauenswürdige IT-Sicherheitsdienstleister. Schon der breitere Einsatz von Kryptografie könnte viele Sicherheitsprobleme lösen. Es gibt seit vielen Jahren Verschlüsselungsverfahren, die, richtig implementiert, einen hohen Schutz bieten. Doch bislang fehlte die Nachfrage in der Industrie.

Dass sich „IT-Security by Design“ mit entsprechenden Investitionen in IT-Sicherheit lohnt, zeigt das deutsche Regierungsnetz, an das alle Ministerien und die meisten Bundesbehörden angeschlossen sind. Es hat einen sehr hohen Sicherheitsstandard, der grundsätzlich auch gegen die Angriffe von Nachrichtendiensten ausgelegt ist. Es gibt bis heute keine Hinweise auf erfolgreiche Hackerattacken, obwohl monatlich bis zu 3.000 Standardangriffe sowie täglich etwa vier bis fünf gezielte Angriffe zu verzeichnen sind.

In Deutschland fühlt sich der Staat verpflichtet, auch für die Privatanwender die Integrität und Vertrauenswürdigkeit bei der Nutzung von Informationstechnik zu schützen. Deshalb haben wir mit dem neuen elektronischen Personalausweis den Schutz von elektronischen Identitäten enorm verbessert. Darüber hinaus hat die Bundesregierung mit dem De-Mail-Gesetz einen Rechtsrahmen geschaffen, wie Bürger, Unternehmen und Behörden sicher online miteinander kommunizieren können.

Auch die Diskussion über das IT-Sicherheitsgesetz sollten wir wieder aufgreifen. Einige Wirtschaftsverbände hatten Bedenken bezüglich der Meldepflicht von Cyberangriffen. Dabei haben wir im Augenblick eine Situation, in der sehr viele Angriffe stattfinden, wir aber nur von wenigen erfahren. Eine erfolgreiche Abwehr der zunehmenden Risiken durch Wirtschaftsspionage und Hackerangriffe lässt sich aber auf Dauer nur bewerkstelligen, wenn man einen Überblick über die aktuelle Lage hat, aus deren Kenntnis man Schutzmechanismen entwickeln kann.
Die Verbesserung der Cybersicherheit ist eine Gemeinschaftsaufgabe von Staat, Wirtschaft und Wissenschaft. Wir müssen daher auch zu einem grenzüberschreitenden Dialog kommen. Daher ist beispielsweise eine gemeinsame europäische Datenschutzgrundverordnung so wichtig, um verlorengegangenes Vertrauen wiederzugewinnen.

ZUR PERSON

Michael Hange
ist seit Oktober 2009 Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Der Diplom-Mathematiker war zuvor im BSI unter anderem als Leiter der Abteilung Beratung und Unterstützung tätig. Hier bildete die Entwicklung des IT-Grundschutzhandbuches zum Aufbau eines wirksamen IT-Sicherheitsmanagements in Verwaltung und Wirtschaft einen thematischen Arbeitsschwerpunkt.

KUNDENDATEN SIND UNSER HÖCHSTES GUT

Der Fahrzeugspezialist Carglass legt höchsten Wert auf Sicherheit und Datenschutz. Wenn er Daten auslagert, dann nur an einen Anbieter aus Deutschland.

Wenn Steinschlag die Windschutzscheibe eines Autos beschädigt, dann wenden sich viele Kfz-Besitzer an das Unternehmen Carglass. Der Autoglasexperte verschließt Scheibenschäden mit einem patentierten durchsichtigen Spezialharz. Da Carglass Partner der meisten führenden Kfz-Versicherer ist, kann ein versicherter Kunde seinen Regulierungsanspruch an Carglass abtreten. Der Glasspezialist rechnet dann direkt mit den Versichereungen ab. „Um die Reparatur abwickeln zu können", sagt Frank Müller, IT-Manager bei Carglass, „vertrauen uns die Kfz-Versicherer ihre Kundendaten an. Für uns ist es also enorm wichtig, hohe Sicherheitsstandards zu erfüllen und den Datenschutz zu gewährleisten. Die Kundendaten sind unser höchstes Gut."

Carglass beschäftigt einen Vollzeitdatenschutzbeauftragten, der die Verträge mit den Versicherern prüft und dafür sorgt, dass Kundendaten intern datenschutzkonform verarbeitet werden (Rechtsgrundlage oder Opt-in-Verfahren). Für die IT-Sicherheit ist ein Team mit über 20 Mitarbeitern unter der Leitung von Frank Müller zuständig. Um seine Aufgabe zu erfüllen, informiert er sich regelmäßig über neue Technologien und Tools. Seiner Meinung nach ist das erforderlich, um mit den Entwicklungen im Cyberbereich Schritt zu halten. „Cyberangriffe", berichtet er, „verändern sich so schnell, dass wir immer mit den neuesten Sicherheitskonzepten arbeiten müssen, um den IT-Betrieb zu schützen."

SICHERHEITSKONZEPT IN DREI STUFEN

Bei der IT-Sicherheit setzt Müller auf ein dreistufiges Konzept aus Next Generation Firewall, demilitarisierter Zone (DMZ) und regelmäßigen Penetrationstests durch professionelle Anbieter. „Unsere Firewall", erklärt der IT-Manager, „inspiziert den Datenverkehr, damit sich Schadsoftware nicht als eine andere Applikation ausgeben kann und ins Netzwerk gelangt. Dies ist ein neues Next-Generation-Firewall-Konzept, welches auf Applikationskontrolle anstatt der herkömmlichen Portkontrolle basiert." Die Penetrationstests dienen dazu, etwaige Sicherheitsschwachstellen aufzudecken und zu schließen, bevor ein Hacker sie ausnutzen kann. „Wir tun unser Bestes, um uns und die Daten unserer Kunden zu schützen", so Frank Müller. Dass die Arbeit nicht vergebens ist, zeigen zahlreiche Angriffe auf die Infrastruktur von Carglass, die registriert werden. Dabei stellt Frank Müller fest, dass insbesondere Botnetzattacken zugenommen haben. „Angriffe", berichtet er, „erfolgen immer häufiger von gekaperten Rechnern, ohne dass deren Besitzer davon Kenntnis haben."

Auf physikalischer Seite sorgen zwei Rechenzentren mit einer Loopverbindung der Telekom für hochverfügbare Systeme. „Die Loopverbindung leitet unseren Datenverkehr redundant über getrennte Leitungen an zwei unterschiedliche Vermittlungsstellen der Telekom." Selbst für den äußerst unwahrscheinlichen Fall, dass eine Vermittlungsstelle ausfällt, bleiben die Systeme des Fahrzeugspezialisten intakt. Neben dem Betrieb eigener Rechenzentren nutzt Carglass die Private Cloud. Dafür kommt nur das Angebot eines deutschen Hostingpartners infrage, der die Daten garantiert ausschließlich in deutschen Rechenzentren speichert und verarbeitet. Und zwar mit einem redundanten Back-up, das ebenfalls in Deutschland liegt. „Die Telekom", betont Müller, „bietet uns hier ein in Deutschland gehostetes Netzwerk und gewährleistet, dass unsere Daten nicht das Land verlassen."

VONEINANDER LERNEN

Um auf dem Laufenden zu bleiben, besucht der IT-Manager Anwendertreffen und Sprecherkreise. „Als Telekom Dialogkunde", erzählt der Sicherheitsspezialist, „werden wir regelmäßig zu Treffen eingeladen, bei denen wir in Ausschüssen und Arbeitsgruppen darüber diskutieren, wie man zukünftige Probleme am besten löst." Neue Erkenntnisse behält der IT-Manager nicht für sich. Carglass ist eine Tochtergesellschaft des weltweit tätigen Belron Konzerns, der in 36 Ländern vertreten ist. Eine internationale Konzernrichtlinie definiert die Anforderungen an IT-Sicherheit und Datenschutz. Die IT-Leiter der weltweiten Gesellschaften tauschen regelmäßig Best Practices miteinander aus, um sich gegenseitig zu unterstützen und voneinander zu lernen. „Einmal im Monat", schildert Müller, „bereitet einer von uns einen Vortrag als Webinar vor." Die anderen IT-Verantwortlichen wählen sich ein und stellen Fragen zu der Lösung, die der Kollege vorstellt. „Das ist ein äußerst wichtiger Austausch für uns, denn wir stehen alle vor den gleichen Herausforderungen."

Die IT-Leiter von Carglass tauschen sich regelmäßig über Sicherheitsthemen aus.

WETTLAUF MIT DEN SPAMMERN

99,9 Prozent des gesamten E-Mail-Aufkommens an die Mailsysteme von T-Online.de und Telekom bestehen aus Spam. Plattformschutz und Spamfilter weisen diese Nachrichten meist sofort ab. Dennoch versuchen Spammer, die Schutzbarrieren zu umgehen.

Trotz des effektiven Schutzes haben Spamversender mitunter Erfolg – bei Angriff und Verteidigung handelt es sich letztlich um ein Hase-und-Igel-Spiel. Am leichtesten lässt sich Spam vermeiden, wenn die Adresse des Empfängers nicht bekannt ist. Kombinationen aus Vor- und Nachnamen sowie Pseudonyme testen Spammer allerdings immer wieder. Und selbst nicht zu erratende Adressen können in die Fänge eines Spamversenders gelangen, etwa wenn ein Virus den Rechner eines Bekannten infiziert oder Hacker Kundendaten von den Servern eines Unternehmens stehlen.

PROVISION FÜR BETRÜGER

Gestohlene E-Mail-Adressen verwenden Betrüger beispielsweise, um sie bei Gewinnspielen und Newslettern unbescholtener Unternehmen einzutragen. Als „Affiliates" erhalten die Betrüger für jede Adresse eine Provision. Affiliatemarketing ist eine internetbasierte Vertriebslösung, bei der zumeist ein kommerzieller Anbieter (Merchant) seine Vertriebspartner (Affiliates) erfolgsorientiert entlohnt.

Ein Spamfilter unterscheidet jedoch leider nicht zwischen gewollten und ungewollten (Spam)-Newslettern. So gelangen mitunter unerwünschte Werbenachrichten in das Postfach eines gut vor Spam geschützten Nutzers.

Noch schwieriger ist die Klassifikation von Spam, wenn die Merkmale der ungewollten Nachrichten variieren. Damit der „Fingerabdruck" einer E-Mail als Spam klassifiziert werden kann, muss zuerst bekannt sein, dass es sich dabei um Spam handelt. Der Empfänger einer entsprechenden Nachricht verbessert den Filter, indem er sie in seinem E-Mail-Center als Spam meldet.

Einige Versender variieren ihre Nachrichten so geschickt, dass jede Variation den Fingerabdruckprozess erneut durchlaufen muss. Der Nutzer hat dann leicht den Eindruck, dass er immer und immer wieder die gleiche Spammail meldet.

GESUNDE SKEPSIS

Spamfilter haben zudem Probleme mit Nachrichten, wenn der Versender Betreff und Inhalt aus wenigen zufälligen Zeichen zusammenstellt. Der Filter klassifiziert die Nachricht als sauber, da sie zu wenig Inhalt enthält. Spammer versenden solche Nachrichten, um Adressen zu validieren: Wird eine vermeintlich fehlerhafte E-Mail zugestellt, erhält der Versender damit die Information, dass die Empfängeradresse existiert.

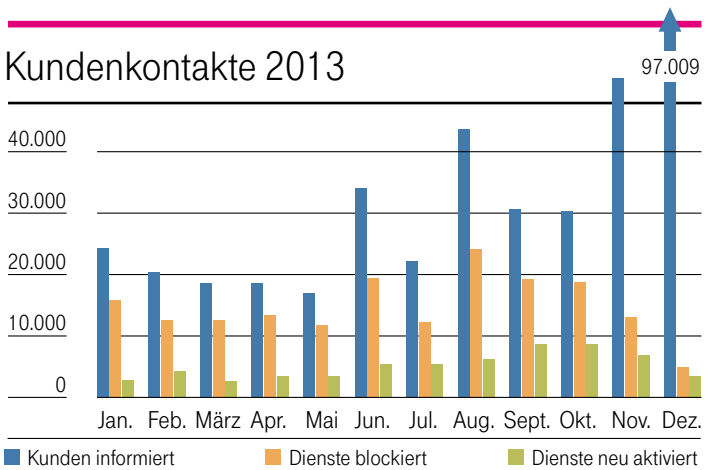
Spammer verkaufen solche Adressen im kriminellen Untergrund. Die Käufer wollen sichergehen, dass sie nicht für frei erfundene, sondern nur für existierende Adressen zahlen. Da Nutzer heute häufiger E-Mail-Adressen wechseln als früher, möchten die kriminellen Käufer garantiert aktuelle Adressen erwerben, die sie als Empfänger von Spam-, Phishing- und Virenmails nutzen können.

INFORMIERT SEIN

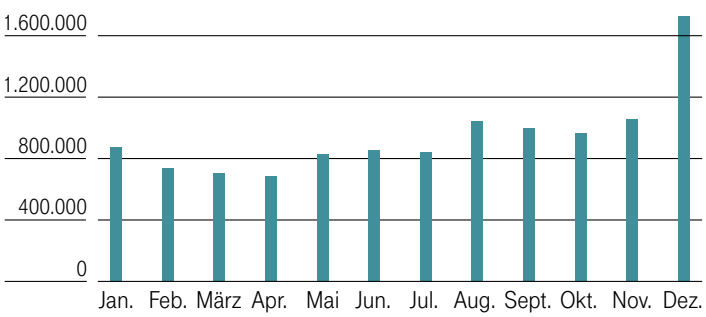
Besonders dreiste Kriminelle wollen Viren und Trojaner auf den Rechnern ihrer Opfer platzieren. Sie hoffen darauf, dass Nutzer, die ahnungslos auf einen Link oder Anhang klicken, auch ihre Kontoauszüge nicht besonders genau prüfen. Deshalb bleibt die Verbesserung der Spamabwehr ein steter Wettlauf mit den Spammern – aber auch ein Kampf um Aufmerksamkeit und gesunde Skepsis der Nutzer: Auch wenn jemand noch niemals unerwartete E-Mails erhalten hat oder sein Spamschutz die meisten unerwünschten Nachrichten fernhält, kann das jederzeit geschehen. Und dann ist es wichtig, informiert und nicht zu sorglos zu sein.

DAS ABUSE-TEAM IST ANSPRECHPARTNER FÜR JEDEN, DER DEN MISSBRAUCH VON INTERNETDIENSTEN DER DEUTSCHEN TELEKOM MELDEN WILL. 2013 GINGEN DIE SICHERHEITSEXPERTEN MEHR ALS EINER MILLION HINWEISE NACH.

Kundenkontakte 2013



Eingegangene Hinweise 2013



IT-SICHERHEIT IST CHEFSACHE

Unternehmen betrachten IT-Sicherheit nach wie vor als kostspielige Pflichtausgabe, sagt **Thomas Tschersich**, IT-Sicherheitschef der Telekom. Dabei würde ein IT-Ausfall ihre Existenz bedrohen.

Die Unternehmen drehen im harten Wettbewerb permanent an der Kostenschraube. Die IT-Sicherheit kann dabei keine Ausnahme machen.
Thomas Tschersich: Auf der Agenda der CIOs stehen auf Platz eins bis vier Kostensenkungs- und Sparmaßnahmen. Natürlich ist es dann schwer, Mehrausgaben für die IT-Sicherheit durchzusetzen. Damit gehen die Unternehmen jedoch ein hohes Risiko ein. Wenn die IT aufgrund von Cyberangriffen ganz ausfallen würde, wäre heute nach wenigen Tagen die Existenz vieler Firmen bedroht. Das wird gern vergessen.

Ist das nicht etwas übertrieben?
Thomas Tschersich: Schon vor Jahren gab es Aussagen, dass eine Bank ohne IT nach wenigen Tagen pleite wäre. Aber selbst kleinere Unternehmen hängen heute von ihrer IT und dem Internet ab. Wer sein Geschäft zum Beispiel weitgehend online abwickelt, für den spielt die Verfügbarkeit seines Onlineshops eine wesentliche Rolle. Ein erfolgreicher Denial-of-Service-Angriff, bei dem die Internetseite lahmgelegt wird, reicht dann aus, das Geschäft zum Erliegen zu bringen. DoS-Angriffe mit bis zu 60-facher Bandbreite gegenüber bisherigen Attacken markieren einen neuen Trend.

Die Ausgaben für IT-Sicherheit müssen also deutlich steigen?
Thomas Tschersich: Nicht zwangsläufig. Aber IT-Sicherheit muss als strategisches Thema gesehen werden. Nur dann bekommt es die verdiente Aufmerksamkeit des Managements und ist Teil der unternehmerischen Verantwortung. In den Risikobewertungen der Unternehmen befinden sich bis heute meist nur die klassischen Risiken wie Kredit- oder Produktionsausfälle. Cyberangriffe hat niemand auf dem Schirm. Hier handeln viele noch nach dem rheinischen Motto „Et hätt noch immer joot jejange – auf hochdeutsch: Es hat noch immer irgendwie funktioniert.

Wie hoch sind denn die Risiken?
Thomas Tschersich: Nur 13 Prozent der Firmen sind dem Cyber Security Report 2013 zufolge noch nie aus dem Internet angegriffen worden. 62 Prozent der Entscheider aus Politik und Wirtschaft sehen im Datenbetrug im Internet und 57 Prozent in Computerviren ein sehr großes Risiko für die Bevölkerung in Deutschland. Die Gefahren werden also erkannt, doch gehandelt wird zu wenig – besonders bei den kleinen und mittleren Unternehmen.

Wie muss man also als Unternehmer mit dem Thema umgehen?
Thomas Tschersich: Sicherheit muss Chefsache sein. Das gilt ganz besonders für die kleinen und mittleren Unternehmen, die nicht über Sicherheitsexperten verfügen. Sie sind genauso wie die großen gefährdet. Aber um die IT – und damit auch um die Sicherheit – kümmert sich nebenbei der Sohn des Nachbarn oder ein interessierter Mitarbeiter, der sein Hobby in die Firma einbringt. Dadurch wird Sicherheit aber oft nicht zu Ende gedacht. Die Firewall und der Virenschutz allein greifen zu kurz. Ein simples Beispiel: Wenn ich meine Daten abends auf Bänder oder DVDs sichere, diese dann aber neben dem Server liegen lasse, reicht ein Einbruch oder ein Feuer aus und alles ist verloren. Das hat wenig mit einem Cyberrisiko zu tun, ist aber immer noch weit verbreitet.

Was kann ein kleines oder mittleres Unternehmen technisch kurzfristig tun?
Thomas Tschersich: Wer sich schützen will, muss unbedingt darauf achten, die neuesten Versionen von Virenschutz und Software auf allen Computern aufzuspielen. Das schließt etwa 90 Prozent aller Sicherheitslücken. Dann sollten Softwareupdates der Anbieter immer so schnell wie möglich durchgeführt werden. Oftmals schließen Updates bekannt gewordene Sicherheitslecks. Und wer sich vor Spionage und Abgreifen von Daten schützen will, sollte unbedingt seinen E-Mail-Verkehr verschlüsseln. Diese drei Maßnahmen kosten zum Beispiel wenig, helfen aber viel.

ZUR PERSON

Thomas Tschersich
ist Chef der technischen Sicherheit der Telekom. Der Elektrotechniker übernahm im Jahr 2000 die Leitung des Bereichs IT-Sicherheit und Informationsschutz. Seit dem Jahr 2001 ist er in zahlreichen beratenden Funktionen bei Bundes- und Landesministerien und Behörden zu technischen Sicherheitsanfragen tätig.

HACKER-TEAM DER TELEKOM

Neue Produkte oder Webauftritte der Telekom unterliegen schon in der Entwicklungs- und Produktionsphase strengen Sicherheitsvorgaben. Damit vor Marktstart wirklich keine Sicherheitslücken bleiben, sucht ein internes Hacker-Team nach versteckten Schlupflöchern.

Rund 30 Mitarbeiter der Telekom versuchen mit allen Mitteln der Hackerkunst Schwachstellen offenzulegen. Damit kommen sie Angriffen zuvor, die ansonsten kriminelle Hacker unternehmen würden. Ungefähr 200 geprüfte Produkte und Websites mussten 2013 die Tests überstehen. Meist lohnen sich die Angriffe: Obwohl detaillierte Anforderungen an die Datensicherheit die Entwicklung von Anfang an begleiten, findet das Hacker-Team im Durchschnitt zehn Schwachstellen pro Test. Der Unterschied zu den Kriminellen ist allerdings, dass die „guten" Hacker am geknackten Safe stehen bleiben und keinen Schaden anrichten.

Die Methoden des internen Hacker-Teams entsprechen denen der kriminellen Hacker. Dafür beobachten die Sicherheitsexperten den „Hackermarkt" permanent und schauen sich die Methoden der Angreifer ab. Die guten Hacker haben gegenüber den kriminellen einen Vorteil: Da sie schon im Vorfeld die kritischen Punkte der Systeme von innen kennen, können sie ihre Angriffe zielgerichteter durchführen. So entdecken sie selbst Schwachstellen, die mancher externe Hacker nicht finden könnte.

Welche neuen Lösungen die Angriffe der Sicherheitsexperten über sich ergehen lassen müssen, entscheidet die Sicherheitsbewertung. Unkritische Lösungen nimmt das Team nur auf besonderen Wunsch unter die Lupe. Zu den geprüften Systemen gehören auch Netzlösungen, Cloud-Anwendungen, interne Systeme, oder DSL-Router. Auch Produkte von Lieferanten müssen sich den Hackern stellen – zu ihrem Vorteil. Denn oft finden sich Lücken bei grundlegenden Angelegenheiten, zum Beispiel durch veraltete Softwarestände. Das nutzen auch kriminelle Hacker sehr häufig aus. Dann hätten sie leichtes Spiel und könnten mit einfachen technischen Mitteln großen Schaden anrichten.

Einmal jährlich wertet das Telekom Hacker-Team alle gefundenen Schwachstellen aus. Die wichtigsten Fehlerquellen fließen dann wieder in die strengen Sicherheitsvorgaben für Entwicklung und Produktion ein.

NICHTS VERGESSEN

Ein neues Workflowtool führt die Teams, die neue Produkte und Systeme für die Telekom entwickeln, strukturiert durch das Privacy-and-Security-Assessment-Verfahren.

Wenn die Mitarbeiter des Konzerns neue Produkte, Systeme oder Plattformen entwickeln, gewährleistet das Privacy-and-Security-Assessment(PSA)-Verfahren der Telekom ein adäquates Sicherheits- und Datenschutzniveau. Das PSA-Portal bildet den kompletten Workflow ab, von der Definition der Sicherheits- und Datenschutzanforderungen – also der Auswahl der relevanten Anforderungen –, über die Dokumentation der implementierten Lösungen und Maßnahmen bis hin zur Freigabe.

Das Tool bildet dafür die Rollen Projektleiter, systemverantwortlicher Sicherheitsexperte und Datenschutzberater ab. Es führt alle beteiligten Mitarbeiter online durch die relevanten Prozessschritte und dokumentiert zugleich den aktuellen Status des Projekts. Auf Knopfdruck geben sie das Projekt für ihre Kollegen aus den anderen Bereichen frei. Das schafft Sicherheit bei der Abarbeitung aller relevanten Anforderungen und ermöglicht, Sicherheit und Datenschutz effizient in Neuentwicklungen umzusetzen.

Ein weiterer Vorteil des webbasierten Projektwerkzeugs liegt in der medienbruchfreien Zusammenarbeit: Ein Wechsel zwischen Excel, PowerPoint und anderen Applikationen entfällt. Das gesamte Projekt wird über eine Onlineoberfläche verwaltet, dokumentiert und lässt sich bei Bedarf exportieren. Wird das neu entwickelte System zu einem späteren Zeitpunkt erweitert, lassen sich die gewählten Anforderungen der vorherigen Version auf das neue System anwenden.

PSA FÜR ALLE

Um international auf dem gleichen Ambitionsniveau zusammenarbeiten zu können, müssen alle Projekte dieselben Sicherheitsanforderungen erfüllen. Darum hat die Telekom ihr Privacy-and-Security-Assessment(PSA)-Verfahren 2011 in allen europäischen Landesgesellschaften ausgerollt. Der Bereich Datenschutz, Recht und Compliance (DRC) definierte 19 PSA-Kernanforderungen. Alle Gesellschaften spiegelten diese Anforderungen an ihren bestehenden Prozessen und ermittelten, ob Anpassungen erforderlich waren. Nun überprüft DRC, welche Fortschritte die Gesellschaften bei der Umsetzung des Verfahrens gemacht haben. Anschließend besuchen Spezialisten aus der Zentrale die Landeseinheiten, um sie bei Bedarf bei weiteren Prozessanpassungen zu unterstützen.

UNERLAUBTER ZUGRIFF NICHT MÖGLICH

Mit Verschlüsselungs- und Authentifizierungsmechanismen schützt die Deutsche Telekom vertrauliche Dokumente aus den Konzerngremien vor unerlaubtem Zugriff.

Wenn Vorstand, Aufsichtsrat, Datenschutzbeirat oder andere Gremien der Deutschen Telekom zusammenkommen, stehen viele wichtige Entscheidungen an. Vorlagen und Beschlüsse müssen unter Verschluss bleiben und dürfen nur autorisierten Personen zugänglich sein. Daher setzt die Telekom seit 2013 auf Onlinedokumentensafes für jedes Gremium, in denen alle Unterlagen wie Protokolle oder geheime Informationen vor unerlaubtem Zugriff geschützt sind.

Die Lösung registriert jeden Zugriff auf die gespeicherten Dokumente, so dass sich immer nachvollziehen lässt, wer welche Datei wie genutzt oder runtergeladen hat. Auch inhaltliche Änderungen werden stets protokolliert, so dass selbst durch autorisierte Personen keine unerkannten Manipulationen möglich sind.

Das Einloggen in den Datensafe erfolgt ähnlich dem Verfahren beim Onlinebanking. Die Gremiumsmitglieder erhalten nach Eingabe von Benutzername und Passwort per SMS eine Einmal-PIN, mit der sie den Zugang freischalten können. Sind sie Mitarbeiter der Telekom, können sie auch ihren elektronischen Unternehmensausweis in Form einer Smartcard einsetzen.

Zusätzlichen Schutz für besonders geheime Telefonate bieten zudem die unternehmensintern zur Verfügung stehenden Voice-over-IP-Telefone, welche die Sprache sicher verschlüsselt übertragen und daher nicht abgehört werden können – weder von innen noch von außen.

ZIELGERICHTET UND FRÜH ERKENNEN

Die Verwundbarkeit weltweit vernetzter Unternehmen nimmt zu. Mehr und mehr nehmen Industriespione und Cybersaboteure das Know-how und die Geschäftsabläufe ins Visier, die für die Wertschöpfung der Unternehmen unentbehrlich sind.

Wer seine Cyber-Detection- und Response-fähigkeiten dieser Bedrohungslage nicht anpasst, hinkt den komplexen und zielgerichteten Angriffen fortwährend hinterher. Um diese ebenso riskante wie frustrierende Verfolgerrolle zu überwinden, bedarf es eines Sicherheitsmanagements auf Basis von Erkenntnissen, das zielgerichtet Informationen verknüpft und in Echtzeit auswertbar macht. Ziel dieser proaktiven Vorgehensweise ist es, sich nicht nur gegen bekannte Angriffe zu schützen, sondern auch die noch unbekannten Angriffe zu erkennen und schnelle Gegenmaßnahmen einzuleiten.

Für die Umsetzung der Advanced-Cyber-Defense (ACD)-Dienste haben T-Systems und RSA ihre Kräfte gebündelt. Der „Intelligence-Driven Security"-Ansatz von RSA basiert darauf, dass sämtliche sicherheitsrelevanten Informationen aus Netzwerken und Anwendungen erfasst, zentral zusammengeführt und analysiert werden. Security wird zu einer Big-Data-Herausforderung. Die Kombination aus moderner IT-Sicherheitstechnik, Expertenwissen und Zugriff auf Datenquellen wie konzerneigene Frühwarnsysteme, ermöglicht den Aufbau dieser neuen Sicherheitssysteme.

Im Zentrum von ACD steht das Next Generation Security Operations Center (NG SOC). Hier tragen die Experten Informationen zu allen relevanten Angriffsszenarien zusammen. Nach innen gerichtet untersuchen die im NG SOC tätigen Sicherheitsexperten, welche Unternehmenswerte wie viel Schutz brauchen und an welchen Stellen die unterstützenden IT-/TK-Systeme angreifbar sind oder bereits angegriffen werden. Nach außen gerichtet klären die Experten die Motive, Methoden und Werkzeuge potenzieller Angreifer auf. Somit erkennen sie relevante Szenarien, noch bevor sie zum Einsatz kommen.

CYBER SECURITY REPORT 2013

Ein Fünftel aller vom Institut für Demoskopie Allensbach für den Cyber Security Report 2013 befragten Unternehmen muss sich täglich oder mehrmals in der Woche gegen Hackerangriffe wehren.

Das Risiko steigt offenbar mit der Unternehmensgröße. Von den Unternehmen mit mehr als 1.000 Mitarbeitern meldete ein Drittel mehrere Angriffe pro Woche. Unter den kleineren Unternehmen mit bis zu 100 Mitarbeitern verzeichneten 16 Prozent häufige Attacken. Gleichwohl nimmt das Thema IT-Sicherheit der Umfrage nach für nahezu alle Unternehmen (92 Prozent) einen hohen Stellenwert ein. Das spiegelt sich auch in den Investitionen wider: 35 Prozent der Entscheider berichten über deutlich, 41 Prozent über etwas gestiegene Ausgaben in diesem Bereich.

Auch das Risikobewusstsein der Führungskräfte ist größer geworden: Während vor einem Jahr rund 42 Prozent der Großunternehmen das Schadensrisiko durch einen Hackerangriff als groß oder sehr groß einstuften, sind es aktuell 53 Prozent. Dennoch fühlt sich die Mehrheit der Unternehmen (56 Prozent) so gut wie möglich auf drohende Gefahren vorbereitet. Rund 40 Prozent besitzen sogar eine umfassende Strategie zum Umgang mit Cybergefahren, 13 Prozent arbeiten daran. Allerdings setzen ebenfalls gut 40 Prozent nur auf Einzelmaßnahmen zum Sichern ihrer IT-Systeme und Firmendaten.

Für die Studie haben die Marktforscher im Auftrag von T-Systems insgesamt 221 Führungskräfte aus großen sowie 293 Entscheider aus mittleren Unternehmen befragt.

VON REAKTION ZU PROPHYLAXE

Das Deutsche Telekom CERT wehrt als schnelle Eingreiftruppe künftig Angriffe ab, bevor sie gefährlich werden. Dafür wertet das Team Daten aus fünf verschiedenen Quellen wie Firewalls oder Proxyservern aus.

Cyberkriminelle variieren ihre Angriffe ständig. Firewall, Proxyserver, Intrusion Prevention und andere klassische Sicherheitsmaßnahmen reichen nicht mehr aus, um mit modernen Angreifern Schritt zu halten. Das Deutsche Telekom CERT (Cyber Emergency Response Team) übernimmt daher zusätzlich präventive Aufgaben. Die Experten sollen Cyberkriminelle abwehren, bevor sie Schaden anrichten können.

„Schutzmaßnahmen wie eine Firewall“, sagt Bernd Eßer, Leiter des Deutsche Telekom CERT, „basieren auf definierten Regeln und greifen nur dann, wenn Angriffe bestimmten Kriterien entsprechen.“ Professionelle Hacker variieren jedoch ihre Methoden, um früher oder später erfolgreich zu sein. „Um diese nicht vorhersehbaren Angriffe frühzeitig abzuwehren“, erklärt Eßer, „werden wir künftig Daten aus fünf verschiedenen Quellen zusammenführen und auswerten.“

Um nicht vorhersehbare Angriffe frühzeitig abzuwehren, wertet das Telekom CERT Daten aus fünf verschiedenen Quellen aus.

MALWARE IDENTIFIZIEREN

Als Quellen dienen die Firewalls des Konzerns, die Intrusion-Prevention-Systeme (IPS), die Proxyserver, die Exchangeserver und die Antiviruslösung der Telekom. Die Firewalls protokollieren etwa, wenn ein Angreifer versucht, offene Ports zu finden, um in die Systeme der Telekom einzudringen. IPS stehen hinter den Firewalls und erkennen, wenn eine Schadsoftware wie ein Botclient das System eines Mitarbeiters infiziert hat. Über einen Bot steuern Hacker befallene Systeme aus der Ferne, lesen Daten aus und attackieren weitere Systeme, um sie zu sabotieren oder ebenfalls zu infizieren. Die IPS-Lösungen der Telekom lernen oder wissen, welche IP-Adressen die feindlichen Server verwenden.

Die Proxyserver der Telekom protokollieren, welche IP-Adresse aus dem Intranet mit welcher Website im Internet kommuniziert. Diese einfachen Protokolldaten werden zu wertvollen Informationsquellen, wenn das Forensik-Team des Konzerns die Schadsoftware in einem verseuchten E-Mail-Anhang identifiziert hat. Erhält ein Telekom Mitarbeiter eine E-Mail mit verdächtigem Anhang, leitet er sie an die IT-Forensiker weiter. Handelt es sich dabei um eine Malware, finden die Sicherheitsspezialisten heraus, auf welche URL sie zugreifen würde, wenn sie sich auf einem System installiert. Nun können sie die Protokolldaten des Proxyservers gezielt nach dieser URL durchsuchen, um Systeme ausfindig zu machen, auf denen sich diese Schadsoftware eingenistet hat. Ähnlich verfahren die Sicherheitsexperten mit den Logdaten der Exchangeserver, die für den Transport der E-Mails im Konzern zuständig sind. Wurde ein bösartiger E-Mail-Anhang identifiziert, suchen die CERT-Spezialisten gezielt nach weiteren E-Mails mit diesem Anhang und bereinigen sie direkt auf den Servern.

VIRUS IN QUARANTÄNE

Die Antiviruslösung der Telekom erkennt Schadsoftware selbstständig und verschiebt sie in Quarantäne. Anhand der entsprechenden Logdaten erkennen die Mitarbeiter des CERT, ob sich Infektionen in einem bestimmten Bereich häufen, weil dort ein Angriff stattfindet. Zudem analysieren die Forensiker der Telekom die vom Antivirusprogramm identifizierte Malware. Sie stellen fest, wie sie sich auf einem infizierten Rechner verhält. Daraufhin können sie gezielt nach Systemen suchen, die entsprechende Kriterien erfüllen sowie die Antivirussoftware modifizieren, damit sie befallene Rechner automatisch bereinigt. Das CERT der Telekom wird die Logdaten der Firewall und des Proxyservers künftig mit den Daten von Reputation Feeds abgleichen. So identifizieren die Teammitglieder IP-Adressen, die mit hoher Wahrscheinlichkeit bösartige Software hosten, ohne dass ein Beschäftigter verdächtige Mailanhänge melden muss.

US-amerikanische Unternehmen bedienen sich häufig eines Big-Data-Ansatzes, um gespeicherte Daten aus allen möglichen Logquellen im Falle eines vermuteten oder tatsächlichen Angriffs im großen Stil auszuwerten. In Europa ist das aus datenschutzrechtlichen Gründen nur eingeschränkt möglich. Darum setzen die Mitarbeiter des CERT auf jahrelange Erfahrung, wie Cyberkriminelle bei ihren Angriffen vorgehen und aus welchen Phasen ein Angriff besteht. Sie können Logquellen gezielt nach Indizien für diese Angriffe auswerten.

Da das CERT ausschließlich die Vorgehensweise externer Cyberkrimineller modelliert, ist das Verfahren datenschutzrechtlich unbedenklich, denn die Use Cases sind so gestaltet, dass sie den Anfangsverdacht eines kriminellen Vergehens begründen und damit dem CERT die weitere Auswertung erlauben. Die Telekom wird die neuen CERT-Leistungen ebenfalls als Managed Services für Industrieunternehmen anbieten.

HERZSTÜCK DER KONZERNSICHERHEIT

Schon der griechische Philosoph Aristoteles stellte fest: Das Ganze ist mehr als die Summe der Einzelteile. Ein Grund für die Sicherheitsbereiche der Telekom noch enger zusammenzuarbeiten.

Seit 2010 ist das Telekom Security Management durch die DQS, eine der führenden Gesellschaften für die Zertifizierung von Managementsystemen in Deutschland, gemäß ISO 27001 zertifiziert. Dies bescheinigt die Funktionsweise des Informationssicherheits-Managementsystems (ISMS) der zentralen Sicherheitsbereiche und bestätigt die hohe Qualität, kontinuierliche Weiterentwicklung und ganzheitliche, risikoorientierte Sicherheitsperspektive des Telekom Security Managements.

Die Zusammenführung der zentralen Sicherheitsfunktion im Vorstandsbereich Datenschutz, Recht und Compliance ist somit der nächste logische Schritt in der konsequenten Weiterentwicklung und Fortführung des Konvergenzgedankens über die virtuelle Zusammenarbeit hin zu einer noch stärker integrierten Sicherheitsorganisation. Ein klares Plus für den Konzern, denn damit wird die ganzheitliche Sicherheitsperspektive bei der Betrachtung und Reaktion auf die steigende Komplexität der Risikolage weiter verstärkt. Dies geschieht weiterhin in engem Schulterschluss mit dem Datenschutz.

SECURITY POLICIES 2.0

„Konkrete Inhalte, für jeden verständliche Formulierungen, die klare Verteilung von Zuständigkeiten, eindeutig definierte Ziele bestimmter Regeln und greifbare Konsequenzen für diejenigen, die sich nicht an die Policy halten." Dies sind für den Gartner-Analysten Les Stevens die entscheidenden Aspekte erfolgreicher Security Policies.

Aus diesen Gründen hat die Telekom auch 2013 weiter an den im Juni 2010 in Kraft gesetzten, zentral formulierten Konzernrichtlinien zur Sicherheit, den Security Policies, gefeilt. Nachdem das Regelungswerk sukzessive konzernweit und einheitlich eingeführt worden ist, fließen inzwischen noch stärker Vorschläge aus den deutschen und ausländischen Unternehmenseinheiten und Tochterunternehmen in die Policies ein. Mit den Security Policies 2.0 haben die Sicherheitsmanager die Vorgaben sprachlich weiter vereinfacht und die bis dahin eher generisch und allgemein formulierten einzelnen Prüfpunkte wie in einer Checkliste aufgelistet. So können die jeweiligen Konzerneinheiten noch schneller überblicken, was sie wie anpacken müssen, um die Sicherheitsvorgaben umzusetzen. Ein Beispiel: Bisher hieß es, dass ein Sicherheitsrisikomanagement aus den vier Schritten Risikoidentifizierung, -bewertung, -behandlung und -akzeptanz besteht. Nun beschreiben die Policies noch genauer, wie denn diese Schritte umgesetzt werden können, und anhand welcher Prüfpunkte die entsprechende Umsetzung nachvollzogen werden kann.

Weiterhin enthalten die Security Policies 2.0 neue und erweiterte Regelungsbereiche. Dazu gehören Themen wie Gewalt am Arbeitsplatz oder Cybersecurity. Hier mussten die Sicherheitsmanager zum Beispiel Regeln für veränderte Risiken durch „Bring your own device" oder durch unabsichtlich eingeschleuste Schadsoftware mit USB-Sticks ergänzen.

INTERNATIONALE ZUSAMMENARBEIT

Das International IT/NT Security Leadership Team sorgt dafür, dass die technischen Sicherheitsbereiche der europäischen Landesgesellschaften mit eigenen Telekommunikationsnetzen die gleichen angemessenen Anforderungen erfüllen.

Der Konzern soll weiter zusammenwachsen und alle Landesgesellschaften sollen auf dem gleichen Ambitionsniveau kooperieren. Um diese Ziele zu erreichen, steuert der Bereich Datenschutz, Recht und Compliance die technische Sicherheit über das International IT/NT Security Leadership Team. Diesem gehören die Leiter der technischen Sicherheitsbereiche aus der Zentrale und der Landesgesellschaften an. Das Team trifft sich alle sechs Wochen und führt einmal pro Jahr einen Strategie-Workshop durch. Dabei erarbeiten die Teilnehmer gemeinsam Themen, mit denen sie sich im Laufe eines Jahres im Rahmen von Special Interest Groups mit Projektcharakter eingehend auseinandersetzen. Diese Arbeitsgruppen entwickeln Lösungen und Hilfestellungen, die sowohl den Landesgesellschaften als auch der Zentrale nutzen, um ihr Sicherheitsniveau kontinuierlich zu erhöhen.

Im Jahr 2013 widmeten sich die Teilnehmer den Kernthemen Distributed-Denial-of-Service(DDoS)-Protection, Patch Management und dem Know-how-Transfer beim sicheren LTE-Ausbau. Sie beschäftigten sich mit Tools und Prozessen zum Schutz vor DDoS-Angriffen, erstellten Konzepte, um Sicherheitsschwachstellen durch Einspielen von Patches effizient und nachhaltig zu beheben, und erarbeiteten Maßnahmen, um Angriffe auf LTE-Netze zu verhindern. Der Austausch zwischen Zentrale und den Landesgesellschaften erfolgt auf mehreren Ebenen, um die Zusammenarbeit und das Networking zwischen den Gesellschaften zu fördern. Die fachliche Zusammenarbeit zwischen den Gesellschaften erfolgt auf der Expertenebene. Die hohe Beteiligung unterstreicht, wie wichtig diese Arbeit für alle Parteien ist.

TELEKOMMUNIKATIONSMISSBRAUCH ERKENNEN UND VERHINDERN

Immer wieder warnen Verbraucherzentralen vor Betrug mit teuren Telefonservicenummern. Die Telekom versucht mit allen rechtlich erlaubten Mitteln, den Missbrauch zu erkennen, und schützt damit Kunden und das eigene Unternehmen, erklärt Volker Wagner, Leiter Group Business Security.

Betrüger manipulieren Telefonverbindungen und treiben damit Rechnungssummen in die Höhe.

Es ist ein Wettkampf gegen virtuelle Gegner und die Zeit. Mit immer neuen Methoden versuchen Betrüger durch unterschiedliche Tricks die Telekommunikationsdienste der Provider so auszunutzen, dass sie damit Geld verdienen. Die durch den Missbrauch verursachten Schäden sind erstaunlich hoch: Laut einer Studie der „Communications Fraud Control Association“ aus dem Jahr 2013 kostet der Betrug die Telekommunikationsbranche weltweit rund 46 Milliarden US-Dollar pro Jahr.

Einige Missbrauchsszenarien machen den größten Teil der Fälle aus. So hacken sich die Täter in Telekommunikationsanlagen oder Voice-over-IP-Anschlüsse ein und steuern dann die Verbindungen. Oder sie stehlen Identitäten oder übernehmen und erschleichen sich Kundenkonten. Besonders teuer wird es für Kunden, wenn sie im Auftrag der Anbieter von einem Telefonanschluss unbemerkt deren teure Servicenummern anrufen. Diese Anrufe stellen die Provider dann ihren Kunden in Rechnung, ohne zu wissen, dass sie solche Dienste niemals in Anspruch genommen haben. Dann kommt es oftmals zum Streit zwischen Provider und Kunde, der diese Entgelte verständlicherweise nicht bezahlen will. Kann die Telekom den Missbrauch nicht nachweisen, bleibt sie letztendlich auf den Kosten sitzen.

VERKEHRS- UND NUTZUNGSDATEN BEOBACHTEN UND FILTERN

Die Telekom setzt spezielle Systeme ein, um solche Missbrauchsvorfälle zu erkennen und zu verhindern. Hierbei muss sie Verkehrs- und Nutzungsdaten und die dazugehörigen Bestandsdaten beobachten, gegebenenfalls filtern und auswerten. Dies passiert unter anderem im Sinne des § 100 des Telekommunikationsgesetzes, nach dem darf der Diensteanbieter „zur Sicherung seines Entgeltanspruchs die Bestandsdaten und Verkehrsdaten verwenden, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder -dienstes aufzudecken und zu unterbinden“.

Nun macht es wenig Sinn, den gesamten Datenverkehr von rund 40 Millionen Kunden komplett zu verfolgen und auszuwerten. Daher nutzen die Experten zur Missbrauchserkennung Systeme, mit denen sich der Datenverkehr nach festgelegten Kriterien unter anderem mit bestimmten Schwellenwerten filtern lässt. Erkennt das System zum Beispiel bei einem Anschluss ein ungewöhnlich hohes Daten- und Gesprächsaufkommen, das erhebliche Kosten verursacht, alarmiert es automatisch. Dann können die Netzexperten der Ursache nachgehen und eventuell den Missbrauch stoppen.

Daneben gibt es auch zeitlich befristete, projektbasierte Maßnahmen zur Missbrauchserkennung. Hierbei durchsuchen die Netzexperten Daten gezielt nach vorher festgelegten Missbrauchsszenarien. Im Rahmen dieses Regelprozesses erarbeiten sie ein Konzept, das unter anderem die zu untersuchenden Datensätze und IT-Werkzeuge genau beschreibt.

WHITE- UND BLACKLISTS ERSTELLEN UND EINSETZEN

Da es sich bei der Missbrauchserkennung um personenbezogene Daten von Kunden handeln kann, dürfen alle Maßnahmen nur in enger Abstimmung mit dem Konzerndatenschutz erfolgen. Ein Szenarienkatalog beschreibt alle datenschutzrechtlich zulässigen Verfahrensweisen für die legale Verkehrs-, Nutzungs- und Bestandsdatenverarbeitung für Missbrauchserkennungs- und ermittlungszwecke.

Alle Szenarien, die der Datenschutz freigibt, sind in einer „Whitelist“ aufgeführt und können dann immer wieder eingesetzt werden. Im Zweifelsfall ist grundsätzlich der Datenschutz einzubeziehen. Die vom Konzerndatenschutz abgelehnten Szenarien landen in der „Blacklist“. Es gibt aber auch bestimmte Verfahren, für die das Missbrauchserkennungsteam jedes Mal die Zustimmung des Datenschutzes und des Rechtsbereichs einholen muss.

ZUR PERSON

Volker Wagner
leitet seit 2008 die Group Business Security (GBS) der Telekom. Der diplomierte Betriebswirt ist im Bereich Sicherheit zudem in den Vorständen der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V., des Unterausschusses für Sicherheit im Bundesverband der Deutschen Industrie e.V. sowie des Verbands für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V. aktiv.

FORCIERTER AUSBAU

Die Deutsche Telekom betreibt ein weltweit verteiltes Frühwarnsystem für Cyberattacken. Honeypots nehmen darin eine zentrale Rolle ein. Aktuell registriert das Netzwerk bis zu 800.000 Angriffe am Tag.

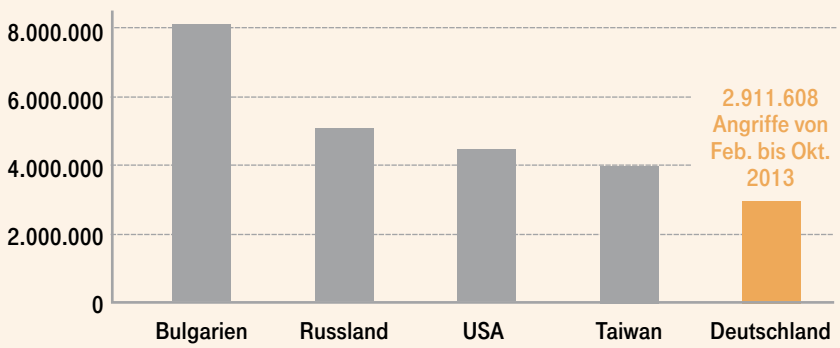
Die „Honigtöpfe" simulieren Schwachstellen, um Angriffe auf sich zu ziehen und analysierbar zu machen. 2013 hat die Telekom das Netz noch einmal deutlich erweitert. Im Jahresverlauf kamen knapp 100 neue Honeypots hinzu, sodass deren Gesamtzahl inzwischen bei 180 liegt.

Um die Informationen des Frühwarnsystems mit einer möglichst breiten Öffentlichkeit zu teilen, hat die Telekom zur CeBIT 2013 ein frei zugängliches Internetportal eingerichtet. Der Sicherheitstacho (www.sicherheitstacho.eu) bietet Echtzeitdaten zur aktuellen Angriffslage an. Zudem ist es möglich, die Angriffe auf einzelne Länder mit Honeypotinstallationen darzustellen. Zudem können sich die Portalbesucher über die Herkunftsländer der Angriffe informieren. Hierbei zeigt sich, dass die meisten Attacken aus China, Russland und den USA erfolgen. In der Regel befindet sich auch Deutschland unter den Top-5-Ländern, von denen Angriffe ausgehen.

Ob die Angreifer in diesen Ländern beheimatet sind, lässt sich aus den Daten des Honeypotnetzes jedoch nicht folgern: Bei der weit überwiegenden Mehrzahl der angreifenden IP-Adressen handelt es sich um gekaperte Fremdrechner, die über das Internet ferngesteuert werden. Die Standorte der im Hintergrund arbeitenden Kommandoserver bleiben für die Sensoren der Honeypots unsichtbar.

DIE TOP 5 DER URSPRUNGSLÄNDER VON ANGRIFFEN

Im Zeitraum von Februar bis Oktober 2013 gingen die meisten Angriffe gegen die Honeypots der Telekom von Bulgarien, Russland und den USA aus. Hacker setzen unterschiedlich viele gekaperte Rechner für einen Angriff ein. Die meisten gekaperten und für Angriffe missbrauchten Rechner wurden in China, den USA und Deutschland lokalisiert.



SICHERE MOBILFUNKKARTEN

Mitte 2013 verbreitete sich die Meldung, dass rund 900 Millionen Handy- und Smartphone-SIM-Karten unsicher seien. Die SIM-Karten der Telekom Kunden waren davon nicht betroffen, da die Telekom selbst bei älteren SIM-Karten einen stärkeren Algorithmus einsetzt als den damals diskutierten.

Konkret ging es um den älteren Verschlüsselungsstandard DES (Data Encryption Standard). Die SIM-Karten mit dieser veralteten Verschlüsselungstechnik können aus der Ferne per SMS gehackt werden. Dabei wird mit der SMS ein Schadcode versendet, der sich selbst installiert. Der Besitzer bemerkt davon nichts. Anschließend könnten Hacker mit der fremden Karte telefonieren, Anrufe umleiten oder Gespräche belauschen. Experten schätzten damals, dass ungefähr ein Achtel aller SIM-Karten weltweit von dem Schadcode befallen werden könnte.

MOBILE HONIGFALLEN

Aktuell betreibt die Telekom neben den circa 180 stationären Honeypots auch mobile Varianten, die verschiedene Smartphones simulieren. Sie registrieren zusammen pro Monat bis zu 30.000 Angriffe.

Die in einem Rechenzentrum betriebenen Honeypots verhalten sich wie ein gejailbreaktes iPhone oder gerootetes Android-Smartphone. Während die Smartphones im Handel mit einer SIM-Karte der Telekom netzseitig sehr gut gegen Cyberangriffe geschützt sind, haben die Telekom Honeypotexperten die Lockgeräte so präpariert, dass Angreifer leichtes Spiel haben. Die Honeypots haben eine öffentliche IP-Adresse. So bieten sie sich als attraktives Ziel für Hackerangriffe an. Im Durchschnitt registrieren die mobilen Honigfallen pro Monat bis zu 30.000 Angriffe. Es lässt sich beobachten, wenn sich jemand auf einem Gerät einloggt und beispielsweise das Adressbuch oder Bilder runterkopieren oder eine Anwendung installieren will, die das Telefon zum Teil eines Botnetzes machen soll. Damit gleichen die Angriffe größtenteils denen auf Rechnern, die an das Festnetz angeschlossen sind.

Ein weiterer mobiler Honeypot, der speziell Android angepasst ist, mit dem Namen „Honeydroid" läuft zurzeit auf einem Samsung Galaxy S4 und einem HTC Desire. Beide Smartphones lassen sich nahezu in vollem Funktionsumfang nutzen, während die installierte Software Angriffe aus dem mobilen Internet detektiert und an das Frühwarnsystem der Telekom weiterleitet. In den zurückliegenden Monaten wurden weniger Angriffe auf die mobilen Honeypots vergezeichnet. Dies könnte damit zusammenhängen, dass sich der zugewiesene IP-Adressraum auf einen Bereich verändert hat, der bisher nicht im Fokus von Angreifern stand.

REGER ZUSPRUCH

Seit Oktober 2013 lädt die Deutsche Telekom Hacker dazu ein, ihre deutschen Internetportale auf Schwachstellen zu prüfen. Wer eine Sicherheitslücke als Erster aufdeckt, erhält eine Geldprämie.

Das Bug Bounty genannte Prämienprogramm ist vom Start weg gut angenommen worden. Im Oktober und November 2013 gingen etwa 500 Hinweise auf Sicherheitsschwachstellen ein. Dank des regen Zuspruchs aus der Internetcommunity ist die Deutsche Telekom in der Lage, die Sicherheit ihrer Webanwendungen noch einmal deutlich zu erhöhen.

Die Initiative basiert auf einer sogenannten Responsible Disclosure Policy. Hierin vereinbart der Hinweisgeber mit der Telekom, die Schwachstelle weder auszunutzen noch anderweitig zu veröffentlichen. Gleichzeitig verpflichtet sich die Deutsche Telekom, die gemeldete Sicherheitslücke schnellstmöglich zu schließen. Das Engagement der Hinweisgeber wird mit einer Geldprämie belohnt. Deren Höhe bemisst sich nach der Kritikalität des Fehlers und des davon betroffenen Portals. Der Fokus des Bug-Bounty-Programms liegt auf allen Webportalen der Domäne *telekom.de. Prämiert werden die Erstmeldungen von Schwachstellen im Programmnode, den die Deutsche Telekom entwickelt hat. Fehler in eingesetzten Drittprodukten sind von den Prämien ausgenommen. Sämtliche Teilnahmebedingungen finden sich unter: www.telekom.com/bug-bounty

ABHÖRSCHUTZ IM MOBILFUNK ERHÖHT

Als erster Netzbetreiber in Deutschland setzt die Telkom den Verschlüsselungsstandard A5/3 für die Sprachübertragung im Mobilfunknetz flächendeckend ein. Damit sind Gespräche auch im GSM-Netz besser gegen mögliches Abhören geschützt. Der Standard wurde bis Ende 2013 bundesweit implementiert.

Für die Verschlüsselung von Handygesprächen müssen die Kunden nicht aktiv werden: Sie erfolgt bei der Funkübertragung zwischen Mobiltelefon und Basisnetz automatisch. Mit dem neuen Standard A5/3 ist die Verschlüsselung im GSM-Netz stärker, der neue Algorithmus gilt bislang als sicher. Im UMTS- und LTE-Netz werden ähnlich starke Verschlüsselungen eingesetzt. Für den neuen Standard musste die Telekom bundesweit neue Hard- und Software an rund 30.000 Basisstationen und zentralen Netzpunkten installieren.

Die Herausforderung bei der Umstellung war, dass bundesweit immer noch circa 50.000 ältere Geräte im Gebrauch sind, die mit dem neuen Verschlüsselungsstandard nicht funktionsfähig sind. Um sicherzustellen, dass diese Kunden nicht plötzlich ohne Empfang dastehen, musste die Telekom eine spezielle Softwarelösung entwickeln und testen. Funktionsfähig bleiben jetzt sämtliche Handymodelle. Bei älteren Modellen werden Gespräche allerdings weiterhin mit dem Standard A5/1 verschlüsselt.

Die Telekom setzt den Verschlüsselungsstandard A5/3 nicht nur in Deutschland ein: In Mazedonien, Montenegro, Polen und Tschechien ist die Technik bereits implementiert. Weitere Länder werden folgen.

WLAN-HOTSPOTS MIT EINGEBAUTER SICHERHEIT

Die Deutsche Telekom will das größte Hotspotnetz der Welt errichten und hat dafür im Juni 2013 die Initiative WLAN TO GO gestartet. Bis zum Jahr 2016 sollen allein in Deutschland 2,5 Millionen neue Hotspots entstehen.

Eine spezielle Konfiguration des Speedport W724V Routers erlaubt es DSL-Kunden, die ungenutzte Bandbreite ihres Anschlusses mit anderen Telekom Kunden zu teilen. Die Telekom hat die Sicherheit der neuen Lösung überprüft.

DSL-Kunden erhalten eine vollständig abgesicherte Lösung, die auf allen Speedport W724V Routern funktioniert. Hat sich ein Breitbandkunde für die Teilnahme an WLAN TO GO entschieden, sendet das Speedport-Gerät zwei unabhängige WLAN-Signale. Somit entstehen zwei vollständig voneinander getrennte Netzwerke: Das eine Netzwerk ist verschlüsselt und bleibt privat. Das andere dient Hotspotnutzern als Zugangspunkt mit der Kennung Telekom_FON.

Ein über die Kennung Telekom_FON eingeloggter Hotspotnutzer hat keinerlei Möglichkeit, auf das private WLAN zuzugreifen. In entgegengesetzter Richtung gilt dasselbe: Auch der Hotspotnutzer muss sich keine Gedanken darüber machen, dass der Anschlussinhaber auf sein mobiles Endgerät zugreifen könnte. Darüber hinaus besteht bei WLAN TO GO keinerlei Haftungsrisiko für eine eventuelle gesetzeswidrige Nutzung durch Dritte. Da ausschließlich authentifizierte Anwender Zugang zu den Hotspots erhalten, kann die Nutzung zurückverfolgt werden.

SPAGAT ZWISCHEN DATENSCHUTZ UND DATENSICHERHEIT

Als Telekommunikationsprovider muss und will die Telekom einerseits die Daten ihrer Kunden mit allen Mitteln schützen. Andererseits schreibt der Gesetzgeber verpflichtend vor, Daten unter bestimmten Voraussetzungen preiszugeben.

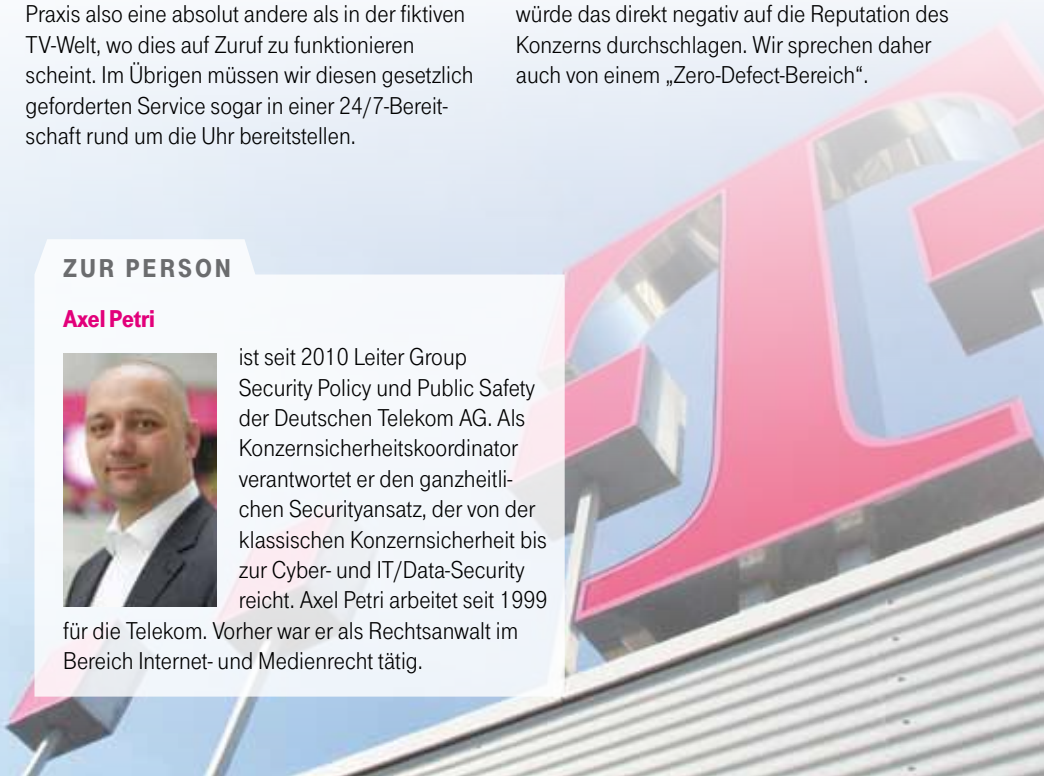
Was verbirgt sich hinter dem Begriff der öffentlichen Sicherheit?
Axel Petri: Der Begriff kommt aus dem Telekommunikationsgesetz (TKG). Hier geht es in Teil 7, Abschnitt 3 um die öffentliche Sicherheit. Gemeint sind all diejenigen Anforderungen, welche die Telekom als Anbieter von Telekommunikationsdienstleistungen zur Aufrechterhaltung von Sicherheit und Ordnung erbringen muss. Welche Pflichten und Rechte bestehen zum Beispiel bei Auskunftsersuchen der Sicherheitsbehörden oder bei der Umsetzung von Überwachungsmaßnahmen sowie der Erteilung von Auskünften an berechtigte Stellen?

Welche Verpflichtungen hat die Telekom konkret?
Axel Petri: Es geht beispielsweise darum, dass wir staatlichen Stellen bestimmte Daten von Telefonanschlüssen mitteilen, Standorte von Mobiltelefonen ermitteln oder aber auch die Überwachung von Telekommunikationsinhalten ermöglichen müssen. Dies bezeichnen wir mit Lawful Interception/Data Provision (LI/DP). Neben diesen in jedem Fernsehkrimi vorkommenden Anwendungsfällen gibt es noch zahlreiche ebenso bedeutende Aspekte der öffentlichen Sicherheit: Dazu gehört die Pflicht, Notrufe unter der Nummer 112 zu ermöglichen, oder dafür zu sorgen, dass für die Aufrechterhaltung der Sicherheit erfolgskritische Amtsträger in bestimmten Situationen bevorrechtigt telefonieren können.

Was genau macht Ihr Bereich in diesen Themen?
Axel Petri: Wir stellen dem Konzern die Expertise an der Schnittstelle zwischen Sicherheit und Recht bereit. Dies reicht von der konkreten Beratung der Fachseiten bis hin zu der strategischen Positionierung des Konzerns und der Einbringung unserer Positionen in Gesetzgebungsverfahren. Im Bereich LI/DP sind wir darüber hinaus diejenigen, die entsprechende Maßnahmen umsetzen, etwa mit Zugriff auf die zugehörigen Datenbanken oder auch Netzelemente.

Unter welchen Voraussetzungen kommt die Telekom den Anfragen der Sicherheitsbehörden nach?
Axel Petri: Oberster und alleiniger Leitgedanke für die Telekom ist die Erfüllung von Recht und Gesetz. Nur wenn alle gesetzlichen Voraussetzungen gegeben sind, setzen wir die Anordnung der Behörde – in der Regel Gerichte oder Staatsanwaltschaften – im Einzelfall um. Hier ist die Praxis also eine absolut andere als in der fiktiven TV-Welt, wo dies auf Zuruf zu funktionieren scheint. Im Übrigen müssen wir diesen gesetzlich geforderten Service sogar in einer 24/7-Bereitschaft rund um die Uhr bereitstellen.

Die öffentliche Sicherheit ist aber doch für alle von höchstem Interesse.
Axel Petri: Neben der öffentlichen Sicherheit geht es auch stets um die Verpflichtung, das Fernmeldegeheimnis der Kunden sowie sonstige datenschutzrechtliche Vorgaben zu beachten. Diese beiden Rechtsgüter sind in der Praxis leider oft gegensätzlich, was sich an der äußerst kontroversen politischen Diskussion um die gesetzliche Regelung der Vorratsdatenspeicherung zeigt. Es gilt also immer, sorgfältig abzuwägen, um sich nicht dem Vorwurf der Strafvereitelung einerseits oder aber des Bruchs des Fernmeldegeheimnisses andererseits auszusetzen. Wir müssen also in diesem sehr öffentlichkeitswirksamen Bereich genau abwägen. Falls Fehler passieren würden, würde das direkt negativ auf die Reputation des Konzerns durchschlagen. Wir sprechen daher auch von einem „Zero-Defect-Bereich".



ZUR PERSON

Axel Petri

ist seit 2010 Leiter Group Security Policy und Public Safety der Deutschen Telekom AG. Als Konzernsicherheitskoordinator verantwortet er den ganzheitlichen Securityansatz, der von der klassischen Konzernsicherheit bis zur Cyber- und IT/Data-Security reicht. Axel Petri arbeitet seit 1999 für die Telekom. Vorher war er als Rechtsanwalt im Bereich Internet- und Medienrecht tätig.

MITARBEITER SORGT FÜR SICHERE E-MAILS

Einen Tag pro Monat bekommen GIS-Mitarbeiter Freiraum für die Entwicklung von Innovationen.

Zeit für Innovationen: Mitarbeiter Wolfgang Bollenbach entwickelte eine Verschlüsselungslösung für private E-Mail-Adressen in einem Ideenprogramm.

„Kunden begeistern und Dinge einfacher machen!“: Wolfgang Bollenbach hat sich diese Leitlinie des Telekom Konzerns zu Herzen genommen. Bei einem Ideenprogramm seines Bereichs entwickelte der Mitarbeiter der Group Information Security (GIS) eine Verschlüsselung für private E-Mail-Adressen – kostengünstig, einfach und am Bedürfnis nach mehr Sicherheit orientiert.

Bollenbach baute mithilfe von Open-Source-Produkten eine eigene Website, die Verschlüsselungszertifikate für E-Mail-Adressen generiert. Das verursacht nahezu keine Kosten. Der Mehrwert des Nutzers ist immens: Auf Basis des S/MIME-Standards können E-Mails komplett von Ende zu Ende verschlüsselt werden.

S/MIME steht für Secure/Multipurpose Internet Mail Extensions und ist ein internationaler Standard für die Verschlüsselung und Signatur von E-Mails. Ein Nutzer kann Verschlüsselungszertifikate auf seine eigenen Endgeräte verteilen. Mittels der Zertifikate kann er seine E-Mails verschlüsselt an jede Person senden, die ebenfalls S/MIME-Zertifikate hat. Zurzeit wird geprüft, inwieweit sich der Service in Telekom Produkte integrieren lässt.

Das Programm „One Day per Month“ legt im Bereich Group Information Security (GIS) den Grundstein für innovative Ideen wie die von Wolfgang Bollenbach. Es bietet GIS-Beschäftigten die Möglichkeit, einen Tag im Monat an einem eigenen Projekt jenseits des Tagesgeschäftes zu arbeiten. Einzige Vorgabe: der Bezug zur Telekom. Seit Beginn des Programms haben die Mitarbeiter im Rahmen des Programms eine ganze Reihe von Ideen entwickelt und umgesetzt – zum Beispiel mobile Honeypots für die Landesgesellschaften.

SICHERHEITSLÜCKE GESCHLOSSEN

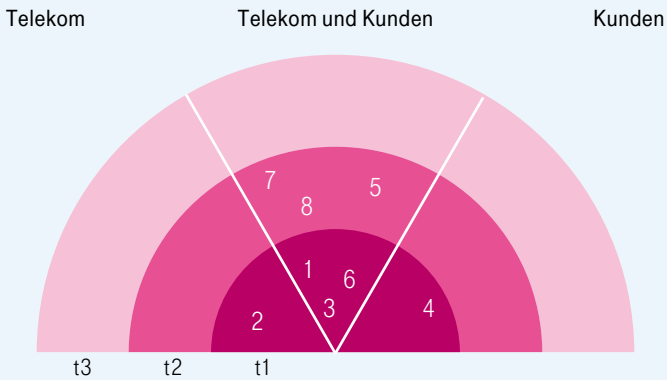
Mitte 2013 hat ein Hacker eine Sicherheitslücke im Kundencenter der Telekom gefunden. Unbekannte hätten die E-Mail-Adressen mit der Endung @t-online übernehmen können, ohne dass die Nutzer etwas davon bemerken konnten. Die Telekom hat daraufhin sofort die Sicherheitslücke geschlossen.

Es gab bis zur Schließung der Lücke keine Anzeichen dafür, dass das Leck ausgenutzt und E-Mail-Konten gekapert wurden. Ein möglicher Angriff hätte über ein Script erfolgen können, das Hacker in einer Internetseite verstecken können. Diese Website hätte hierzu auch aus der telekom.de -Domain kommen müssen. Klicken Nutzer auf die infizierte Website, beginnt im Hintergrund das Script seine Arbeit.

Das Schadprogramm hätte dann zunächst die E-Mail-Adresse des Nutzers geändert. Zum Beispiel von Müller-90@t-online.de in Müller-80@t-online.de. Daraufhin verfällt die ursprüngliche E-Mail-Adresse und der Hacker beantragt für sich die Adresse Müller-90@t-online.de neu. Der ehemalige Besitzer bekommt keine neuen E-Mails mehr, da sie beim neuen Besitzer der Adresse landen. Die Telekom hat nach dem Hinweis des Hackers die Sicherheitslücke durch eine zusätzliche Abfrage des Passwortes geschlossen.

GEFAHRENRADAR

Mit dem Bedrohungsradar stellt das Deutsche Telekom CERT die Entwicklung von Cybergefahren dar. Das Werkzeug dient dem Unternehmen dazu, Bedrohungen frühzeitig zu identifizieren und Sicherheitsmaßnahmen zu planen.



BEDROHUNGEN

1 Advanced Persistent Threats (APT)
2 Spear Phishing gegen Telekom-Mitarbeiter
3 Mobiler Schadcode
4 Angriffe auf mobiles Banking
5 Denial-of-Service-Angriffe auf DNS-Infrastruktur
6 Angriffe auf DSL-Router
7 Angriffe auf CAN-Bus von Fahrzeugen
8 Angriffe auf Smart TVs

ENTWICKLUNGSSTADIEN

t1 Aktive Ausnutzung einer bekannten Schwachstelle
t2 Schwachstelle vorhanden und Ausnutzbarkeit nachgewiesen
t3 Schwachstelle vorhanden und theoretisch ausnutzbar

WER WIRD BEDROHT?

Der Radar zeigt, wer von einer Bedrohung betroffen ist: der Kunde, der Produkte und Dienste von der Telekom bezieht (rechter Sektor), die Telekom mit ihren internen Systemen (linker Sektor) oder beide gemeinsam (mittlerer Sektor).

E-MAIL MADE IN GERMANY

Ob Großunternehmen, mittelständische Firma, Handwerksbetrieb oder Privatperson: Die E-Mail birgt ein großes Risiko, sich Trojaner oder Viren einzufangen. Und die elektronische Nachricht ist offen wie eine Postkarte, bei der jeder auf dem Transportweg mitlesen kann.

Für E-Mail-Sicherheit zu sorgen, ist also eine der Pflichtaufgaben für eine sichere IT. Dabei greifen aktuelle Virenscanner und Firewalls zu kurz. Sie filtern zwar einen Großteil der Schadsoftware aus dem E-Mail-Verkehr, doch sie sorgen nicht dafür, dass Fremde die Inhalte einer E-Mail mitlesen können. Denn E-Mails überträgt das Internet vom Absender zum Empfänger grundsätzlich unverschlüsselt. Auf ihrem Weg leiten die am Transport beteiligten Provider die E-Mails aber über viele verschiedene Computer. Dabei kann jeder halbwegs technisch versierte Hacker mit einfachen Mitteln die E-Mail mitlesen. Und in den elektronischen Nachrichten verbergen sich oft interessante Informationen für Kriminelle – zum Beispiel Kontonummern.

E-MAILS VERSCHLÜSSELT ÜBERTRAGEN

Der einzige wirksame Schutz besteht demnach darin, vertrauliche E-Mails zu verschlüsseln. Die Telekom hat daher zusammen mit United Internet eine Brancheninitiative für sichere E-Mail-Kommunikation in Deutschland gestartet, der später auch freenet beigetreten ist. Mit „E-Mail made in Germany“ werden die E-Mails der Nutzer von GMX, T-Online.de, WEB.DE und freenet auf allen Übertragungswegen zwischen den E-Mail-Servern und in den Rechenzentren automatisch verschlüsselt. Die Nutzer müssen also nichts weiter tun. Zudem gibt es eine Kennzeichnung für E-Mail-Adressen, sodass Nutzer vor dem Mailversand erfahren, ob die ausgewählten Empfängeradressen den Sicherheitsstandards des Mailverbundes entsprechen. Für die Verschlüsselung verwenden die Partner ausschließlich in Deutschland produziertes Schlüsselmaterial und Open-Source-Lösungen, die keine Hintertürchen wie kommerzielle Produkte haben können.

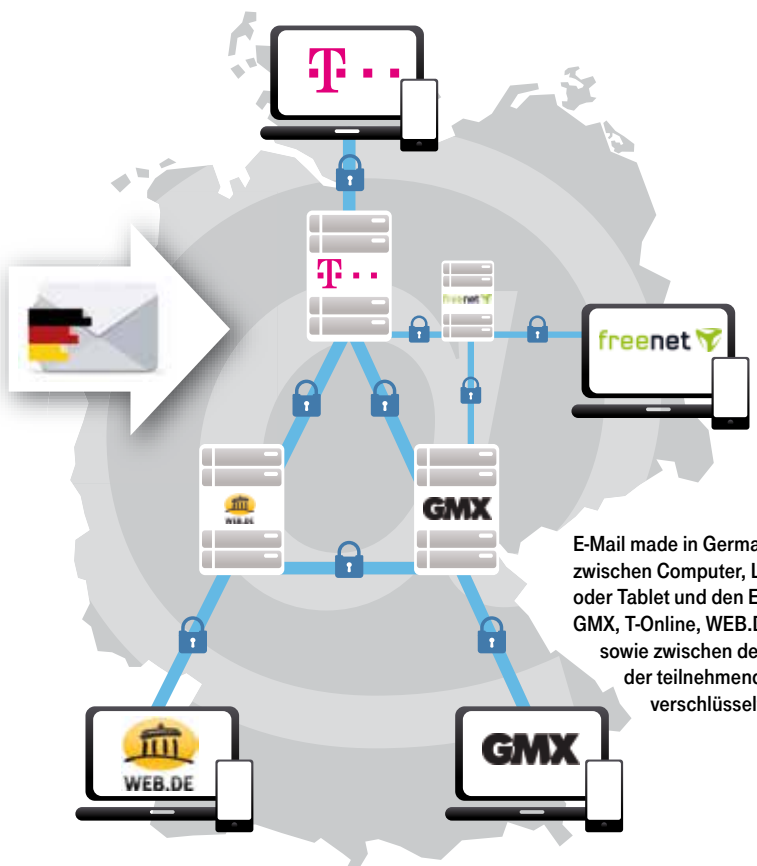
„E-Mail made in Germany kann man vergleichen mit einer Postkarte, die wir nicht nur in einen Umschlag stecken, sondern wir packen alle geschlossenen Umschläge zusätzlich in Postsäcke. Damit sind Sender und Empfänger auf der Strecke ausradiert“, erklärt der IT-Sicherheitschef der Telekom, Thomas Tschersich. Das Versenden zu anderen E-Mail-Anbietern wie Google, Yahoo oder Microsoft ist weiter möglich. Allerdings stellt E-Mail made in Germany hierfür weder die sichere Übertragung noch die Datenverarbeitung in Deutschland sicher. Tschersich weiter: „Die Partner der Initiative garantieren zudem, dass sie alle Daten ausschließlich in Deutschland verarbeiten. Damit unterliegen sie dem strengen deutschen Datenschutz – ohne mögliche Aufweichungen oder Regelungen ausländischer Instanzen.“

NACHWEISBAR, SICHER UND ZUVERLÄSSIG

Noch einen Schritt mehr für die Sicherheit bietet De-Mail, die einem Einschreiben mit Rückschein entspricht. Hier bekommen die Absender vom Empfänger die Bestätigung, dass er die Mail gelesen hat. Wie bei E-Mail made in Germany können Angreifer die Inhalte einer De-Mail auf ihrem Weg durch das Internet nicht mitlesen oder verändern.

De-Mail darf nicht jeder Provider ohne vorherige Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) anbieten. Dies gewährleistet ein einheitliches und geprüftes Sicherheitsniveau.

Rechtliche Basis für De-Mail bietet das De-Mail-Gesetz, welches die Mindestanforderungen an einen sicheren elektronischen Nachrichtenaustausch regelt. Darüber hinaus sorgt das Gesetz für ein geregeltes Verfahren, wie diese Anforderungen und die De-Mail-Anbieter überprüft werden. Das sind wichtige Voraussetzungen für den Aufbau von Vertrauen in die Sicherheit und für die Qualität der De-Mail-Dienste. Die gesetzlichen Regelungen stellen zudem sicher, dass alle De-Mail-Nutzer aller De-Mail-Anbieter sich untereinander erreichen können.



E-Mail made in Germany überträgt Daten zwischen Computer, Laptop, Smartphone oder Tablet und den E-Mail-Servern von GMX, T-Online, WEB.DE und freenet sowie zwischen den Rechenzentren der teilnehmenden E-Mail-Dienste verschlüsselt.

NUTZERFREUNDLICHE IT-SICHERHEIT

Es müssen mehr Zeit und Geld in die IT-Sicherheit investiert werden – besonders in die Usability von Sicherheitslösungen. Nur wenn Sicherheit bedienbarer wird, dann bewerten wir sie nicht länger als störend. Davon ist Professor Matthew Smith, Informatiker an der Universität Bonn, überzeugt.

Egal, was letztendlich der Auslöser für den Boom der Apps war: Die praktischen Anwendungen für Smartphones und Tablet-PCs haben die Bedienbarkeit von Software revolutioniert. Mussten sich Anwender bis dahin durch tagelange Schulungen kämpfen, ging mit den Apps auf einmal alles leichter: runterladen und installieren – schon lassen sich die meisten Anwendungen ohne Abtauchen in Handbücher bedienen.

Diese neue Leichtigkeit der Softwarebedienung fehlt den meisten IT-Sicherheitslösungen. Selbst technisch ausgereifte Angebote verstauben in den Regalen der Anbieter, während immer neue Sicherheitslücken den Cyberkriminellen das Leben vereinfachen. Bisher lief ein Großteil der Entwicklungen im IT-Sicherheitsbereich nach dem Prinzip: Die Nutzer haben sich der Technologie anzupassen. Sie sollen lernen, wie sie die Systeme richtig benutzen. Dieses Prinzip müssen wir umkehren. In der Forschung für benutzbare IT-Sicherheit und Privatsphäre – Usable Security and Privacy – entwickeln wir daher Sicherheitslösungen, die sich den Nutzern anpassen, also einfach zu verstehen und zu bedienen sind.

Das fängt bei kleinen Ideen an. Beispiel Apps: Obwohl bedienerfreundlich, liest sich kaum jemand vor deren Installation die seitenlangen Sicherheitsinformationen über die Rechte einer App durch. Warum auch, wenn die praktische App das Smartphone zur Taschenlampe oder Waage wandelt? Doch in den Rechten – Permissions – verstecken sich – meist kleingedruckt – wichtige Hinweise, was eine App neben ihrem offensichtlichen Zweck noch mit dem Smartphone machen darf. Sie greift möglicherweise auf Kontaktdaten oder Standort zu. Ob der Anbieter diese Daten zu Werbezwecken oder für Datenanalysen an Unternehmen verkauft, ist dann ungewiss, aber wahrscheinlich. So macht der App-Anbieter den Nutzer zum Produkt.

Die schlechte Usability von Sicherheitslösungen kostet Zeit und Nerven.

TRANSPARENZ SCHAFFEN

Das ist legitim, solange der Anbieter transparent macht, was er mit den Daten der Nutzer vorhat. Nur dann können Letztere selbst entscheiden, ob sie diese Daten preisgeben wollen. Für diesen Zweck haben wir als ein Beispiel für menschenzentrierte IT-Sicherheit eine Anwendung für Android-Geräte entwickelt, die plakativ verdeutlicht, welche Daten der App-Anbieter wie nutzen will. Wird eine App etwa auf das Telefonbuch des Smartphones zugreifen, dann wählt unsere Software einen Kontakt aus diesem Telefonbuch mit dem Hinweis aus: „Diese App greift auf die Telefonnummer Ihrer Mutter zu." Oder sie zeigt den aktuellen Standort auf einer Karte an und sagt: „Diese App sieht, dass Sie sich gerade hier befinden." Und wenn sie die Kamera anschalten kann, zeigt unsere App dazu das aktuelle Kamerabild. Wir erreichen damit nicht die perfekte Sicherheit. Aber wir schaffen Transparenz. Der Nutzer soll verstehen, was die App kann. Mit einer eigenen Studie konnten wir verdeutlichen, dass die bildlichen Hinweise auf die Fähigkeiten einer App das Downloadverhalten der Nutzer verändern. Sie installierten auf ihren Smartphones weniger Programme mit nicht nachvollziehbaren Rechten.

Usability beginnt aber schon in der Entwicklung von Software. Viele Sicherheitslücken sind auf Programmier- und Konfigurationsfehler zurückzuführen. Wir hätten die technischen Möglichkeiten, mehr Sicherheit zu gestalten. Aber wir haben nicht die Menschen, welche die Systeme sicherheitsgerecht einrichten und betreiben können. Unser Forscherteam hat in mehreren Studien Hunderte von Entwicklern und Administratoren befragt und in Systemen gezielt nach Fehlern gesucht. Wir konnten feststellen, dass viele Entwickler und Administratoren nicht wissen, welche Sicherheitslücken in ihren Systemen stecken.

Entwickler arbeiten oftmals unter hohem Zeit- und Kostendruck an zunehmend komplexen Systemen. Ihnen ist es nahezu unmöglich, bei Millionen von Lines of Code alle Schwachstellen zu erkennen und zu schließen. Daher müssen wir als Nutzer im Livebetrieb die zahlreichen Sicherheitslücken ausbaden, die schon in der Programmierung hätten geschlossen werden können. Dem Angreifer genügt aber ein einziger Fehler, um in das System einzudringen. Zudem ist ein Sicherheitscode sehr komplex und schwierig zu programmieren. Daher müssen wir auch die Ausbildung der Entwickler verbessern. Zu lange schon gilt IT-Sicherheit als optionale und manchmal sogar als unbeliebte Disziplin und wird im Kurrikulum mancher Unis und Fachhochschulen nicht angeboten. Ich plädiere sehr dafür, das IT-Sicherheit Teil der Grundausbildung und Pflichtfach in der Informatik sein muss und dabei insbesondere auf die Anwendbarkeit durch den Menschen geachtet werden soll.

ZUR PERSON

Matthew Smith
ist Professor für Benutzbare IT-Sicherheit und Privatsphäre an der Rheinischen Friedrich-Wilhelms-Universität Bonn und Mitarbeiter des Fraunhofer Institut FKIE. Sein Studium der Technischen Informatik hat er mit Auszeichnung abgeschlossen. Smith forscht seit vielen Jahren auf dem Gebiet der IT-Sicherheit, insbesondere befasst er sich mit der Benutzbarkeit von IT-Sicherheitssystemen.

GESCHÄFTSFELD CYBER SECURITY

T-Systems hat das IT-Sicherheitsportfolio in der Geschäftseinheit Cyber Security gebündelt. Der Leiter, Dr. Jürgen Kohr, verfolgt eine Strategie, die sich nach den Leitideen von Transparenz, Kompetenz, Einfachheit und Kooperation ausrichtet.

WhatsApp, New York Times, Adobe oder Präsident Obamas Onlineauftritte: Professionelle Hacker nutzten im Jahr 2013 jede Lücke in den digitalen Systemen von Unternehmen, Privatpersonen oder Behörden, um aus unterschiedlichen Motiven Schaden anzurichten. Sich erfolgreich Cyberkriminellen entgegenzustellen, fällt schwer. Zu schnell wechseln die Angreifer ihre digitalen Waffen und ändern ihre Taktik.

Aber wie schützen CIOs ihre Unternehmen nun am besten? Der Fokus liegt auf dem vertrauensvollen Austausch über die akute Bedrohungslage zwischen Experten und Management über Unternehmensgrenzen und Branchen hinweg. Unter dem Motto „Security is for Sharing" baut T-Systems eine Art digitale Nachbarschaftshilfe auf, bei der das Geschäftsfeld als Mediator fungiert. Ziel ist es, den Austausch über Sicherheitsfragen auf Entscheiderebene zu verstetigen. Die gewonnenen Erkenntnisse fließen dann in neue Produkte und Abwehrstrategien ein. Transparenz verkürzt so den Vorsprung der Angreifer und macht über verbesserte Abwehr die Angriffskosten der Cyberkriminellen von Mal zu Mal teurer.

„CLEAN PIPE": SICHERHEIT EINFACH AUS DER TELEKOM CLOUD

Die größten Gefahren lauern in der Geringschätzung des Risikos und in der mangelnden Sensibilität für die eigene Attraktivität als Ziel für Cyberangriffe. Nur wenige Firmen verfügen über die erforderlichen Ressourcen und Kompetenzen, um mit zielgerichteten Angriffen umzugehen. Gerade dem Mittelstand fällt es schwer, mit Technik und geschultem Personal dem Tempo immer neuer Angriffe und ausgefeilter Angriffsmethoden standzuhalten. Vielfach bemerken sie diese gar nicht oder zu spät. Die Zeit, in der ein Angreifer unentdeckt seinen Angriff vorantreibt, muss sich daher drastisch verkürzen. Nur so können Gegenmaßnahmen eher starten und den Schaden begrenzen. 2014 wird T-Systems mit „Clean Pipe" neue Securityservices aus der Cloud erproben und sie Mitte des Jahres einer ersten Kundengruppe zur Verfügung stellen. Mit Clean

Pipe werden schädliche Inhalte in den Leitungen des Internets automatisch in den Rechenzentren herausgefiltert. Kleine und mittlere Firmen profitieren so von Schutzmechanismen, die sonst nur Großunternehmen zur Verfügung stehen. T-Systems kooperiert hier mit der deutschen Firma LANCOM. Diese hat einen Router entwickelt, der vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert ist. Voraussichtlich Anfang 2016 soll die Infrastruktur für Clean Pipe im Konzern stehen, um den Datenstrom von bis zu einer Million mittelständischer Unternehmen in der Telekom Cloud zu reinigen.

SICHERHEITSKOOPERATION FÜR GROSSKONZERNE

Wer Sicherheitsvorfälle erst messen muss, bevor er sie abwehren kann, hinkt zielgerichteten Angriffen fortwährend hinterher. Um hier die „Verfolgerrolle" zu überwinden, ist ein Sicherheitsmanagement auf Basis von Erkenntnissen vonnöten, das Informationen präzise verknüpft und in Echtzeit auswertbar macht. Angriffe bereits erkennen, bevor sie ihre volle Wirkung entfalten – dieses Ziel verfolgt der Konzern mit „Advanced Cyber Defense by Telekom".

„ACD by Telekom" kombiniert moderne IT-Sicherheitstechnik, Expertenwissen und Zugriff auf Datenquellen wie die konzerneigenen Frühwarnsysteme – Honeypots – für ein aktives Cybersicherheitsmanagement, das die IT-Sicherheit eines Unternehmens steuert und dynamisch auf Angriffe reagieren kann. Für den Aufbau eines Next Generation Service Operation Centers bündelt der Konzern seine Kräfte mit der Firma RSA. Der „Intelligence-Driven-Security"-Ansatz des IT-Sicherheitsdienstleisters erfasst möglichst viele Informationen aus Netzwerken und Anwendungen, führt diese zusammen und bewertet sie mittels Big-Data-Analysen.

VERSCHLÜSSELUNG DER TELEKOM IN DER CLOUD

Ein weiterer Schwerpunkt der Strategie ist es, Securityinnovationen über Start-ups und Risikokapital schneller für den Markt zu erschließen. Aktuell treibt der Geschäftsbereich mit der kalifornischen Firma CipherCloud, an der T-Venture beteiligt ist, das Thema Verschlüsselung und Cloud voran. Die Kooperation zielt darauf, das Arbeiten auch mit den verschlüsselten Daten, die in der Cloud liegen, zu ermöglichen. Das ist das Neue an der Lösung, die zudem mit Schlüsseln des Telekom-eigenen Trust-Centers ausgestattet werden soll. Die CipherCloud-Lösung wird die sichere Nutzung und volle Kontrolle von Daten in privaten, hybriden und öffentlichen Cloud-Applikationen ermöglichen und wird so auch Datenschutz- und Regulierungsbedenken gerecht.

ZUR PERSON

Dr. Jürgen Kohr
ist Leiter des Geschäftsfeldes Cyber Security, T-Systems. Er war Strategiechef in der IT-Großkundensparte und davor Stabsleiter von Telekom Vorstand Reinhard Clemens. Der Diplom-Kaufmann treibt die Entwicklung neuer Sicherheitsprodukte voran. Er ist auch Mitglied im Investment Commitee des Infrastrukturfonds der T-Venture, des Venture-Capital-Unternehmens der Deutschen Telekom AG.

E-MAILS OHNE UMWEGE

Als im Herbst 2013 die Empörung über die Abhörpraktiken der Geheimdienste ihren Höhepunkt hatte, brachte die Telekom das Thema nationales- oder Schengen-Routing ins Spiel. Daraufhin entbrannte eine Diskussion über das angebliche Ende des freien Internets. Eine Klarstellung.

In einer Kampagne gehe es um den vermeintlichen Schutz vor US-Geheimdiensten, schrieb unter anderem die Frankfurter Rundschau. „Internetverkehr, der seinen Start- und seinen Zielpunkt in Deutschland hat, soll nur noch über Leitungen und Server in Deutschland laufen. Das ist theoretisch möglich. Doch was bringt's? So gut wie nichts." Damit hatte der Kommentator zumindest korrekt dargestellt, was manche Redakteure bis dahin als Ende des freien Internets interpretiert hatten. Doch darum geht es nicht: Es gibt keine Abschottung oder Zensur von Verkehr aus dem Ausland ins Inland wie in China. Selbstverständlich können Telekom Kunden auch in Zukunft alle Dienste nutzen, die sie nutzen möchten – ganz gleich, von wo auf der Welt sie angeboten werden.

Internet der kurzen Wege: Wenn Daten innerhalb von Deutschland transportiert werden, dürfen ausländische Geheimdienste nicht mitlesen.

NATIONALES ROUTING ALLTAG IN DEN USA

Natürlich wird Internetverkehr auch in Zukunft nach Großbritannien, in die USA und sonst wo in der Welt fließen. Es ist jedoch nicht ersichtlich, warum Datenpakete zum Beispiel von Frankfurt nach Berlin über London oder New York laufen. Vielmehr geht es darum, dass Daten den Rechtsraum, in dem sie anfallen und verarbeitet werden, auch beim Transport zwischen Anfangs- und Endpunkt nicht verlassen. In den USA ist dieses nationale Routing längst Alltag und Teil der Verträge zwischen Netzbetreibern und Regierung. Verlassen die Daten die Landesgrenze nicht, hätten ausländische Geheimdienste zumindest keinen legalen Zugriff mehr. Dass sie in Deutschland spionieren, lässt sich durch Datenrouting nicht verhindern. Das ist dann aber illegal und birgt diplomatische Probleme für die Spione.

TECHNISCH MACHBAR UND POLITISCH SINNVOLL

Alle Marktteilnehmer wägen beim Routing ab zwischen Sicherheit und Aufwand. Heute läuft der nationale Verkehr teilweise über das Ausland, weil große Carrier mit Überkapazitäten und Kampfpreisen Verkehr an sich ziehen. Die Telekom hat keinen Einfluss auf die Routinggepflogenheiten anderer Carrier. Da sie aber über das größte Netz in Deutschland verfügt, ist zumindest für die eigenen Kunden nationales Routing technisch machbar und sicherheitspolitisch sinnvoll. Zum Beispiel lassen sich E-Mails von einem Telekom Anschluss ohne Umwege über das Ausland an eine deutsche T-Online-Adresse schicken. Wenn andere Provider sich diesem Routing anschließen, lassen sich die Datenverkehre von Deutschland nach Deutschland auch providerübergreifend im Inland transportieren. Dies umzusetzen, dafür käme auch ein Gesetz infrage.

GESETZLICHE REGELUNG IN DER EU GEWÜNSCHT

Routingtabellen werden ständig geändert, abhängig von Veränderungen in den Netzen, freien Kapazitäten und deren Preisen. Die Mitberücksichtigung von sicherheitspolitischen Zielsetzungen ist ohne größere Zusatzkosten umsetzbar, muss aber politisch legitimiert werden. Der Telekom ist durchaus bewusst, dass sie mit dem Vorschlag des nationalen Routings nur einen Teil – möglicherweise auch nur einen kleinen Teil – des Datenverkehrs erfasst. Und wenn sich die EU-Staaten auf eine gemeinsame Verordnung verständigen würden, könnte schon ein größerer Teil des Gesamtverkehrs im Schengen-Raum geschützt werden. Manche mögen das als Marketinggag bezeichnen. Andere sehen das zumindest als guten Anfang, raus aus der Betroffenheitsdiskussion, in die konkrete Umsetzung neuer Sicherheitsmaßnahmen zu kommen. Und jeder Schritt in Richtung mehr Sicherheit ist auf jeden Fall besser, als weiter in Untätigkeit zu verharren.

NATIONALES ROUTING IN GROSSEN TEILEN UMGESETZT

Ein nationales Routing für Kunden der Telekom ist heute schon zu einem Großteil umgesetzt. Verkehre von Deutschland nach Deutschland transportieren unsere Netze innerhalb der deutschen Grenzen. In Ausnahmefällen, zum Beispiel durch selten auftretende Engpässe, werden Alternativrouten durch europäische Nachbarländer gewählt. Die Telekom hat zudem direkte Netzverbindungen zu fast allen relevanten nationalen Providern. Wenn alle Provider in ihren Netzen ähnlich verfahren, entsteht ein de facto flächendeckendes nationales Routing. Dies erfordert zunächst keine Abstimmung mit anderen Providern. Somit verändert der Vorschlag nicht den Wettbewerb und greift auch nicht in die Netzneutralität ein.

INFEKTIONSSCHUTZ

Um das Risiko eingeschleppter Infektionen zu minimieren, pilotiert die Deutsche Telekom im Foyer der Konzernzentrale in Bonn eine neue Scanstation, die mobile Datenträger in Sekundenschnelle auf möglichen Virenbefall überprüft.

Das Szenario treibt IT-Sicherheitsmanagern zunehmend den Schweiß auf die Stirn: Immer mehr Mitarbeiter bringen eigene Datenträger ins Unternehmen und führen sie ungeprüft in die Firmenrechner ein. Potenziellen Angreifern kommt das Laisser-faire der Anwender mehr als gelegen: Je besser ein Firmennetz nach außen geschützt ist, desto wichtiger werden USB-Sticks, SD-Karten und DVDs, um doch noch ein Einfallstor zu finden. Stuxnet ist das wohl prominenteste Beispiel. Hier wurde einem Mitarbeiter der Urananreicherung im iranischen Natanz ein infizierter USB-Stick „zugespielt". Und tatsächlich gelang es den Angreifern, in die Leittechnik der Atomanlage einzudringen, obwohl diese rein technisch gesehen vollständig abgeschottet war.

TESTLAUF FÜR PRÜFSTATION

Die Telekom testet seit Herbst 2013 ein nutzerfreundliches Prüfgerät für mobile Datenträger. Die sogenannte Scanstation steht im öffentlich zugänglichen Eingangsbereich der Telekom Zentrale in Bonn. Neben den Mitarbeitern sind auch alle Besucher eingeladen, ihre mobilen Datenträger prüfen zu lassen. In die hölzerne Stele der Scanstation ist ein Touchscreen eingelassen, der den Nutzer auffordert, seine mobilen Datenträger einzuführen. Hierzu stehen Eingänge für USB-Sticks, SD-Karten und DVD-ROMs zur Verfügung. Anschließend führt die Scanstation den Prüfvorgang automatisch durch. Dabei werden alle Arten von Malware gesucht. Die verwendeten Suchalgorithmen stammen von vier Anbietern für Antivirensoftware.

Scanstation prüft USB-Sticks, SD-Karten und DVDs auf Malware.

Die Auswertung der auf den Datenträgern gespeicherten Daten erfolgt rein lokal in der Scanstation. Über den Touchscreen erfahren die Anwender das Ergebnis der Prüfung. Stellt die Scanstation einen Befall mit Malware fest, bietet sie an, die Schadsoftware zu entfernen. Falls die Desinfektion das Löschen von Daten erfordert, erhält der Nutzer eine entsprechende Vorabnachricht. Der Datenträgerbesitzer ist zu jeder Zeit Herr der Lage und kann entscheiden, bis zu welchem Punkt er sich unterstützen lassen will.

Zwei Welten, ein Smartphone: Mit SiMKo 3 verschlüsselt telefonieren und trotzdem im Internet surfen.

HOCHSICHERE MOBILE KOMMUNIKATION

Anfang September 2013 hat das Security-Smartphone SiMKo 3 (Sichere Mobile Kommunikation) die Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgreich abgeschlossen und offiziell die Zulassung für die Geheimhaltungsstufe VS-NfD (Verschlusssache – Nur für den Dienstgebrauch) erhalten.

Mitgliedern der Bundesregierung sowie Mitarbeitern von Ministerien und Bundesbehörden steht für besonders vertrauliche Nachrichten damit erstmals ein Mobilgerät zur Verfügung, das den neu entwickelten L4-Hochsicherheitsmikrokern als Betriebssystem in sich trägt. Im Oktober 2013 folgte der Smartphone-Variante von SiMKo 3 ein Tablet-Prototyp auf Basis des Samsung Galaxy Note 10.1.

SiMKo 3 ist nicht nur für Datenanwendungen wie Mail, Kalender, Kontakte und Aufgaben da. Schon heute lässt es sich auch als abhörsicheres Kryptotelefon verwenden, das verschlüsselte Telefonate auf Basis von Voice over IP mit hochsicheren Verschlüsselungsverfahren bietet. Zusätzlich wird für die Verwendung in Bundesbehörden der Behördenstandard SNS (Sichere Netzübergreifende Sprachverschlüsselung) in den nächsten Monaten integriert. Geht ein Gerät verloren, kann niemand durchsehen, was darauf gespeichert ist. Die certgate-Kryptokarte sorgt für die Benutzerauthentisierung und verschlüsselt alle Daten auf dem Gerät. Zudem lässt sich der Inhalt des Geräts aus der Ferne löschen.

Beide Geräte können sicher auf derselben Plattform betrieben werden, sodass für die Nutzer kein zusätzlicher Aufwand und keine Investitionen für eine zweite Infrastruktur anfallen. Bei Kern und Sicherheitstechnik des SiMKo 3 setzt die Telekom durchgängig auf Unternehmen aus Deutschland. So kommt die Kryptokarte von certgate, für verschlüsselte Verbindungen sorgt NCP – beides Unternehmen aus Nürnberg. Das L4-Mikrokernsystem haben die TU Dresden, das Dresdener Start-up Kernkonzept, die Telekom Innovation Laboratories sowie das Berliner Start-up Trust2Core entwickelt. Möglich wurde die Implementierung des Kerns durch eine besonders enge Zusammenarbeit mit Weltmarktführer Samsung.

Impressum

Herausgeber

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

Fotos

Deutsche Bahn,
Deutsche Telekom,
Fotolia, iStockphoto

Stand: 1/2014

www.telekom.com/datenschutz

www.telekom.com/sicherheit