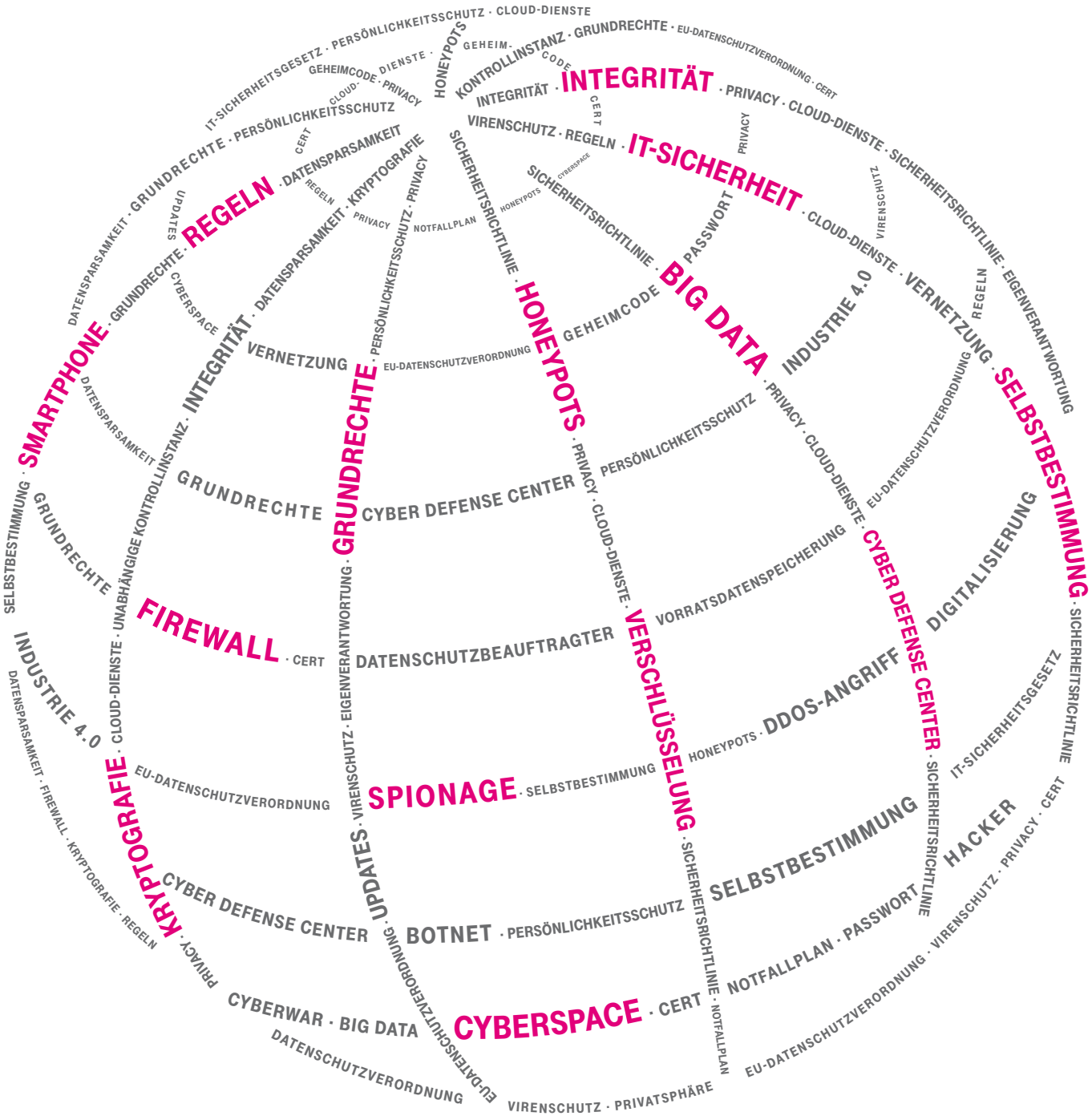


DATENSCHUTZ UND DATENSICHERHEIT

BERICHT 2014

ERLEBEN, WAS VERBINDET.

INHALT


„ALLE KONFLIKTE
FINDEN HEUTZUTAGE
AUCH IM NETZ STATT.“

Wer dachte, ein Jahr nach den Enthüllungen von Edward Snowden verlöre das Thema Cybersicherheit an Bedeutung, sieht sich getäuscht. Zwar dominierten 2014 die Krisen in der Ukraine und im Nahen Osten die Schlagzeilen der Medien und das neue Jahr hat mit schrecklichen Anschlägen islamistischer Terroristen begonnen. Aber auch diese Konflikte haben wichtige virtuelle Komponenten.

Von der Werbung neuer Kämpfer über die Propagandaschlacht in sozialen Medien bis zu Angriffen auf IT-Systeme: Es gibt heutzutage keinen Konflikt mehr, der nicht auch im Netz ausgetragen wird. Das Thema Cybersicherheit verdient also weiterhin große Aufmerksamkeit. Zumal die Angriffsflut aus Viren, Würmern und Trojanern weiter zunimmt. Allein das Frühwarnsystem der Telekom registriert bis zu eine Million Cyberattacken täglich, Tendenz steigend.

Und auch die Aufarbeitung der Snowden-Affäre ist längst nicht abgeschlossen. Noch immer haben wir kein vollständiges Bild seiner Erkenntnisse und damit fehlen uns wichtige Informationen, um die Daten unserer Kunden besser schützen zu können und mögliche Schwachstellen in den Systemen zu schließen. Die politischen Konsequenzen lassen ebenfalls weiter auf sich warten: Für mich ist es nicht nachvollziehbar, warum wir nicht zumindest innerhalb der EU auf gegenseitige Spionage verzichten können.

In unserer zunehmend vernetzten Gesellschaft müssen die Menschen Vertrauen in die digitale Welt und neue Dienste haben. Dafür sind deutlich mehr Anstrengungen nötig. Es fehlt teilweise an den Grundlagen: Die Telekom setzt sich deshalb für mehr Forschung und Bildung im Bereich Datenschutz und Cybersicherheit ein. Beispielsweise durch den eigenen Lehrstuhl, den wir an der Hochschule für Telekommunikation in Leipzig eingerichtet haben.

Wir brauchen zudem gut vernetzte schnelle Eingreiftruppen in Unternehmen, um uns gegenseitig unverzüglich über neue Gefahren informieren zu können. Die Telekom hat ihr Team im Cyber Defense Center deutlich verstärkt und fördert die Ausbildung von Spezialisten. Dafür haben wir gemeinsam mit der IHK Köln das Qualifikationsprogramm „Cyber Security Professional“ ins Leben gerufen.

„Wir brauchen gut vernetzte schnelle Eingreiftruppen in den Unternehmen.“

Die Telekom wird sich zudem auch in Zukunft für eine Ende-zu-Ende-Verschlüsselung sämtlicher Datenübertragungen einsetzen. Wichtig ist, dass Sicherheit bei allen Stufen der Wertschöpfungskette mitgedacht wird: Auch die Hersteller von Hard- und Software sollten verpflichtet werden, Sicherheitslücken schnell zu schließen. Schließlich liegt Sicherheit nicht allein in den Händen der Infrastrukturbetreiber. Wir müssen viel enger zusammenarbeiten, um unsere Gesellschaft für die Digitalisierung fit zu machen. Denn fest steht: Die Vernetzung nimmt immer weiter zu. Nicht nur Menschen, sondern auch Maschinen kommunizieren miteinander und ganze Wertschöpfungsketten werden digitalisiert. Damit steigt zwangsläufig auch die Verletzlichkeit durch virtuelle Angriffe. Mehr IT-Sicherheit sollte also weiterhin ganz oben auf der Prioritätenliste stehen.

ZUR PERSON

Dr. Thomas Kremer
ist seit Juni 2012 Vorstandsmitglied Datenschutz, Recht und Compliance sowie seit 2014 kommisarischer Personalvorstand 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.

„DEUTSCHLAND FÜHREND BEI IT-SICHERHEIT UND DATENSCHUTZ IN EUROPA“

„Die digitale Welt ist keine eigene Welt und darf kein rechtsfreier Raum sein“, sagt Bundesinnenminister **Dr. Thomas de Maizière** im Interview für den „Bericht Datenschutz und Datensicherheit“ der Deutschen Telekom.

Herr Minister, warum brauchen wir eine Reform des Datenschutzes?
Dr. Thomas de Maizière: Die Möglichkeiten, Daten aufzuzeichnen und zusammenzuführen, sind in den vergangenen Jahren rasant gewachsen. Eine aktuelle Studie der Marktforschungsfirma Gartner spricht davon, dass bis 2020 mehr als 30 Milliarden Geräte miteinander vernetzt sein werden. Daten fallen fast überall an: in Alltags- und Haushaltsgeräten, intelligenten Stromzählern ebenso wie in Autos und Maschinen. Es entsteht ein riesiges Potenzial für neue Produkte und Geschäftsmodelle. Diese Entwicklung wird oft auch mit dem Stichwort „Big Data“ assoziiert. Es sind erst die großen Mengen an Informationen, die beispielsweise durch Zusammenführung in Profilen uns zum einen neue Erkenntnisse und Chancen ermöglichen, zum anderen aber auch neue Risiken für die Privatsphäre in sich bergen. Hierauf muss auch das Datenschutzrecht Antworten geben. Wir brauchen auch ein gemeinsames Datenschutzrecht in der EU. Der deutsche Rechtsrahmen ist zu klein angesichts des Internets. Chancengleichheit hilft auch deutschen Anbietern.

Muss es also für die digitale Welt zukünftig spezielle Rechte geben?
Dr. Thomas de Maizière: Die digitale Welt ist keine eigene Welt und darf kein rechtsfreier Raum sein. Prinzipiell muss also das Gleiche gelten wie in der sogenannten analogen Welt. Natürlich benötigt man in Bezug auf die Besonderheiten des Internets angepasste Regelungsmechanismen, andere Instrumente. Das kennen wir ja schon bei anderen neuen Entwicklungen. Aber es wäre verfehlt, zu behaupten, das Internet und alles, was damit verbunden ist, würden per se einen eigenen, in sich geschlossenen Regulations- und Wertemechanismus brauchen.

Wie können wir uns diese „angepassten Regelungsmechanismen“ denn vorstellen?
Dr. Thomas de Maizière: Der Datenschutz muss seine Steuerungsfunktion in den neuen Datenverarbeitungsprozessen behalten. In dem Maße, in dem sich Umschlag und Verknüpfung von Daten vermehren, müssen die Mechanismen zum Schutz der Privatsphäre angepasst werden. Transparenz und Informiertheit, Fremdsicherung und Selbstdatenschutz bilden den Rahmen

> „DER ANREIZ FÜR DEN BÜRGER, DATEN IN FREMDE HÄNDE ZU GEBEN, STEIGT MIT DER KLARHEIT DES SCHUTZKONZEPTS UND DESSEN EFFEKTIVEM VOLLZUG.“

auch für Big Data. Von der Datensouveränität haben beide Seiten etwas: Der Anreiz für den Bürger, Daten in fremde Hände zu geben, steigt mit der Klarheit des Schutzkonzepts und dessen effektivem Vollzug. Regelungsmechanismen für ganz Europa dienen diesem Ziel. Nichts macht im Internetzeitalter an Landesgrenzen so wenig halt wie unsere Daten. Deshalb bedeutet Anpassung auch und in erster Linie Harmonisierung und Durchsetzbarkeit allgemeingültiger Regeln.

Wie laufen die Verhandlungen in Brüssel um die europäische Datenschutzgrundverordnung aus Ihrer Sicht?
Dr. Thomas de Maizière: Wir machen Fortschritte. Der Europäische Rat möchte die Verhandlungen der Datenschutz-Grundverordnung in diesem Jahr abschließen. Daher arbeiten die Mitgliedstaaten seit Monaten intensiv daran, sich zu ausgewählten Teilen der Grundverordnung zu einigen. Diese Einigungen stehen zwar unter dem Vorbehalt einer Gesamteinigung, aber es ist ein Instrument gefunden, mit dem sich der Rat kapitelweise einer Gesamteinigung nähert.

Welche Themen werden denn in Brüssel aktuell diskutiert?
Dr. Thomas de Maizière: Es geht in Brüssel um das Viereck Bürgernähe, Rechtssicherheit, Modernisierung und Harmonisierung. Der Bürger kann sich der Integrität seiner Privatsphäre nur sicher sein, wenn ihm die Institutionen vor Ort größtmöglichen Schutz gewähren. Die Behauptung der europäischen Internetwirtschaft gegenüber den großen Konzernen außerhalb Europas kann nur gelingen, wenn diese sich europäischem Recht unterwerfen.
Die Internettauglichkeit ist ohne Regeln zur Pseudonymisierung und Profilbildung nicht zu denken.

Gerade das Beispiel der Profilbildung zeigt doch, wie wichtig klare Regelungen zum Schutz der Betroffenen sind …
Dr. Thomas de Maizière: Richtig! Und es zeigt, wie schwierig es ist, diese mit den berechtigten Interessen der Unternehmen an einer solchen Auswertung von Daten in einen angemessenen Ausgleich zu bringen. Schließlich ermöglichen Profilbildungen oft auch wertvolle Erkenntnisse. Deswegen setzt sich die Bundesregierung für klare rechtliche Regelungen ein.

Müssen wir nicht auch stärker den technischen Datenschutz einbeziehen?
Dr. Thomas de Maizière: Das ist unser erklärtes Ziel. Deshalb setze ich mich für eine Stärkung des Konzepts der Pseudonymisierung in der Datenschutz-Grundverordnung ein. Damit wird die Identifizierung der Personen erheblich erschwert, von denen die Daten ursprünglich stammen. So kann den Betroffenen die Sorge genommen werden, dass ihre persönlichen Daten bei Big-Data-Anwendungen missbräuchlich genutzt werden. Indem man zugleich Unternehmen in weiterem Umfang als sonst die Verarbeitung pseudonymisierter Daten erlaubt, schafft man außerdem Anreize, die Pseudonymisierung tatsächlich auch durchzuführen. Deutschland hat deshalb einen eigenen Vorschlag auf EU-Ebene gemacht. In Bezug auf den technischen Datenschutz ist darüber hinaus eine weitere Regelung zum Datenschutz „by design“ und „by default“ zu erwähnen. Danach sollen die Verarbeiter zu datenschutzfreundlichen Voreinstellungen verpflichtet werden.

Wir sprechen über Datenschutz in der EU und gerade haben Sie auch das deutsche Datenschutzrecht angesprochen. Wie steht es mit internationalen Unternehmen, gerade auch aus den USA?
Dr. Thomas de Maizière: Wir werden in der Datenschutz-Grundverordnung das Marktortprinzip verankern, das heißt, das einfache Prinzip wird sein: „Unser Markt, unsere Regeln.“ Damit gilt das europäische Datenschutzrecht auch für alle Unternehmen aus Asien oder den Vereinigten Staaten, die ihre Dienste oder Waren in der EU anbieten – und zwar unabhängig davon, ob sie hier eine Niederlassung haben oder nicht. Wir wollen „Forum Shopping“ verhindern, gleiche Wettbewerbschancen schaffen und ein europaweites Niveau für den Schutz der Privatsphäre des Bürgers garantieren.

Sie sind nicht nur für das Datenschutzrecht, sondern auch für die IT-Sicherheit zuständig. Die Bundesregierung hat unter Ihrer Federführung den Entwurf für ein IT-Sicherheitsgesetz vorgelegt. Welches Ziel verbinden Sie mit diesem Gesetz?
Dr. Thomas de Maizière: Kern des Vorhabens ist es, die IT-Systeme in den Bereichen, die für unsere Gesellschaft von elementarer Bedeutung sind, gegen Angriffe und Störfälle abzusichern. Das betrifft insbesondere die Energieversorgung und das Gesundheitswesen bis hin zu Banken und Versicherungen. Hierzu führen wir branchenweit einheitliche Sicherheitsstandards und Meldepflichten ein. Damit wird das IT-Sicherheitsniveau in diesen Bereichen spürbar angehoben und zugleich unser Bild von der tatsächlichen Gefährdungslage im Cyberraum deutlich geschärft. Wir schaffen es auf diesem Weg auch, dass die Nutzung des Internets sicherer wird. Und nicht zuletzt stärken wir das Bundesamt für Sicherheit in der Informationstechnik und bauen die Ermittlungszuständigkeiten des Bundeskriminalamts im Bereich des Cybercrime weiter aus.

Das Vorhaben ist zu Beginn in der Wirtschaft auf große Skepsis gestoßen. Wie sind Sie dem begegnet?
Dr. Thomas de Maizière: Nach meinem Eindruck hat sich inzwischen auch in der Wirtschaft die Erkenntnis durchgesetzt, dass wir angesichts der unverändert angespannten IT-Sicherheitslage dringend etwas für die IT-Sicherheit unserer kritischen Infrastrukturen tun müssen. Dabei war es mir wichtig, auf die bestehenden Kooperationsformen zwischen Staat und Wirtschaft aufzusetzen und von Anfang an für ein transparentes Verfahren zu sorgen. So hat sich im Laufe der Ressortabstimmung eine sachorientierte Debatte über den Gesetzentwurf entwickelt, aus der wir noch viele gute Anregungen zur weiteren Verbesserung unserer Regelungsvorschläge bekommen haben. Dies hat die Akzeptanz bei den Unternehmen deutlich erhöht.

Auch bei der IT-Sicherheit müssen wir die europäische Ebene im Blick haben. Haben Sie nicht die Sorge, dass die derzeit in Brüssel verhandelte Richtlinie zur Netz- und Informationssicherheit Ihre nationalen Bemühungen obsolet macht oder gar konterkariert?

Weiter auf Seite 8 >

Dr. Thomas de Maizière: Nein. Die Arbeiten am IT-Sicherheitsgesetz und die Verhandlungen in Brüssel liegen in meinem Haus in einer Hand. Unser Ziel ist es, in den von der Richtlinie erfassten Bereichen einen größtmöglichen Gleichklang zu erreichen. Natürlich ist es eine große Herausforderung, zwei Vorhaben von solcher Komplexität und Reichweite zu synchronisieren. Zumal wir ja bekanntermaßen nur einer von 28 Mitgliedstaaten sind. Mit dem IT-Sicherheitsgesetz haben wir aber nunmehr national ein Zeichen gesetzt, das nach meinem Eindruck auch in Brüssel verstanden worden ist.

Wenn man über die Verbesserung der IT-Sicherheit spricht, muss man auch über die deutsche IT-Sicherheitswirtschaft reden. Wie bewerten Sie die Rolle der nationalen IT-Sicherheitswirtschaft, auch und gerade nach den Snowden-Veröffentlichungen?

Dr. Thomas de Maizière: Unsere IT-Sicherheitswirtschaft zählt zu den leistungsfähigsten deutschen Zukunftsbranchen. Die über 9.000 überwiegend kleinen und mittleren Unternehmen sind für sichere und zuverlässige Speziallösungen bekannt, die auch im Ausland unter dem Siegel „Made in Germany“ erfolgreich vermarktet werden. Denken Sie nur an die Kompetenzen dieser Unternehmen in den Bereichen der Verschlüsselungstechnologien und der Kryptohardware. Dieses Potenzial werden wir nutzen, um das Vertrauen der Nutzerinnen und Nutzer in sichere digitale Infrastrukturen nachhaltig zu stärken.

ZUR PERSON

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

STRENGERE DATENSCHUTZREGELN ALS ANTRIEB FÜR DEN DIGITALEN BINNENMARKT IN EUROPA

„Zu meinen wichtigsten Prioritäten für 2015 gehören der Abschluss der Reform der Europäischen Datenschutzregelungen und die Wiederherstellung des Vertrauens in den transatlantischen Datenverkehr“, sagt Věra Jourová, EU-Kommissarin für Justiz und Verbraucherschutz.

Seit der Einführung der bestehenden Datenschutzrichtlinie 1995 haben technologischer Fortschritt und Globalisierung die Art und Weise, wie unsere Daten verarbeitet werden, grundlegend verändert. Gerade im Internet und in den sozialen Medien stellt uns der Schutz der Privatsphäre und unserer Daten immer wieder vor neue Herausforderungen. 92 Prozent der Europäer haben heute die Sorge, dass ihre Daten von mobilen Apps gesammelt werden, ohne dass sie darin eingewilligt haben. Und 89 Prozent wollen wissen, wann die auf ihrem Smartphone gespeicherten Daten an Dritte weitergegeben werden.
Die geltenden Regeln müssen an die neuen Gegebenheiten angepasst werden. Nur so ist es möglich, für unsere Bürgerinnen und Bürger ein hohes Schutzniveau und freien Datenfluss sicherzustellen. Zur Stärkung der Persönlichkeitsrechte im Internet und zur Förderung von Europas digitaler Wirtschaft hat die Europäische Kommission daher im Januar 2012 eine Reform der EU-Datenschutzrichtlinie vorgeschlagen. Der Abschluss dieser Reform ist ein zentraler Baustein sowohl für den Bereich Justiz und Grundrechte als auch für den digitalen Binnenmarkt – zwei der zehn Schlüsselprojekte der Kommission. Daher ist es wichtig, die laufenden Verhandlungen über die Reform zügig abzuschließen und die neuen Regeln zu implementieren. Dabei können wir auf die in den letzten Monaten erzielten guten Fortschritte aufbauen. Unser Ziel ist und bleibt es, die Verhandlungen erfolgreich abzuschließen und die Reform gemeinsam mit den Co-Gesetzgebern in 2015 zu verabschieden.

AUFBAU EINES DIGITALEN BINNENMARKTES

Daten sind in unserer Zeit eine starke Währung. Die einzige Möglichkeit, das Vertrauen der Menschen in das Internet, Datenströme und auch in neue Technologien im Allgemeinen zu bewahren, ist ein robustes Datenschutzrecht, das auch effektiv durchgesetzt wird. Denn Datenschutz ist nicht nur ein Recht. Datenschutz und das Vertrauen, das durch die effektive Durchsetzung der anwendbaren Regelung entsteht, sind Voraussetzung für den digitalen Binnenmarkt. Durch die geplante Datenschutz-Grundverordnung werden die Europäischen Datenschutzgesetze harmonisiert. An Stelle von 28 verschiedenen nationalen Datenschutzgesetzen gilt in Europa in Zukunft nur noch ein Regelwerk. Um die Dinge zu vereinfachen, werden wir Verwaltungsaufwand reduzieren und Bürokratie abbauen, wie zum Beispiel unnötige Meldepflichten für Unternehmen. Damit entlasten wir die Unternehmen und erhöhen die Rechtssicherheit für ihre Geschäfte. Die Reform schafft gleiche Wettbewerbsbedingungen für die digitale Wirtschaft in Europa: Unternehmen aus Drittländern wie den USA müssen sich mit ihren Angeboten in Europa an unsere Spielregeln halten und dasselbe Datenschutzniveau wie ihre europäischen Wettbewerber gewährleisten.

Ein umfassendes und modernes Datenschutzrecht schafft Vertrauen unter den Verbrauchern. Menschen, die auf den Schutz ihrer persönlichen Daten vertrauen können, werden eher geneigt sein, Waren und Dienstleistungen online zu kaufen. Unternehmen, die verantwortungsbewusst mit personenbezogenen Daten umgehen, haben einen Wettbewerbsvorteil. Ein klares und durchsetzbares Datenschutzrecht wird den digitalen Binnenmarkt voranbringen. Die potenziellen Vorteile eines digitalen Binnenmarkts sind immens. Doch um ihn zu ermöglichen, müssen wir uns auf neue Technologien wie Big Data, Cloud Computing und das Internet der Dinge einstellen. Diese Technologien und diese Investitionen werden den europäischen Markt nur erreichen, wenn klare Datenschutzbestimmungen gelten. Das Europäische Parlament hat die Bedeutung der

> „EIN UMFASSENDES UND MODERNES DATENSCHUTZRECHT SCHAFFT VERTRAUEN UNTER DEN VERBRAUCHERN.“

ZUR PERSON

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

Datenschutzreform schon früh erkannt. Mit echter Führungsstärke wurde ein breiter Konsens für die Unterstützung der Vorschläge der Kommission gefunden. Die Mitgliedsstaaten haben mehr Zeit gebraucht, da ihre Positionen weiter auseinander lagen. Jetzt haben sie jedoch begonnen, sich anzunähern und gemeinsam voranzuschreiten. Die EU-Staats- und Regierungschefs haben die Bedeutung „einer starken EU-Datenschutz-Grundverordnung bis 2015“ bekräftigt. Dies kommt keine Minute zu früh. Die Welt wartet nicht auf uns. Wenn wir den Erfolg des digitalen Binnenmarkts in Europa wollen, muss uns die Datenschutzreform gelingen – und zwar bald. Die Bürgerinnen und Bürger und die Unternehmen in Europa warten darauf.

DAS RECHT AUF VERGESSENWERDEN („GOOGLE-ENTSCHEIDUNG“)

Das Vertrauen wiederherzustellen, ist jedoch nicht alleinige Aufgabe der EU. Die Wirtschaft muss ebenfalls ihren Beitrag leisten. Als Reaktion auf das jüngste Urteil des Europäischen Gerichtshofs zum Recht auf Vergessenwerden wurde der Vorwurf der „Zensur“ laut. In Wirklichkeit gibt die „Google-Entscheidung“ den Menschen keinen Freibrief, die Löschung von Inhalten aus dem Internet zu verlangen, nur weil diese ihnen nicht zusagen. Die Entscheidung mahnt eine ausgewogene Balance zwischen den legitimen Interessen von Internet-Nutzern und den Grundrechten der Bürger an. Eine Balance, die in jedem Einzelfall gefunden werden muss. Der Gerichtshof hat klargestellt, dass Suchmaschinen persönliche Daten kontrollieren und Unternehmen wie Google sich deshalb beim Umgang mit personenbezogenen Daten nicht ihrer Verantwortung nach europäischem Recht entziehen können. Wir sollten uns auch der Tatsache bewusst sein, dass das Recht auf Vergessenwerden weder von der Kommission noch vom Gerichtshof soeben erst erfunden wurde. Es war bereits Bestandteil der Bestimmungen von 1995. Mit der Datenschutzreform aktualisieren wir dieses Prinzip und schaffen eine eindeutige Regelung für das digitale Zeitalter. Damit machen wir deutlich, dass die EU-Bestimmungen für alle Unternehmen gelten, die europäischen Verbrauchern Produkte oder Dienstleistungen anbieten – unabhängig davon, ob sich ihre Server innerhalb oder außerhalb der EU befinden. Wie die Gerichtsentscheidung, so hat auch die Datenschutzreform das Ziel, für eine gerechte Balance der Rechte zu sorgen: Wir wollen den Bürgerinnen und Bürgern die Kontrolle über ihre persönlichen Daten geben und gleichzeitig die Meinungs- und Medienfreiheit ausdrücklich schützen. Wir wollen die Rechte der Menschen stärken und verlässliche Bedingungen für Unternehmen im digitalen Binnenmarkt schaffen.

INTERNATIONALE DATENSTRÖME

Zu meinen obersten Prioritäten zählt auch, das Recht auf Datenschutz in unseren Beziehungen zu anderen Ländern zu bewahren. Ich will dafür sorgen, dass unsere Safe-Harbor-Vereinbarung mit den USA auch wirklich sicher ist. Darüber hinaus sollen alle EU-Bürger Datenschutzbestimmungen auch vor US-amerikanischen Gerichten durchsetzen können. Werden personenbezogene Daten zu kommerziellen Zwecken transatlantisch übermittelt, ist die Safe-Harbor-Vereinbarung mit den USA für Europäer die wichtigste Grundlage für den Schutz ihrer Daten. Bürgerinnen und Bürger in Europa fragen sich: Wie sicher ist Safe-Harbor eigentlich? Schützt es unsere persönlichen Daten? Brauchen wir es überhaupt?
Vor allem möchte ich das Safe-Harbor-Abkommen verbessern. Geschäftliche Beziehungen mit den USA sind wichtig – sowohl für uns als auch für unsere amerikanischen Partner. Trotzdem sollten Geschäftschancen nicht auf Kosten der Grundrechte unserer Bürgerinnen und Bürger realisiert werden. In der Europäischen Union hat jeder das grundlegende Recht auf Schutz seiner persönlichen Daten. Dieses Grundrecht gilt unabhängig davon, wo die Daten erhoben oder verarbeitet werden. Wir haben hohe Standards in Europa und wir müssen dafür sorgen, dass diese Standards sowohl in der Europäischen Union als auch international respektiert werden.
Wir machen auf diesem Gebiet zwar Fortschritte, aber es gibt noch einiges zu tun. Mein Ziel ist es, das Safe-Harbor-Abkommen in den kommenden Monaten zu verbessern. Die Aussetzung des Abkommens bleibt jedoch als Möglichkeit bestehen, sollten die Verhandlungen nicht zu dem gewünschten Ergebnis führen.
Darüber hinaus setze ich die Verhandlungen mit den USA über eine Rahmenvereinbarung zum Datenschutz für den Datenaustausch im Bereich der Strafverfolgung fort. Es ist mein Wunsch, dass wir unsere wichtige transatlantische Kooperation bei der Strafverfolgung verstärkt fortsetzen. Dafür brauchen wir jedoch ein solides Gerüst von Datenschutzbestimmungen, die für beide Seiten akzeptabel sind. In diesem Bereich sind ebenfalls Fortschritte erzielt worden, aber wir warten noch auf eine Gesetzesänderung des US-amerikanischen Kongresses, damit EU-Bürger ihre Datenschutzrechte vor amerikanischen Gerichten genauso wie US-Bürger geltend machen können. Ein aufgewertetes Safe-Harbor-Abkommen und eine europäisch-amerikanische Rahmenvereinbarung wären ein großer Schritt vorwärts für die transatlantische Kooperation im Datenschutz. Dies wäre auch ein wichtiges Signal für andere europäisch-amerikanische Schlüsselprojekte wie zum Beispiel TTIP.

Das müssen wir schaffen.

MEHR RECHTSKLARHEIT UND RECHTSSICHERHEIT

Die europäische Datenschutz-Grundverordnung könnte aufgrund des Marktortprinzips und der Regelungen für Datenübermittlungen in Drittstaaten weit über Europa hinausreichen, glaubt **Andrea Voßhoff**, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Wie schätzen Sie die aktuellen Entwicklungen zum Datenschutz auf europäischer Ebene ein?
Andrea Voßhoff: Die Entwicklungen auf EU-Ebene stimmen mich grundsätzlich positiv. Das Europäische Parlament hat mit seinem Beschluss vom März 2014 zahlreiche sinnvolle Verbesserungen des Kommissionsentwurfs der Datenschutz-Grundverordnung vorgeschlagen und hiermit einen wichtigen Beitrag für das Reformvorhaben geleistet. Ich hoffe jetzt, dass der Rat in den kommenden Monaten seine Beratungen ebenfalls abschließt und zu einer einheitlichen Position findet. In Teilbereichen, wie dem Marktortprinzip und der Regelung von Drittstaatenübermittlungen sowie der für Deutschland wichtigen Frage, in welchem Umfang bestehendes Datenschutzrecht im öffentlichen Bereich, etwa im Gesundheits- oder Sozialbereich, beibehalten werden kann, ist dies erfreulicherweise ja bereits erfolgt.

Was sind wichtige Schwerpunkte, um ein angemessenes Datenschutzniveau in Europa zu erreichen?
Andrea Voßhoff: Zunächst halte ich eine europäische Datenschutz-Grundverordnung aus grundsätzlichen datenschutzpolitischen Erwägungen für notwendig: Zum einen kann sie angesichts globaler Datenströme und globaler Herausforderungen einen hohen Standard setzen, dessen Wirkung aufgrund des Marktortprinzips und der Regelungen für Datenübermittlungen in Drittstaaten weit über Europa hinausreicht. Zweitens trägt sie für Bürgerinnen und Bürger sowie für Unternehmen zu mehr Rechtsklarheit und Rechtssicherheit bei, denn als künftig unmittelbar geltendes Recht vereinheitlicht sie die unterschiedlichen datenschutzrechtlichen Ansätze in den 28 EU-Mitgliedstaaten. Und drittens modernisiert sie das 20 Jahre alte europäische Datenschutzrecht ohne dabei die bewährten Prinzipien der EG-Datenschutzrichtlinie aus dem Jahre 1995 aufzugeben.

Was die Schwerpunkte der Datenschutz-Grundverordnung anbelangt, so muss zunächst abgewartet werden, worauf sich das Parlament und der Rat am Ende des Gesetzgebungsverfahrens einigen. Von der Grundtendenz her halte ich den von der Europäischen Kommission mit ihrem Vorschlag aus dem Jahre 2012 eingeschlagenen Weg der Beibehaltung der bewährten Grundprinzipien des Datenschutzes bei gleichzeitiger Stärkung der Betroffenenrechte und der Präzisierung der Verpflichtungen der verantwortlichen Stelle, für richtig. Besonders zu erwähnen sind auch die beabsichtigten gesteigerten Anforderungen an den technologischen Datenschutz.

Ebenso befürworte ich im Grundsatz die neuen Formen der Zusammenarbeit der Datenschutzbehörden im Rahmen des „One-Stop-Shop“ und des Kohärenzverfahrens. Auch die verbesserten Sanktionsmöglichkeiten, die den Aufsichtsbehörden künftig zur Verfügung stehen sollen, sind sachgerecht. Ein weiteres wichtiges Thema betrifft die Frage, wie mit Persönlichkeitsprofilen umgegangen werden soll. Das Europäische Parlament hat hier Vorschläge gemacht, die in die richtige Richtung gehen, indem es eine Definition der Profilbildung fordert und die Voraussetzungen, unter denen Persönlichkeitsprofile erstellt und genutzt werden dürfen, gegenüber der jetzigen Rechtslage präzisiert.

Ist Ihre Behörde und sind die Landesbehörden mit Blick auf die neuen Entwicklungen gut aufgestellt?

Andrea Voßhoff: Die Aufsichtsbehörden des Bundes und der Länder werden sich den Aufgaben und Herausforderungen vor allem auf europäischer und internationaler Ebene stellen. Es ist absehbar, dass zum Beispiel die neuen Formen und Verfahren der Kooperation und Zusammenarbeit der Datenschutzbehörden im Rahmen des „One-Stop-Shop“ und des Kohärenzverfahrens im Europäischen Datenschutzausschuss zu einem deutlich erhöhten Fallaufkommen führen werden. Die Datenschutz-Grundverordnung sieht zudem zusätzliche Aufgaben der Datenschutzaufsicht in unterschiedlichen Bereichen vor, etwa bei der Vorabprüfung risikoreicher Datenverarbeitungen, im Rahmen von Zertifizierungen oder in Bezug auf Drittstaatenübermittlungen. Ganz generell werden die Herausforderungen an den Datenschutz mit zunehmender Digitalisierung und Vernetzung aller Gesellschafts- und Lebensbereiche steigen. Die Behörden müssen hierfür in sachlicher und personeller Hinsicht gestärkt werden, und zwar bevor die Datenschutz-Grundverordnung in Kraft tritt.

Andrea Voßhoff ist seit Januar 2014 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

> „DIE EIGENTLICH BEMERKENSWERTE AUSSAGE DES EUGH-URTEILS ZU GOOGLE IST, DASS EUROPÄISCHES DATENSCHUTZRECHT AUCH FÜR UNTERNEHMEN AUSSERHALB DER EU GILT.“

Werden durch die neuen Regelungen Wettbewerbsnachteile der europäischen Industrie gegenüber anderen Unternehmen ausgeglichen und wenn ja, wie wird das nachgehalten werden?

Andrea Voßhoff: Die Datenschutz-Grundverordnung wird für Unternehmen bereits deshalb Vorteile gegenüber der bisherigen Situation bieten, weil sie das regulatorische Umfeld innerhalb der EU vereinheitlicht und gegenüber der jetzigen Rechtslage vereinfacht. Unternehmen, die in unterschiedlichen EU-Mitgliedstaaten niedergelassen und tätig sind, müssen sich künftig nicht mehr mit unterschiedlichen nationalen Datenschutzgesetzen, sondern ausschließlich mit der Datenschutz-Grundverordnung befassen, die überall in der EU einheitlich gilt. Die Regeln der Datenschutz-Grundverordnung gelten durch das Marktortprinzip zudem auch für Unternehmen aus Drittstaaten, so dass diese bei Betätigung auf dem europäischen Markt in puncto Datenschutz denselben Wettbewerbsbedingungen unterliegen. Schließlich wird mit der Einführung des "One-Stop-Shops" eine Forderung der Wirtschaft nach weniger Bürokratie umgesetzt. Ich halte es für sinnvoll, dass die Wirksamkeit dieser neuen

Andrea Voßhoff: „Der Begriff Big Data scheint auf den ersten Blick unvereinbar mit datenschutzrechtlichen Grundsätzen. Aber ist das wirklich so?“

Instrumente in der Praxis überprüft wird. Daher befürworte ich die im Entwurf der Datenschutz-Grundverordnung vorgesehene Evaluierungsklausel.

Wie sehen Sie in diesem Zusammenhang das Urteil des EuGH zu Google? Hat es auch Auswirkungen auf andere wirtschaftliche Bereiche als die Suchmaschinen-Betreiber?
Andrea Voßhoff: Vordergründig betrachtet garantiert das EuGH-Urteil den Internet-Nutzern das „Recht auf Vergessenwerden“ in der Suchmaschine von Google. Andere Suchmaschinenbetreiber sehen sich ebenfalls in der Pflicht und befolgen berechtigte Löschanträge von Nutzern. Die eigentlich bemerkenswerte Aussage des EuGH ist jedoch, dass europäisches Datenschutzrecht auch für Unternehmen außerhalb der EU gilt, wenn die Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung in einem EU-Land ausgeführt wird. Es reicht dabei aus, dass die Niederlassung die Datenverarbeitung unterstützt und fördert, zum Beispiel durch Werbemaßnahmen. Insoweit findet das Urteil nicht nur Anwendung für Google und andere Suchmaschinenbetreiber, sondern hat auch Auswirkungen auf andere Online-Bereiche.

Halten Sie Transparenz- und Widerspruchslösungen im Gegensatz zu reinen Einwilligungslösungen für ein taugliches Mittel zur Rechtfertigung von Datenverarbeitungen?
Andrea Voßhoff: Die Einwilligung trägt dem Recht auf informationelle Selbstbestimmung in besonderer Weise Rechnung, weil die Betroffenen vor Beginn der Datenverarbeitung um Zustimmung gefragt werden müssen. Hiervon unterscheidet sie sich von Widerspruchslösungen, bei denen die Betroffenen oft erst nachträglich von der Verarbeitung ihrer Daten erfahren und hiergegen vorgehen können. Widerspruchslösungen sind daher immer ein Weniger zu der Einwilligung. Die Einwilligung ist nach deutschem und europäischem Recht allerdings an strenge Voraussetzungen geknüpft - sie muss ausdrücklich erfolgen, auf einer freien Entscheidung beruhen und in Kenntnis aller relevanten Umstände erklärt werden. Daran müssen sich auch Anbieter aus anderen Ländern halten, wenn sie sich auf die Einwilligung ihrer Nutzer berufen. Ziel muss es sein, den hohen europäischen und deutschen Datenschutzstandards auch und gerade im Kontext der globalen Online-Datenverarbeitung zu mehr Wirksamkeit zu verhelfen - und eben nicht, die europäischen Standards vor dem Hintergrund internationaler Gepflogenheiten aufzuweichen.

Sollten Big-Data-Modelle weniger strengen Anforderungen unterliegen, um die für die Gesellschaft wichtigen Informationen heben zu können?
Andrea Voßhoff: Der Begriff „Big Data“ – schillernd und mysteriös zugleich – scheint auf den ersten Blick unvereinbar mit datenschutzrechtlichen Grundsätzen. Aber ist das wirklich so? Natürlich werden bei den bislang bekannten Big-Data-Modellen riesige Datenmengen verarbeitet und es besteht die Gefahr, die ursprünglich rechtmäßig für einen bestimmten Zweck erhobenen Daten nun zweckentfremdet zu verwenden. Gerade aus diesem Grund müssen die bekannten und bewährten Datenschutzgrundsätze wie Datensparsamkeit und Zweckbindung besonders beachtet werden. Zudem sollten stärker noch als bisher Konzepte zur Pseudonymisierung und Anonymisierung entwickelt werden. Vielfach erfüllen anonymisierte Datenbestände den mit der Big-Data-Anwendung angestrebten Zweck.

Wenn Sie sich aus Datenschutzsicht etwas von einem Unternehmen wünschen würden, was wäre Ihr vordringlichster Wunsch?
Andrea Voßhoff: Auch wenn sich Wünsche mit meinem Amt nicht gut vereinbaren lassen, so wäre ich dennoch zumindest zufrieden, wenn alle Unternehmen den Grundgedanken „Datenschutz als Wettbewerbsvorteil“ noch stärker in ihrem Bewusstsein verankern würden. Die wesentlichen Vorgaben von Privacy by Design und Privacy by Default sollten zum Mindeststandard bei allen Projekten gehören. Bei gewissenhafter Umsetzung dieser Vorgaben gibt es im Ergebnis nur Gewinner: die Unternehmen, die Kunden und nicht zuletzt der Datenschutz.

ZUR PERSON

Andrea Voßhoff
ist seit Januar 2014 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Die Rechtswissenschaftlerin war von 1998 bis 2013 Mitglied des Deutschen Bundestages und dort ordentliches Mitglied im Rechtsausschuss. Von 2010 bis 2013 übernahm Andrea Voßhoff in der CDU/CSU-Bundestagsfraktion die Aufgabe als Rechtspolitische Sprecherin.

DATENSCHUTZ UND DATENSICHERHEIT – EUROPAS ROLLE IN DER WELT

„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten“ – so besagt es Artikel 8 der Charta der Grundrechte der EU. Damit hebt die EU den Datenschutz auf eine Ebene mit anderen Grundrechten wie der Menschenwürde oder der Meinungsfreiheit und nimmt die Rolle eines globalen Vorreiters ein. Im Grundgesetz findet das Wort „Datenschutz“ keine explizite Nennung.

Wie keine andere technische Revolution verändert die Digitalisierung unser Sozial- und Arbeitsverhalten, unsere Kommunikation, Wettbewerbsfähigkeit, das Verhältnis von Staaten zueinander, die Strafverfolgung, Einzel- und Eigentumsrechte, Urheberrecht und geistiges Eigentum bis hin zum Grundrecht auf Datenschutz oder noch darüber hinausgehend die Privatsphäre.

Die Herausforderungen, die mit der technologischen Entwicklung, dem Internet und der Globalisierung einhergehen, sind in ihrem Ausmaß weder vollständig realisiert noch rechtsstaatlich reguliert. Wer heute den Umgang mit Daten regulieren will, sieht sich konfrontiert mit Fragen von
- Grundrechtsschutz: Datenschutz, Privatsphäre, Menschenwürde, Meinungsfreiheit, Pressefreiheit, Eigentumsfreiheit
- globalem Wettbewerb und Wachstum: Wertschöpfung, Innovation
- Datensicherheit und Sicherheitsbelangen: Strafverfolgung, Nachrichtendienste, Cyber-Abwehr, Verteidigung.

DATENSKANDALE ERSCHÜTTERN DAS VERTRAUEN

Strukturen verschwimmen zunehmend, Datenskandale erschüttern das Vertrauen der Verbraucher und daher müssen sich die entsprechenden Kontrollbehörden, z.B. Kartellämter und die höchstrichterlichen Rechtsprechungen ändern. Es muss umgedacht werden: Das Bild, das der Staat der „Feind“ der Freiheit des Einzelnen ist, lässt sich bei den heute existierenden Datenmonopolisten kaum aufrechterhalten. Die Privatsphäre des Einzelnen wird heute nicht durch den Staat bedroht und dennoch wird es eine Privatsphäre, wie wir sie vor zehn Jahren noch kannten, in der Zukunft so nicht mehr geben. Sie wird sich ändern und wir sind als Gesetzgeber aufgefordert, einen neuen Ansatz zu finden. Wenn Daten die Währung der Zukunft darstellen, dann müssen auch Kartellämter auf Datenmonopole reagieren!

Datensicherheit muss in der europäischen Forschung und innovativen Unternehmen immer wieder neu überprüft werden, um diese gegen Ausspähung sicherer zu machen. Verschlüsse-

> „Überall dort, wo Daten von EU-Bürgern verarbeitet werden, soll auch EU-Recht gelten.“

lungstechnologie wird eine neue Rolle spielen. Dort, wo Gesetzgebung die rechtliche Verwirklichung von Grundrechten meint, prallen unterschiedliche politische Kulturen und Wertvorstellungen aufeinander. Der Datenschutz und die Datensicherheit gehören längst dazu und sind fest in der politischen Agenda verankert. Die Juncker-Kommission hat mit Günther Oettinger einen Kommissar für digitale Wirtschaft und Gesellschaft und mit Andrus Ansip einen Kommissar für den digitalen Binnenmarkt. Damit dürfte auch jeder verstanden haben, dass die EU die Rolle eines Vorreiters in digitalen Fragen einnehmen will. Europa hat erkannt, dass die USA die absolute Hauptrolle spielen, aber auch, dass es nicht mehr die zweite Geige spielen will.

EU-USA-RAHMENABKOMMEN SCHLEUNIGST VERABSCHIEDEN

Die Aufgabe der EU wird es sein, für ihre Bürger ein rechtliches Umfeld zu schaffen, welches das Vertrauen der Verbraucher in die digitale Nutzung durch starke Rechte herstellt, gleichzeitig aber Innovationen und damit Wachstum und Wettbewerb im Datenbereich zulässt. Ziel muss es sein: Überall dort, wo Daten von EU-Bürgern verarbeitet werden, soll auch EU-Recht gelten. Besonderes Augenmerk muss auf den Transfer von Daten europäischer Bürger in Drittstaaten gelegt werden. Hier zeigt sich Europa entschlossener und fordernder: Da ein globales „Datenverkehrsabkommen“ nicht realistisch scheint, müssen zumindest mit den USA gleiche Wettbewerbsbedingungen vereinbart werden. Falls dies nicht gelingt, muss Europa einen eigenen Weg einschlagen. Daher muss das EU-USA-Rahmenabkommen schleunigst verabschiedet und der Safe Harbor Mechanismus aufgehoben und juristisch auf neue Füße gestellt werden.

Die EU kann zum Vorbild werden und so beweisen, dass es möglich ist, die globalisierte Digitalisierung des Menschen an den Rahmen „analoger“, grundrechtsbezogener Werte anzupassen.

ZUR PERSON

Axel Voss

ist seit 2009 Mitglied des Europäischen Parlaments und dort seit 2014 Mitglied und stellvertretender Vorsitzender des Rechtsausschusses sowie rechtspolitischer Sprecher der CDU/CSU-Gruppe. Zuvor war der Rechtsanwalt Mitglied im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres und hat sich vor allem mit der Migrationspolitik, der Asylproblematik, dem Datenschutz und der grenzüberschreitenden polizeilichen und justiziellen Zusammenarbeit beschäftigt.

„UNGLEICHGEWICHT BEIM DATENSCHUTZ VERZERRT WETTBEWERB“

Die Telekom hält sich an die deutschen Datenschutzgesetze, während für Datensammler aus den USA andere Regeln gelten. Das hält der Vorstandvorsitzende Timotheus Höttges für problematisch. Es brauche dringend einheitliche und länderübergreifende Vorgaben.

Herr Höttges, im Jahr eins nach den Snowden-Enthüllungen und wenige Wochen nach dem 3. Cyber Security Summit: Hat sich die Bedrohungslage geändert?
Timotheus Höttges: Bedrohungslagen ändern sich mit der Weltpolitik. Insofern: ja. Die vielen Konfliktherde in der Welt wirken sich natürlich auch auf die Cybersicherheit aus. Die Konfliktparteien setzen moderne Kommunikationstechnik nicht nur für Propaganda oder die Kommunikation untereinander ein. Sie greifen ihre Gegner zudem über das Netz an. Insofern hat sich die Bedrohungslage durch Cyberangriffe zusätzlich verschärft.

Gibt es Anzeichen für gezielte Terroranschläge auf Computernetze und öffentliche Infrastrukturen?
Timotheus Höttges: Es ist ja leider so, dass wir die Angreifer in den meisten Fällen nicht identifizieren können. Wir sollten aber politisch motivierte Angriffe nicht ausschließen, auch wenn es bisher nur wenige Beispiele dafür gibt. Ein hoch entwickelter Trojaner soll seit Jahren Unternehmen aus Energie, Luftfahrt und Forschung ausgespäht haben. Es gab auch einen Angriff syrischer Hacker auf die Wasserversorgung in Haifa. Und in den Vereinigten Staaten wurden im Jahr 2013 rund 60 Prozent mehr Cyberangriffe auf öffentliche Infrastrukturen registriert als im Jahr davor. Die NSA hat jüngst erklärt, chinesischen Hackern sei es bereits gelungen, in Computersysteme von US-Stromversorgern einzudringen. Damit seien sie in der Lage, solche Systeme lahmzulegen.

Was können wir gegen diese zusätzliche Bedrohung tun?
Timotheus Höttges: Klar ist erst mal, dass jeder von uns Opfer eines Angriffs werden kann. Und sei es indirekt über den Ausfall von Infrastrukturen. Es kann sich niemand mehr darauf zurückziehen, dass es ihn nicht betreffen wird. Wir brauchen deshalb unbedingt eine übergreifende Zusammenarbeit von Staaten, Unternehmen und Organisationen. Nur gemeinsam lässt sich der Bedrohung begegnen. Leider sehe ich aber wenig Bewegung, was länderübergreifende Regelungen angeht.

„Wir müssen alles für den Schutz und die Sicherheit der Daten unserer Kunden tun. Das ist ein wichtiger Teil unserer Geschäftsgrundlage.“

Auch im Nach-Snowden-Jahr scheinen sich Deutschland und die USA in Fragen eines gemeinsamen Datenschutzverständnisses kaum angenähert zu haben.
Timotheus Höttges: Wir müssen die bestehenden Ungleichheiten beim Datenschutz in Europa und den USA abbauen. Das hohe europäische Datenschutzniveau ist ein Segen, aber es sorgt auch für Wettbewerbsverzerrung in der digitalen Wirtschaft: Amerikanische Unternehmen machen fast alles – wir erlauben uns fast nichts. Deswegen brauchen wir dringend die europäische Datenschutz-Grundverordnung. Damit würden

ZUR PERSON

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.

für alle Unternehmen, die ihre Dienstleistungen EU-Bürgern anbieten, die gleichen Vorgaben gelten. Auch wenn die Unternehmen selbst ihren Sitz nicht in Europa haben.

Was würde das den europäischen Unternehmen bringen?
Timotheus Höttges: Das würde für mehr Gleichgewicht sorgen und dafür, dass sich unsere Investitionen in Datenschutz und Datensicherheit auch auszahlen. Die Entscheidung des US-Senats, die von Barack Obama versprochene Geheimdienstreform zu blockieren, ermutigt allerdings nicht gerade. Ich bin mir aber sicher, dass auch die US-amerikanischen Unternehmen über diese Entscheidung nicht sehr erfreut sind. Für sie ist Europa ein wichtiger Markt und die Kunden wollen klare Antworten auf die Datenschutzfragen. Wir merken das insbesondere an unseren Großkunden, die immer mehr nach IT-Dienstleistungen „made in Europe“ fragen.

Aber es landen doch auch massenhaft Daten europäischer Verbraucher bei amerikanischen Unternehmen.
Timotheus Höttges: Umso wichtiger ist es für die Industrie und für die Konsumenten, dass es verlässliche Spielregeln gibt. Wir brauchen einen einheitlichen europäischen Datenschutz, der keine Schlupflöcher lässt. Es darf nicht dazu kommen, dass Daten europäischer Verbraucher außerhalb Europas ganz anders behandelt werden können als hier in Europa.

Das sehen Internetkonzerne aus Übersee sicher anders.
Timotheus Höttges: Daten, die in Europa entstehen, sollten einem einheitlichen europäischen Datenschutzrecht unterliegen. Jeder Anbieter, der sich an diese Regeln hält, hat Zugang – egal ob das Unternehmen aus Amerika, Asien oder Europa kommt. Das ist keine Zersplitterung des Internets, sondern das schafft digitale Rechtssicherheit.

Warum engagiert sich gerade die Telekom so stark für das Thema Datensicherheit?
Timotheus Höttges: Das ist ganz einfach: Wir verarbeiten und speichern zig Millionen Daten unserer Kunden. Unseren Rechenzentren vertrauen viele Unternehmen sogar geschäftskritische Informationen an. Daher müssen wir alles für den Schutz und die Sicherheit der Daten unserer Kunden tun. Wenn unsere Kunden uns nicht mehr vertrauen, dann würde das einen wichtigen Teil unserer Geschäftsgrundlage zerstören.

Wie schützt sich die Telekom selbst?
Timotheus Höttges: Dazu nur ein paar Beispiele. Wir sind dabei, eine Geschäftseinheit Cybersecurity aufzubauen, in der alle sicherheitsrelevanten Bereiche zusammengefasst sind. Diese Einheit ist sowohl für unsere eigene Sicherheit zuständig als auch für die Vermarktung von Sicherheitsprodukten und -dienstleistungen. Wir bilden seit 2014 als erstes Unternehmen in Deutschland Cyber Security Professionals aus, da es zu wenig IT-Sicherheitsexperten gibt. Wir haben ein eigenes Cyber Defense Center in Betrieb genommen, integrieren Sicherheit von Anfang an in unsere Produkte und entwickeln gemeinsam mit Partnern ein umfassendes Lösungskonzept zum Schutz vor Angriffen aus dem Internet.

Cybersicherheit war bisher eher ein Thema für Fachkreise und weniger fürs Management. Hat sich das geändert?
Timotheus Höttges: Der Cyber Security Summit zeigt, dass sich etwas verändert hat. Die Zahl der Teilnehmer aus der Industrie hat von Jahr zu Jahr zugenommen. Aber auch das Interesse an unseren Sicherheitslösungen oder Cloud-Angeboten spiegelt das gestiegene Interesse wider. Das hat auch viel mit dem Thema Datenschutz zu tun. In Deutschland gibt es eine vergleichsweise strenge Gesetzgebung. Die Unternehmen wollen wissen, wo ihre Daten gespeichert werden, und sie wollen die Gewissheit, dass sensible Kunden- und Unternehmensdaten bestmöglich geschützt sind. Sie vertrauen jetzt mehr europäischen Lösungen, weil sie Angst vor Hintertüren haben, über die auf ihre Daten zugegriffen werden kann.

Wie schützt sich ein Vorstandsvorsitzender eines Anbieters von IT- und Telekommunikationslösungen gegen Datenmissbrauch?
Timotheus Höttges: Meine Passwörter habe ich in einem sehr sicheren Programm geschützt. Mails verschicke ich über einen sicheren Telekom Server. Private Bilder stelle ich nicht ins Internet und einen Dienst wie Whats App nutze ich nicht. Bei den Cloud-Diensten vertraue ich nur unseren eigenen Produkten.

„WIR BRAUCHEN UNBEDINGT EINE ÜBERGREIFENDE ZUSAMMENARBEIT VON STAATEN, UNTERNEHMEN UND ORGANISATIONEN.“

SELBSTBESTIMMUNG IN GEFAHR

Was passiert, wenn Staaten und Unternehmen Daten ihrer Bürger und Kunden ungebremst mitlesen, speichern und auswerten? Dann verlieren wir unsere digitale Souveränität und letztendlich unsere Selbstbestimmung, warnt **Dr. Claus-Dieter Ulmer**, Konzernbeauftragter für den Datenschutz der Deutschen Telekom.

Herr Dr. Ulmer, das Bundesverfassungsgericht hat vor drei Jahrzehnten in einem Urteil den Begriff der „informationellen Selbstbestimmung" geprägt. Damals war der Gründer von Facebook noch nicht geboren und Google startete erst 15 Jahre später. Hatten die Verfassungsrichter hellseherische Fähigkeiten?
Dr. Claus-Dieter Ulmer: Das Bundesverfassungsgericht wollte mit dem Begriff der informationellen Selbstbestimmung deutlich machen, dass jeder Bürger das Recht hat, grundsätzlich über die Preisgabe und vor allem die Verwendung seiner Daten selbst zu entscheiden. Damals gab es einen Streit über die Volkszählung, die viele Bürger ablehnten. Wenn wir sehen, wo und in welchem Umfang heute Daten gesammelt und ausgewertet werden, hat diese Entscheidung umso mehr an Bedeutung gewonnen.

Die Bundesverfassungsrichter haben 2008 auch das systematische Abgreifen von Kommunikationsdaten und die Erstellung von Persönlichkeitsprofilen angeprangert. Dies seien schwere Eingriffe in das Grundrecht.
Dr. Claus-Dieter Ulmer: Die beiden Entscheidungen des Bundesverfassungsgerichts bezogen sich zwar auf staatliche Eingriffe, haben aber auch unmittelbar Wirkung für die Wirtschaft. Denn die Gefährdung der informationellen Selbstbestimmung geht heute sehr stark auch von den Unternehmen aus. Die Geschäftsmodelle einiger weltumspannender Internetanbieter basieren darauf, personenbezogene Datensätze in großem Stil zu sammeln, auszuwerten und zu verkaufen.

Wer Google, Facebook oder Smartphone-Apps nutzt, macht das aber freiwillig. Worin liegt also das Problem?
Dr. Claus-Dieter Ulmer: Das Problem ist der totale Kontrollverlust über die eigenen Daten. Jeder weiß inzwischen, dass seine Daten in den sozialen Medien mehr oder weniger öffentlich sind und von den Anbietern in großem Umfang für eigene Zwecke genutzt werden. Was aber genau mit den Daten passiert, welche Daten wie verknüpft und an wen für welchen Zweck verkauft werden, das weiß von den Nutzern niemand. Jedem sollte jedoch bekannt sein, was ein Unternehmen mit seinen Daten macht. Und dann kann er oder sie entscheiden, ob das in Ordnung ist oder nicht. Eine pauschale Zustimmung zu unbekannten Auswertungsaktivitäten ist dagegen gleichzusetzen mit dem Verlust der Selbstbestimmung.

Also wollen Sie soziale Medien oder Apps verbieten?
Dr. Claus-Dieter Ulmer: Nein, es geht nicht um Verbote. Es geht um Aufklärung, Transparenz und einen Ausgleich der Interessen. Es gibt sehr viele Apps, die absolut sinnvoll sind, und Suchmaschinen bringen unbestritten mehr Klarheit in das unendliche Internetangebot. Aber wir wissen nicht, mit welchen Algorithmen beispielsweise Google personenbezogene Daten analysiert. Hier sind vor allem wirtschaftliche Interessen im Spiel. Dabei spreche ich nicht nur von den offensichtlichen Auswertungen, die dem Zweck der gezielten Bewerbung eines Produkts dienen.

Wir wissen auch nicht, ob und an wen die Daten verkauft werden. Vielleicht an Banken, um Hinweise auf die Kreditwürdigkeit zu bekommen, auf die wir keinen Einfluss haben. Oder an Versicherungen, weil sie wissen wollen, ob es Hinweise auf „teure" Erkrankungen gibt. Selbst derjenige also, der vermeintlich „nichts zu verbergen" hat, läuft Gefahr, fremdbestimmt zu werden – ohne dass er es merkt.

Und wie kann mehr Transparenz aussehen?
Dr. Claus-Dieter Ulmer: Indem mir klar und deutlich angezeigt wird, was mit meinen Daten passiert, bevor ich sie eingebe. Datenschutzhinweise dürfen nicht pauschal als Freibrief formuliert sein, sondern müssen konkret angeben, zu welchem Zweck die Daten genutzt werden. Das geht auf Internetseiten ganz einfach mit Pop-ups oder gut erkennbaren Links zu den Datenschutzhinweisen und verständlichen Einwilligungserklärungen. Für die Produkte und Dienstleistungen der Telekom handhaben wir das so. Das hat uns in Bezug auf Datensicherheit und Datenschutz sehr viel Vertrauen bei den Kunden gebracht.

Müssen Daten denn immer personenbezogen ausgewertet werden?
Dr. Claus-Dieter Ulmer: Es lassen sich viele Schlüsse aus anonymisierten Daten ziehen. Und dann halte ich eine Analyse auch für vollkommen legitim. Das hat es schon in der realen Welt immer gegeben. Damals haben Unternehmen versucht, mit Befragungen herauszufinden, wie sich ein Produkt in einem bestimmten Umfeld am besten bewerben lässt. Auch die Auswertung von pseudonymen Daten ist datenschutzfreundlich gestaltbar und sollte verstärkt ermöglicht werden.

Die heute zum Teil praktizierte Profilbildung führt dazu, dass die Angebote immer stärker auf eine Einzelperson und deren vermeintliches Profil zugeschnitten werden. Etwas anderes bekommen wir dann im Zweifel nicht mehr angezeigt. Dies kann zum Verlust der Selbstbestimmung führen. Politisch kann es langfristig sogar den Verlust der Pluralität in der Meinungsbildung bedeuten. Das ist etwas, was niemand von uns wollen kann.

ZUR PERSON

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

NETZZENTRIERTE SICHERHEIT

Wie wird sich der Markt für IT-Sicherheitsprodukte und -Dienstleistungen entwickeln? Im optimistischsten Fall würde sich der Produktionswert laut einer Studie des Bundeswirtschaftsministeriums bis ins Jahr 2020 auf 26,4 Milliarden Euro mehr als verdoppeln. Unabhängig vom Marktvolumen glaubt Telekom IT-Sicherheitschef Thomas Tschersich, dass sich der Markt vor allem qualitativ verändern wird.

Herr Tschersich, IT-Sicherheit steht nicht erst seit Edward Snowden weit oben auf der Agenda von Unternehmen. Durch überdurchschnittliches Wachstum glänzt der Markt trotzdem nicht. Wie ist das zu erklären?
Thomas Tschersich: Nach wie vor sehen viele Unternehmen IT-Sicherheit als reinen Kostenfaktor und nicht als Investition in die Zukunft. Daran ändern auch steigende Zahlen über finanzielle Schäden durch Kriminalität und Spionage im Internet wenig. Erst wenn das Kind in den Brunnen gefallen ist, erkennen viele die Risiken. Dann kann es aber zu spät sein.

Liegt es möglicherweise auch daran, dass Antivirensoftware und Firewalls längst zur Standardausstattung gehören?
Thomas Tschersich: In der Tat ist der Markt inzwischen nahezu abgedeckt – zumindest bei den Unternehmen. Bei den Privatverbrauchern bestehen erstaunlicherweise jedoch immer noch Sicherheitslücken. Firmen müssen sich allerdings die Frage stellen, ob eine auf Software basierende IT-Sicherheit noch ausreicht. Sicher hilft sie gegen massenhaft auftauchende unspezifische Viren und Würmer. Aber gegen Angriffe von professionellen Auftragshackern taugt sie nicht mehr wirklich.

Was hilft denn dann?
Thomas Tschersich: Ganz wichtig wird in Zukunft proaktives Monitoring der Sicherheitslage. Also nicht allein abwarten, ob die Burgmauer hält. Sondern die Burg verlassen, das Umfeld beobachten und schon die Wege zur Burg säubern. Das geht einher mit der technischen Entwicklung von Arbeitsplätzen sowie der zunehmenden Mobilisierung unserer Arbeit und unseres Alltags. Software, Daten und Rechenkapazität werden sich weiter in die Cloud verlagern. Wir haben nur noch schlanke Endgeräte, die nichts anderes als eine Verbindung ins Netz darstellen.

Wie sollen wir uns dann gegen Cyberangriffe und Hacker schützen?
Thomas Tschersich: Das werden künftig verstärkt die Netzprovider übernehmen, zum Beispiel die Telekom. Durch unsere Netze muss alles durch, was Unternehmen und Privatnutzer an Daten austauschen. Über unsere Netze greifen sie auf Internetseiten zu, empfangen E-Mails oder sehen fern. Was liegt also näher, als die Zufahrtswege sauber zu halten? Sicherheit verlagert sich ins Netz. Wir sprechen von netzzentrischer Sicherheit. Wir müssen doch schon heute zu unserem eigenen Schutz die Netze reinigen. Diesen Service werden wir vermehrt auch unseren Kunden anbieten. Das macht Sicherheit für sie einfacher, da sie sich um nichts mehr selbst kümmern müssen. Neben dem Grundschutzniveau können Kunden künftig erweiterte Sicherheitsfunktionen buchen, wie sie heute Bandbreite buchen.

Gibt es dafür bereits Beispiele?
Thomas Tschersich: Wir bieten einen Schutz gegen Distributed-Denial-of-Service-Angriffe an – kurz DDoS. DDoS-Attacken legen Webserver oder ganze Netzwerke durch Überlastung lahm. Wer auf seinen Webshop angewiesen ist oder Kundenservices online anbietet, ist dann nicht mehr erreichbar. Schlimmstenfalls kann das Tage dauern. Damit werden Unternehmen erpressbar. Solche DDoS-Angriffe haben stark zugenommen.

Aber Firewalls fangen solche Angriffe doch ab.
Thomas Tschersich: Sie besitzen eine immense Schlagkraft. In der Spitze bombardieren DDoS-Attacken ihr Ziel mit bis zu 400 Gigabit pro Sekunde. Firewalls schließen dann zwar die Zugänge und die Server gehen nicht in die Knie, aber die Übertragungswege sind trotzdem verstopft und die Services unerreichbar. Damit hat die Firewall vordergründig zwar geholfen, der Onlineshop funktioniert trotzdem nicht mehr.

Wie lautet die Antwort der Telekom?
Thomas Tschersich: Wir können solche DDoS-Angriffe schon in unserem Backbone abfangen, also in unserem Basisglasfasernetz. Wenn wir erkennen, dass es ein Angreifer auf bestimmte IP-Adressen unseres Kunden abgesehen hat, lenken wir das Bombardement um. Wir saugen es förmlich ab, bevor es die Firewall des Kunden erreicht. Das ist nur im Backbone möglich. Solche Sicherheitsservices werden wir künftig auch für andere Angriffstypen anbieten.

Also eine Art Sicherheit as a Service?
Thomas Tschersich: Unsere Kunden bekommen Sicherheit mit ihrem Tarif inklusive. So, wie sie heute mit ihrem MagentaEINS Tarif Festnetz und Mobilfunk aus einer Hand bekommen, ist dann Sicherheit als Flatrate eingeschlossen.

Die Kunden brauchen dann keine Antivirensoftware mehr?
Thomas Tschersich: Nur dann, wenn sie komplett alles über das Netz abwickeln. Wenn sie noch einen PC mit USB-Anschluss und DVD-Laufwerk haben, könnten sie sich darüber infizieren. Das können wir als Provider nicht verhindern. Dafür müssen sie weiterhin eine Securitysoftware nutzen. Aber der Trend ist klar vorgezeichnet. Das sieht man am Beispiel von Smartphones und Tablet-PCs, die kaum noch lokale Schnittstellen haben.

ZUR PERSON

Thomas Tschersich
ist Leiter der Sicherheitsabteilung 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.

ZWISCHEN INTERNETKRIMINALITÄT UND GEOPOLITISCHEN KRISEN

Zum dritten Mal in Folge diskutierten Anfang November 2014 in der Bonner Zentrale der Telekom Vertreter der Bundesregierung, Europäischen Union, NATO, US-Regierung und Topmanager international führender Unternehmen über die digitale Verteidigung in einer zunehmend vernetzten Welt. Auf dem Spitzentreffen – veranstaltet von der Münchner Sicherheitskonferenz und der Telekom – standen Themen rund um den Schutz kritischer Infrastrukturen, das Spannungsfeld zwischen Datenschutz und Datensicherheit sowie Aufklärungsbedarf und Vorbeugung im Mittelpunkt.

Zu den rund 180 Teilnehmern gehörten unter anderem Brigitte Zypries, parlamentarische Staatssekretärin im Bundeswirtschaftsministerium und ehemalige Bundesjustizministerin, zuständig für Digitalpolitik, der beigeordnete NATO-Generalsekretär Sorin Ducaru, verantwortlich für die neuen sicherheitspolitischen Herausforderungen des Verteidigungsbündnisses, der Vorsitzende des Außenausschusses im Europäischen Parlament Elmar Brok, der Cyberbeauftragte des amerikanischen Außenministeriums Christopher Painter sowie der amerikanische Anwalt und Datenschutzexperte Ben Wizner, der Edward Snowden juristisch vertritt.

„Wir müssen leider ganz lapidar feststellen, dass der Krieg als Element der Politik nach Europa zurückgekehrt ist. Das hat weitreichende Auswirkungen auf die Cybersicherheit. Moderne Internetkommunikationstechnik wird genutzt, um den Gegner zu verwirren und Propaganda zu betreiben."
Wolfgang Ischinger
Vorsitzender der Münchner Sicherheitskonferenz

„Unser Ziel, Deutschland bei der Digitalisierung zu einem führenden Land in Europa zu machen, kann nicht ohne das wichtige Thema IT-Sicherheit erreicht werden."
Brigitte Zypries
Parlamentarische Staatssekretärin im Bundeswirtschaftsministerium

„Staaten und Unternehmen sind zunehmend abhängiger von IT und werden dadurch immer angreifbarer und manipulierbarer – bis hin zur Stilllegung von Infrastruktur."
Elmar Brok
Vorsitzender des Außenausschusses im Europäischen Parlament

„Wir sehen beim derzeitigen politischen Umgang mit dem Thema Cyber Warfare einen bemerkenswerten Zuständigkeitswirrwarr – auf nationaler, europäischer sowie multinationaler Ebene."
Karl-Theodor zu Guttenberg
Chairman Spitzberg Partners LLC

„Die Staaten sind bei der Bedrohung durch Nuklearwaffen zusammengerückt und haben sich darauf geeinigt, bestimmte Handlungen zu unterlassen und zu sanktionieren. Eine ähnliche Vorgehensweise ist auch für den Cyber Warfare denkbar."
Christopher Painter
Cyberbeauftragter des amerikanischen Außenministeriums

„Es ist nicht zielführend, eine Sicherheitsstrategie zu nutzen, die sich allein darauf konzentriert, möglichst viele Daten anzuhäufen, um daraus dann die heiße Spur zu generieren."
Clemens Binninger
Vorsitzender des Parlamentarischen Kontrollgremiums

„Ich mache mir mehr Sorgen um jene Daten, die Bürger ganz freiwillig im Internet preisgeben. Sie sehen nicht die Gefahren, was mit diesen Daten passiert. Dies ist allerdings kein datenschutzrechtliches Problem, da die Bürger selbst der Verarbeitung ihrer Daten zustimmen."
Klaus-Dieter Fritsche
Staatssekretär und Geheimdienstkoordinator im Bundeskanzleramt

„Es wird nicht leichter, eine Nadel im Heuhaufen zu finden, wenn du den weltweit größten Heuhaufen aufbaust", bezweifelt Snowden-Anwalt **Ben Wizner** die Effektivität eines massenhaften Anhäufens von Daten.

„Ich weiß, dass Sie befürchten, dass wir auf Ihre Kommunikation zugreifen und Ihre Daten entwenden. Wenn diese Angst tatsächlich bestätigt wird, fällt die digitale Wirtschaft wie ein Kartenhaus in sich zusammen."
Ciaran Martin
Leiter Government & Industry Cyber Security beim britischen Geheimdienst GCHQ

„Auf beiden Seiten der Welt wird es tatsächlich so gesehen, dass wir uns bereits in einem Cyberwar befinden und dass wirtschaftliche Kriegsführung erlaubt und notwendig ist, um das Wohlergehen einer Nation voranzubringen."
Elmar Theveßen
Stellvertretender Chefredakteur des ZDF

SICHERHEIT UND MEDIENKOMPETENZ

Im November 2014 fand in der Bonner Telekom Zentrale der erste Sicherheitsgipfel für Kinder und Jugendliche statt. Er ist Teil einer Reihe von Projekten und Initiativen, mit der die Telekom jungen Menschen die Chancen der digitalen Welt aufzeigen und diese zum verantwortungsbewussten Umgang mit digitalen Medien ermutigen will.

Ungewohnte Geräuschkulisse in der Zentrale der Telekom. Einen Tag nachdem an gleicher Stelle 180 Vertreter von Bundesregierung, EU, NATO, US-Regierung und Topmanager internationaler Unternehmen über digitale Verteidigung in einer zunehmend vernetzten Welt diskutiert hatten, lud die Telekom am 4. November 200 Kinder zum ersten Cyber Security Summit for Kids ein. Mittendrin der gesamte Vorstand der Deutschen Telekom AG, der sich den kompetenten Fragen der Kinder stellte.

„Der viel beschworene Digital Native muss jetzt auch mündig werden im Umgang mit den Risiken der digitalen Welt und von Anfang an eine verantwortungsvolle Nutzung mitlernen. So gestalten wir eine zukunftsfähige, sichere digitale Gesellschaft", erklärte Timotheus Höttges, Vorstandsvorsitzender der Deutschen Telekom. Dass Kinder zumindest verantwortungsvoll mit ihren Smartphones umgehen können, erlebte der Telekom Chef selbst, als er einen Schüler aufs Glatteis locken wollte. „Kannst du mir gerade mal dein Passwort für dein Smartphone verraten?", so Höttges. Keine Chance. Selbstbewusst lehnte der Schüler mit der Feststellung ab: „Nee, das mache ich nicht. Das ist geheim und geht niemanden etwas an."

Beim ersten Cyber Security Summit for Kids wurden auch die Gewinner des bundesweiten Wettbewerbs „Medien, aber sicher!" ausgezeichnet. Die Telekom hatte in Kooperation mit der Frankfurter Allgemeinen Zeitung die besten Projekte und Initiativen gesucht, die junge Menschen im Bewusstsein für Möglichkeiten und Risiken digitaler Medien stärken. Besonders überzeugt hat die Jury dabei das Projekt „Jetzt – im Netz" der Uhlandschule, einer Grundschule im baden-württembergischen Wurmlingen. Die Viertklässler betätigten sich als kleine Forscher, sammelten Informationen zum Thema Internet und erarbeiteten einen eigenen Bewertungsbogen für Kinderseiten im Internet.

TEACHTODAY

Teachtoday ist eine Initiative der Telekom zur Förderung der Medienbildung. Sie zeigt Wege des kompetenzorientierten Lernens mit digitalen Medien auf und bietet Tipps sowie Materialien zum verantwortungsvollen und sicheren Umgang mit neuen Informations- und Kommunikationstechnologien. Teachtoday rückt das kompetenzorientierte Lernen mit digitalen Medien in den Mittelpunkt und unterstützt Lehrkräfte, Schulleitungen und Schulsozialarbeiter, aber auch Eltern sowie Schülerinnen und Schüler.

teachtoday
Lernen neu denken

Mobile Geräte im Klassenzimmer, Datenschutzfragen und Urheberrechte: Was sind die Herausforderungen unserer digitalisierten Welt? Und wie können Lernende und Lehrende die zunehmende Digitalisierung am besten für die eigenen Ziele nutzen? Unter dem Motto „Lernen neu denken" unterstützt die Initiative Interessierte, Potenziale der Digitalisierung zu nutzen und Herausforderungen kompetent zu begegnen.

Hierfür bietet die Initiative auf der Website **www.teachtoday.de** auch zu den Themen Datenschutz und -sicherheit Materialien und unterrichtspraktische Formate, die entlang aktueller mediendidaktischer Entwicklungen die Zukunft des Lernens schon heute erfahrbar machen. Die Dokumente zu den Themen Datenschutz und -sicherheit eignen sich für den Einsatz im Unterricht, an Elternabenden oder zum Austausch im Kollegium.

MEDIEN, ABER SICHER!

Auf dem Cyber Security Summit for Kids erprobten sich 200 Kinder zwischen neun und zwölf Jahren erstmals an einem neuen Parcours, der spielerisch Medienkompetenz und Wissen zu digitalen Medien vermittelt. An fünf verschiedenen Stationen wurden in aktionsreichen Übungen und Aufgaben verschiedene Bereiche der Mediennutzung aufgegriffen und Themen wie Spielzeiten, Datenschutz und Cybermobbing behandelt. Ab Frühjahr 2015 können Schulen den kompletten Parcours, der sich an ein „Jump-and-run"-Computerspiel anlehnt, kostenlos bei der Telekom ausleihen.

EIN NETZ FÜR KINDER

Die Telekom unterstützt zudem die Initiative „Ein Netz für Kinder", mit der die Bundesregierung hochwertige Onlineinhalte für Kinder fördert, die dazu anregen, sich mit dem jeweiligen Thema auch im Alltag zu beschäftigen. „Ein Netz für Kinder" bietet dazu kindgerechte und sichere Websites und hilft Jungen und Mädchen in moderierten Foren dabei, die verschiedenen Nutzungsmöglichkeiten sozialer Netzwerke in einem sicheren Umfeld auszuprobieren.

ein netz für kinder

Im Rahmen von „Ein Netz für Kinder" haben Unternehmen und Verbände mit **www.fragFINN.de** einen sicheren Surfraum für Kinder zwischen 6 und 12 Jahren geschaffen. Die Kindersuchmaschine bietet Kindern eine sichere Startrampe ins Internet. Eine Whitelist mit Internetangeboten führt Kinder zu unbedenklichen, interessanten und vielfältigen Webinhalten. Die Grundlage für die Auswahl der Websites bildet ein von Experten entwickelter Kriterienkatalog. „Mit den üblichen Browsern haben Kinder es schwer, für sie geeignete Websites zu finden. Zudem besteht die Gefahr, dass sie ungewollt und schnell auf ungeeigneten Webinhalten landen", erklärt Fritz-Uwe Hofmann, der die Telekom in der Initiative vertritt. „Für die Telekom ist ‚Ein Netz für Kinder' ein Baustein des umfassenden Engagements für Datenschutz und Datensicherheit."

„WIR MÜSSEN DIE WETTBEWERBS-VERZERRUNG BESEITIGEN“

Jan Philipp Albrecht, Abgeordneter im Europäischen Parlament, glaubt, dass 2015 die EU-Datenschutz-Grundverordnung verabschiedet wird. Damit werde endlich verhindert, dass Unternehmen sich durch Umgehung von Datenschutzregeln einen Wettbewerbsvorteil verschaffen.

Herr Albrecht, wo stehen die Verhandlungen zur EU-Datenschutz-Grundverordnung?
Jan Philipp Albrecht: Trotz einer fast dreijährigen Debatte zum Kommissionsentwurf und einer umfassenden Position des Europäischen Parlaments scheint es im Ministerrat noch immer erheblichen Klärungsbedarf zu geben. Jedenfalls hat er bis Ende 2014 noch keinen kompletten Text vorgelegt. Vor Juni 2015 wird es keine umfassende Position des Rates geben. Sollte es der Ministerrat dann nicht schaffen, sich für die Verhandlungen mit dem Europäischen Parlament bereit zu erklären, wird die Verabschiedung der Verordnung im Jahr 2015 nur noch sehr schwer zu erreichen sein. Das wäre ein Schaden für uns alle: für die Verbraucher und für die Unternehmen im europäischen Markt.

Besteht bei so viel Diskussion nicht die Gefahr, dass es am Ende ein Kompromiss auf kleinstem Nenner sein wird?
Jan Philipp Albrecht: Das Europäische Parlament hat einen Kompromiss gefunden, der alles andere als der kleinste gemeinsame Nenner ist. Da werden die individuellen Datenschutzrechte und Pflichten für die Datenverarbeiter auf höchstem Niveau geregelt – zum Teil sogar höher als das deutsche Datenschutzniveau. Das Ganze ist versehen mit sehr klaren Prinzipien und klaren Verfahren für die Datenschutzbehörden, sodass ein hohes Maß an Rechtssicherheit geboten wird. Dieses Recht lässt sich auch mit starken Sanktionen durchsetzen, die sich an den Sanktionen des Wettbewerbsrechts der Europäischen Union orientieren.

Warum tun sich manche Länder so schwer damit, einen gemeinsamen europäischen Datenschutz voranzutreiben?
Jan Philipp Albrecht: Es sperren sich diejenigen Länder, die den Druck von bestimmten Unternehmen auf dem Markt verspüren. Unternehmen, die ihren Sitz explizit in die Länder gelegt haben, deren Datenschutzprinzipien ein etwas niedrigeres Niveau haben und deren Datenschutzbehörden schlechter ausgestattet sind, haben im Moment einen Wettbewerbsvorteil. Und diese Wettbewerbsverzerrung will die große Mehrheit der EU-Länder beseitigen. Deswegen ist diese Datenschutzverordnung der Europäischen Union der wohl wichtigste und auch größte, langfristig gedachte Beitrag zur Schaffung eines Fundaments, das global wirken kann und auch zum Umdenken der großen Global Player führen könnte.

Besteht nicht die Gefahr, dass sich internationale Unternehmen den europäischen Datenschutzbestimmungen entziehen werden?
Jan Philipp Albrecht: Wir wollen innerhalb des europäischen Markts Gleichheit schaffen. Jedes Unternehmen, das im europäischen Markt seinen Sitz hat, muss sich dann an die gleichen Regeln halten. Dies gilt auch für die Unternehmen, die selbst keinen Sitz in der Europäischen Union haben. Sitzt ein Unternehmen beispielsweise in Indien und bietet Produkte oder Dienstleistungen für Europäer, zum Beispiel Cloud-Services, dann muss es auch die europäischen Datenschutzregeln beachten. Ansonsten drohen empfindliche Marktstrafen, die beim Wettbewerbsrecht schon heute funktionieren.

EU-Parlament, -Kommission und -Ministerrat ringen um die EU-Datenschutz-Grundverordnung. 2015 soll der einheitliche Datenschutzstandard für die Europäische Union verabschiedet werden.

Oder diese Unternehmen ziehen sich aus Europa zurück.
Jan Philipp Albrecht: Die Europäische Union ist der größte Binnenmarkt der Welt. Große Internet- und IT-Anbieter werden sich in Zukunft nicht von diesem Markt fernhalten können, sondern sie werden sich überlegen, ob sie nicht einfach gleich den europäischen Standard als den höchsten bei sich implementieren. Dies könnte dann die Standards in anderen Ländern nach oben ziehen und letztendlich dafür sorgen, dass ein weltweiter Standard gesetzt wird.

ZUR PERSON

Jan Philipp Albrecht,
Jahrgang 1982, hat Rechtswissenschaften studiert. Der Wolfenbütteler ist seit 1999 Mitglied bei den Grünen. Seit 2009 ist er der jüngste deutsche Abgeordnete im Europäischen Parlament. Er ist stellvertretender Vorsitzender des Innenausschusses und stellvertretendes Mitglied im Ausschuss für Binnenmarkt und Verbraucherschutz. Während seiner ersten Legislaturperiode von 2009 bis 2014 war er Mitglied im Innenausschuss und stellvertretendes Mitglied im Rechtsausschuss. Von Dezember 2012 bis Oktober 2013 war Jan Philipp Albrecht auch Koordinator für den Sonderausschuss gegen organisiertes Verbrechen, Korruption und Geldwäsche.

Sie haben gesagt, Sie seien froh, dass auch die Bundesregierung endlich konstruktiv an den Verhandlungen um das Thema teilnimmt. Was meinten Sie damit?
Jan Philipp Albrecht: Die Bundesregierung hat fast zwei Jahre gebraucht, um sich tatsächlich dazu durchzuringen, die Datenschutzverordnung anzuerkennen, wie sie die Kommission vorgeschlagen hat. Zuvor hatte die Bundesregierung dafür geworben, dass sich die Wirtschaft stärker mit Selbstverpflichtungen und Modellen der freiwilligen Datenschutzmaßnahmen beschäftigt. Dies hat dem Vorschlag und auch dem breiten Willen der Parlamentarier im Europäischen Parlament diametral widersprochen. Es ist der Eindruck entstanden, dass man versucht hat, das Ganze in die Länge zu ziehen. Das hat Misstrauen geschürt und dem Prozess geschadet.

Sie sagen, dass die EU-Datenschutz-Grundverordnung im Vergleich zur deutschen Datenschutzgesetzgebung noch mal strenger ist?
Jan Philipp Albrecht: In manchen Teilen geht die Verordnung im Sinne der Verbraucher und durchaus im Sinne der besseren Klarheit für Unternehmen sowie der größeren Rechtssicherheit darüber hinaus. Gerade in Bezug auf den Umgang mit der Einwilligung der Verbraucher bei der Datenverarbeitung hat das deutsche Datenschutzniveau in den vergangenen Jahren durchaus gelitten. Im Sinne der Direktmarketing-interessen hat man sehr weite Ausnahmen bei der Zustimmung der Betroffenen geschaffen und ein sehr schwammiges, zum Teil in der Praxis auch sehr verstecktes Umgehen der Datenschutzbestimmungen ermöglicht.

Jetzt neigen wir Deutschen dazu, die Amerikaner für ihren Umgang mit Daten zu verurteilen. Sind die Europäer nur Engel?
Jan Philipp Albrecht: Nein, dem ist nicht so. Das Ausmaß, personenbezogene Daten zu sammeln und zu verwerten, hat auch in Europa enorm zugenommen. Auch europäische Unternehmen haben im Goldrausch übersehen, dass es ein paar Grundregeln gibt sowie Werte, die sie nicht einfach missachten sollten. Es gibt auch in den USA viele Unternehmen, die sehr viel Wert darauf legen, die Gesetzgebung zum Datenschutz und zur Privatsphäre zu beachten.

Was hilft es uns, wenn wir uns in der EU einig werden, aber das gleiche Problem weiterhin mit Ländern wie USA oder China besteht?
Jan Philipp Albrecht: Wir werden einen transatlantischen oder gar globalen Standard nur dann erreichen, wenn wir vorher unsere eigenen Hausaufgaben machen. Erst wenn wir in Europa für ein einheitliches, klar verständliches Datenschutzgesetz gesorgt haben, können wir über einen transatlantischen Datenschutz verhandeln.

Spüren Sie inzwischen in Gesprächen mit Vertretern von Google und Facebook ein gewisses Einsehen, dass man mit Daten anders umgehen sollte?
Jan Philipp Albrecht: Absolut! Ich bin in den letzten fünf Jahren regelmäßig nach Washington und ins Silicon Valley geflogen. Dort habe ich mich mit den Unternehmen, aber auch mit den Vertretern im Kongress intensiv ausgetauscht. Mein Eindruck: Am Anfang war es noch ganz schwierig, die Brücke über den Atlantik zu schlagen, wenn es um den Umgang mit personenbezogenen Daten und um Privatsphäre ging. Mittlerweile gibt es ein großes Verständnis für die Herangehensweise der Europäer an dieses Thema. Es findet ein großes Umdenken bei den Unternehmen statt, weil sie erkennen, dass das für sie ein bestimmender wirtschaftlicher Faktor wird, wie sie mit Datenschutz und Datensicherheit umgehen.

Jan Philipp Albrecht setzt sich seit Jahren für ein einheitliches EU-weites Datenschutzrecht ein

Hand aufs Herz: Werden wir Ende 2015 die Verordnung haben?
Jan Philipp Albrecht: Ich bin Optimist und sage deswegen: Wir werden diese Verordnung auf jeden Fall in diesem Jahr bekommen. Dann gilt zwei Jahre später der einheitliche Datenschutzstandard in Europa. Damit wir auch wirklich diese Verordnung hinbekommen, muss es eine Einigung der Minister bis zum Frühjahr geben. Eine entsprechende Einigung wird es nur geben, wenn gerade die Unternehmen den Druck auf die Bundesregierung und auf die anderen Regierungen im Ministerrat noch mal erhöhen.

Sie sind Mitglied des Datenschutzbeirats der Telekom. Halten Sie die Arbeit des Beirats für sinnvoll?
Jan Philipp Albrecht: Die Telekom hat deutlich versichert, dass der Datenschutzbeirat völlig unabhängig und keine PR-Aktion darstellt, sondern wirklich ein effektives Gremium zur Schaffung einer besseren Datenschutzpraxis. Das halte ich für einen mutigen, absolut richtigen und notwendigen Schritt. Er ist für alle Unternehmen in dieser Größe und mit dieser Rolle in Europa ein absolutes Vorbild. Ich kann nur hoffen, dass er sehr viele Nachahmer findet. Für die Telekom bedeutet dieser Beirat einen Riesengewinn. Sie kann einen Goldstandard für Datenschutz und Verbraucherstandards im Netz setzen.

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 zumUmgang 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 2014 kam der Datenschutzbeirat zu vier Sitzungen zusammen. Im Fokus standen dabei Themen wie die Bewertung von Datenschutz- und Sicherheitsaspekten von mobilen Bezahldiensten, Anonymisierungsverfahren für Big-Data- Lösungen, die Qivicon-Smart-Home-Plattform oder die Zusammenarbeit mit Mozilla für die Einführung datenschutzfreundlicher Smartphones.

DIE AKTUELLEN MITGLIEDER DES DATENSCHUTZBEIRATS:

Jan Philipp Albrecht
Abgeordneter des Europäischen Parlaments, Mitglied im Innenausschuss und stellvertretendes Mitglied im Ausschuss für Binnenmarkt und Verbraucherschutz, Verhandlungsführer des Europäischen Parlaments für die geplante Datenschutz-Grundverordnung

Wolfgang Bosbach
CDU, MdB, Vorsitzender des Innenausschusses des Deutschen Bundestags

Peter Franck
Mitglied des 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)

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

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

MANDAT VERLÄNGERT: DATENSCHUTZBEIRAT SETZT ARBEIT FORT

Die externen Sachverständigen setzen ihre Arbeit fort: Der Telekom Vorstand hat das Mandat des Gremiums um zwei weitere Jahre verlängert.148 Empfehlungen in 28 Sitzungen – die Bilanz des Datenschutzbeirats nach rund sechs Jahren Arbeit bei der Telekom kann sich sehen lassen. Die Experten schauen sich beispielsweise neue Geschäftsfelder an und untersuchen, wie Daten bei der Telekom gespeichert und verarbeitet werden. „Wir steigen tief in Geschäftsmodelle, Produkte und Prozesse der Telekom ein, um das Unternehmen beim Thema Datenschutz zu beraten“, betont Lothar Schröder, Vorsitzender des Gremiums und stellvertretender Aufsichtsratsvorsitzender der Telekom. Der Telekom Vorstand hat Ende 2014 das Mandat des Gremiums um weitere zwei Jahre verlängert. „In Zeiten, in denen durch die Vernetzung von Maschinen und Produktionsabläufen sowie die Auswertung von Massendaten neue Geschäftsmodelle entstehen, wollen wir nicht auf die Beratung durch externe Experten verzichten“, erläutert Dr. Thomas Kremer, Vorstand Datenschutz, Recht und Compliance bei der Telekom, die Entscheidung. Das zwölfköpfige Gremium wird zudem durch den ehemaligen Datenschutzbeauftragten des Bundes, Peter Schaar, hochkarätig ergänzt. Lothar Schröder: „Die Telekom ist inzwischen das Unternehmen der Branche, dem die Kunden am meisten vertrauen. Wir wollen unseren Beitrag dazu leisten, dass dieser Vorsprung weiter ausgebaut wird.

VORSPRUNG DURCH VERTRAUEN

Vertrauen ist im digitalen Zeitalter mehr denn je eine wichtige Währung für den dauerhaften Erfolg eines Unternehmens. Genauso wichtig wie das Vertrauen von Kunden und Partnern ist das Vertrauen der Mitarbeiter in ihren Arbeitgeber, sagt Lothar Schröder, stellvertretender Aufsichtsratsvorsitzender der Deutschen Telekom.

„Welche Unternehmen halten Sie für vertrauenswürdig, wenn es um den Umgang mit persönlichen Daten geht?“ Diese Frage hatte das Institut für Demoskopie Allensbach Mitte 2014 einer repräsentativen Stichprobe der Bevölkerung in Deutschland gestellt. Das Ergebnis hat mich, der sich seit vielen Jahren für den Datenschutz im Telekom Konzern einsetzt, nicht überrascht. Unter den am meisten bekannten Unternehmen der Telekommunikations- und Internetbranche führt die Telekom mit deutlichem Abstand die Tabelle der vertrauenswürdigen Unternehmen an. Sie konnte den Vorsprung gegenüber dem Zweitplatzierten im Vergleich zum Vorjahr noch mal deutlich steigern.

Der Datenschutzbeirat der Telekom setzt sich genauso wie das Management des Konzerns seit Jahren aus tiefer Überzeugung für den Schutz der Kunden- und Mitarbeiterdaten ein. Nach dem durch die Snowden-Enthüllungen ausgelösten Entsetzen über das staatliche Abgreifen von Kommunikationsdaten jeglicher Art bis hin zum Abhören der Handyverbindungen von politischen Verbündeten haben der Datenschutzbeirat und der Vorstand ihren Einsatz für noch mehr Datenschutz und Datensicherheit weiter verstärkt. Dieses Engagement schlägt sich im positiven Ergebnis der Vertrauensfrage des Allensbach-Instituts nieder.

NICHT NACHLASSEN

Bei aller Freude über das Resultat dürfen wir uns aber nicht auf diesen Lorbeeren ausruhen. Zwar hält fast die Hälfte der Bevölkerung die Telekom für vertrauenswürdig, doch genauso viele haben keine Meinung zur Vertrauenswürdigkeit des Unternehmens. Das müssen wir ändern und daher weiter deutliche Signale aussenden: Die Telekom setzt sich mit allem Nachdruck für den Datenschutz ein.

Auch wenn das deutsche Datenschutzrecht weltweit zu den strengsten gehört, kämpfen wir in zwei Bereichen seit Jahren vergeblich um Verbesserung. In einer globalisierten digitalen Welt endet der Datenschutz nicht an der Landesgrenze. Daher brauchen wir dringend die seit Jahren immer wieder neu diskutierte EU-Datenschutzverordnung. Wir brauchen sie, um wenigstens in der Europäischen Union gleiches Recht – und gleiche Pflichten – für alle zu schaffen. Wir brauchen sie aber auch, um in einer zunehmend von digitalen Geschäftskonzepten geprägten Wirtschaft faire Wettbewerbsbedingungen zu erzielen.

BESCHÄFTIGTENDATENSCHUTZ

Zudem brauchen wir in Deutschland ein eigenständiges Beschäftigtendatenschutzgesetz. Viele allgemeine Bedingungen des Datenschutzes sind nicht auf den Beschäftigtendatenschutz anwendbar. Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen. In einigen Bereichen fehlen klare oder ausreichende rechtliche Vorgaben: beispielsweise bei der Videoüberwachung, bei der Haftung, dem Einsatz biometrischer Verfahren oder der Verarbeitung von Bewerberdaten und dem Rückgriff auf soziale Netzwerke. Es fehlen ausreichende Mitbestimmungsrechte, bessere Rechte der Datenschutzbeauftragten und ein Verbandsklagerecht.

DATENSCHUTZ FÜR ARBEITNEHMER

Unternehmen muss klar sein, wo aus datenschutzrechtlicher Sicht die Grenzen liegen. Weil bisher viele der Fragen nicht im Gesetz geregelt sind, sondern Gerichte von Fall zu Fall entscheiden, bedarf es einer eindeutigen gesetzlichen Regelung.

Für die Arbeitnehmer ist es bitter, dass es nach wie vor kein Gesetz zur Regelung des Beschäftigtendatenschutzes gibt. Umso wichtiger ist es, dass Unternehmen mit ihren Mitarbeitern wenigstens eine interne Beschäftigtendatenschutzregelung vereinbaren. Hier bedaure ich sehr, dass das Management der Telekom 2014 keine Regelung angeboten hat, welche die Zustimmung der Mitbestimmungsgremien finden konnte. Eine von Arbeitgeber- und Arbeitnehmerseite fair ausgearbeitete Vereinbarung wäre ein weiterer Baustein der Telekom auf dem Weg zu einem Unternehmen, das sich ohne Wenn und Aber zu einem hohen Datenschutz bekennt. Ich bin mir sicher, dann würde die Vertrauenskurve bei der Bevölkerung, den Partnern und bei den Arbeitnehmern ein weiteres Stück nach oben gehen.

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)“.

GEMEINSAM VERANTWORTUNG ÜBERNEHMEN

Verantwortung, Selbstbestimmung und Unabhängigkeit sind nicht nur in der analogen Welt sondern auch im digitalen Raum Ausdruck von Freiheit. Wenn Deutschland und Europa digital souverän sein wollen, müssen auch die gesetzlichen Rahmenbedingungen für Datenschutz und Datensicherheit dies widerspiegeln.

Vertrauen ist die Basis unseres Geschäfts. Und das müssen wir uns jeden Tag aufs Neue verdienen, auch wenn wir wissen, dass die Menschen der Telekom in puncto Datenschutz und Datensicherheit mehr vertrauen, als jedem anderen Anbieter im Internet. Digitale Dienste bleiben ungenutzt, wenn Nutzerinnen und Nutzer befürchten, dass ihre persönlichen Daten nicht ausreichend geschützt sind. Das Grundvertrauen in einen sicheren Cyberraum wurde im vergangenen Jahr wiederholt auf eine harte Probe gestellt. Fehlendes Vertrauen führt zu weniger Umsatz und Wachstum – gerade auch bei neuen Anwendungen wie Cloud-Diensten.

Wenn die ITK-Branche Vertrauen etablieren will, muss sie gemeinsam Verantwortung für mehr Sicherheit übernehmen. Dafür müssen alle Marktteilnehmer an einem Strang ziehen und gleiche Mindeststandards einhalten. Das gilt für uns als Netzbetreiber ebenso wie für alle anderen Anbieter von Produkten und Diensten im Cyberraum. Leider hat dieser Punkt in den Diskussionen über ein IT-Sicherheitsgesetz in Deutschland und eine Netz- und Informationssicherheitsrichtlinie auf europäischer Ebene bislang wenig Beachtung gefunden. Bislang wurden nur die Netzbetreiber verpflichtet. Für ein hohes Schutzniveau im Cyberraum müssen aber alle Akteure verpflichtet werden, an der Beseitigung von Schadensvorfällen mitzuwirken. Dies gilt insbesondere für Hardware- und Softwarehersteller sowie Internetdienste. Diese Akteure sind bisher ohne überzeugende sachliche Rechtfertigung nicht in der gebotenen Klarheit vom Anwendungsbereich der geplanten gesetzlichen Regelungen erfasst.

EUROPÄISCHE REGELN FESTLEGEN

Damit bleibt ein großer Teil des Internetverkehrs ungeschützt. Denn die meisten Daten verarbeiten die Anbieter der Dienste, wie zum Beispiel Cloud-Dienste, E-Mail-Dienste oder soziale Netzwerke. Wäre es da nicht sachgerecht, eben diese auch zur Einhaltung von Mindeststandards für mehr Cybersicherheit direkt zu verpflichten? Gleiches gilt für die Anbieter und Lieferanten von Hard- und Software. Angriffe erfolgen sehr oft mittels manipulierter Hard- und/oder Software. Was läge da näher, als diese Anbieter zu verpflichten, für Sicherheits-Updates etwaiger Schwachstellen zu sorgen und damit einen ureigenen Beitrag zur Beseitigung von Sicherheitslücken zu leisten. Nur, wenn wir gemeinsam als ITK-Branche Verantwortung übernehmen, lässt sich das Ziel größerer Sicherheit im Cyberraum erreichen. Ausnahmen für Diensteanbieter oder Hard- und Softwarehersteller sind deshalb nicht sinnvoll.

Das Internet ist global, gleichzeitig sind aber die Spielregeln immer noch den unterschiedlichen Rechtssystemen und ihren jeweiligen nationalen Ausprägungen unterworfen. Augenfällig wurde dies in den vergangenen Monaten im Bereich

> „WIR MÜSSEN DIE MENSCHEN BEFÄHIGEN, DIGITAL SOUVERÄN ZU AGIEREN.“

Datenschutz und Datensicherheit, wo gerade im transatlantischen Verhältnis unterschiedliche Auffassungen zur Balance aus Freiheit und Sicherheit offenbar wurden.

Europa muss hier einen eigenen Weg finden. Denn auf eine globale Einigung bei allen relevanten Rechtsfragen zu warten, ist ein frommer, aber realitätsferner Wunsch. Selbst da, wo es multilaterale Vereinbarungen gibt, wie zum Beispiel bei der Rechtshilfe, wurden diese missachtet. Für die europäische Wertegemeinschaft – und dies betrifft Gesellschaft und Wirtschaft gleichermaßen – ist es zielführender, zunächst für den eigenen Rechtsraum die Spielregeln zu definieren, an die sich alle Akteure, egal woher sie auf der Welt kommen, zu halten haben. Es gilt das Marktortprinzip.

Das hat nichts mit Abschottung, Ausgrenzung oder Wirtschaftsprotektionismus zu tun. Es ist Ausdruck der Souveränität, sich auch für die digitale Welt einen Rahmen zu geben, der klar definiert, zu welchen Werten wir im europäischen Cyberraum stehen und was wir als damit unvereinbar ablehnen. Gleichzeitig schaffen wir damit nationale Sonderregeln ab. Die geplante europäische Datenschutz-Grundverordnung ist da ein wichtiger Schritt. Denn mit ihr sollen gleiche Regeln für alle digitalen Dienste in der EU gelten, auch wenn sie von Anbietern aus Übersee für europäische Bürger erbracht werden.

MEHR UNABHÄNGIGKEIT IN EUROPA

Europa muss seine digitale Souveränität zurückgewinnen. Zur digitalen Souveränität gehören nicht nur einheitliche europäische Regelungen, hierzu gehört vor allem die industrielle Kompetenz, sicherheitsrelevante Soft- und Hardware selbst zu entwickeln und wo nötig auch in Europa zu produzieren. Dazu zählen der Ausbau sicherer und innovativer IT-Systeme sowie die Bereitstellung sicherer digitaler Transportwege als Garant für die künftige digitale Entwicklung unserer Gesellschaft. Dazu gehört aber ebenso die Förderung von Forschung und Entwicklung innovativer, vertrauenswürdiger High-Tech-Lösungen in Schlüsselbereichen, wie zum Beispiel Netzwerkkomponenten.

Dabei müssen zunächst die sicherheits- und industriepolitisch wichtigen Bereiche identifiziert werden. In diesem Zusammenhang ist nicht nur die technologische Kompetenz entscheidend, sondern auch die Fähigkeit des Einzelnen, diese Kompetenz auch anwenden zu können. Wir müssen die Menschen befähigen, digital souverän zu agieren, d.h., mit digitalen Medien nicht nur umzugehen, sondern sich auch mit ihren relevanten Sicherheitsaspekten und möglichen Risiken auseinanderzusetzen.

Die digitale Souveränität Europas erfordert massive Anstrengungen und erhebliche Investitionen in Forschung und Entwicklung von sicheren IT-Lösungen, aber auch in die Aus- und Weiterbildung. Die europäische Industrie tut hier schon viel. Hierzu bedarf es auch erheblicher Anstrengungen des Staates. Gerade die Erfahrung in anderen erfolgreicheren Wirtschaftsregionen der Welt zeigt, dass es ohne staatliche Leuchtturm-Projekte kaum geht.

ZUR PERSON

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

GRENZEN ÜBERWINDEN UND KOOPERIEREN

Cyberkriminalität ist zum Kriminalitätsfeld mit den höchsten Zuwachsraten geworden. Die Aufklärungsquoten sind demgegenüber noch gering. Eine erfolgreiche strafrechtliche Verfolgung von Cyberstraftaten erfordert den verstärkten Aufbau von spezialisierten Einheiten bei den Strafverfolgungsbehörden und eine enge Kooperation zwischen Strafverfolgungsbehörden und Privatwirtschaft.

Cyberkriminalität, im weiteren Sinne verstanden als Gesamtheit aller Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden, war bis vor wenigen Jahren noch eher ein Randphänomen in den Kriminalitätsstatistiken. Dies hat sich grundlegend geändert. Kein anderes Kriminalitätsfeld wächst so rasant wie Cyberkriminalität. Die aktuellen Kriminalitätsstatistiken weisen bei Cyberstraftaten mit ihren vielfältigen Erscheinungsformen teilweise mehrstellige Zuwachsraten aus, wobei allgemein noch von einem beträchtlichen Dunkelfeld nicht zur Anzeige gelangter Straftaten ausgegangen wird.

Durch die zunehmende Bedeutung der IT als Bestandteil des privaten und beruflichen Alltags und der immer stärkeren Vernetzung aller Lebensbereiche steigen auch die Manipulations- und Angriffsmöglichkeiten für Cyberkriminelle. Mit einer weiteren Zunahme von Cyberstraftaten dürfte damit zu rechnen sein. Auch die wirtschaftlichen Folgen von Cyberkriminalität haben ein enormes Ausmaß: Im Jahre 2013 bezifferte eine gemeinsame Studie der Internetsicherheitsfirma McAfee und des Centers for Strategic and International Studies (CSIS) die durch Cyberkriminalität verursachten Kosten für die Wirtschaft auf weltweit bis zu einer halben Billion US-Dollar pro Jahr. Andere Schätzungen liegen sogar noch höher.

HERAUSFORDERUNG FÜR STRAFVERFOLGUNGSBEHÖRDEN

Bedingt durch die hohen Wachstumsraten, nimmt der Bereich Cyberkriminalität in der Aufgabenwahrnehmung von Strafverfolgungsbehörden einen immer größeren Raum ein. Die Erfolgsquote bei der Bekämpfung von Cyberkriminalität im Vergleich zur klassischen Kriminalität ist jedoch unterdurchschnittlich. Der ehemalige Chef des Bundeskriminalamts, Jörg Ziercke, beklagte jüngst in einem Interview, dass rund 70 Prozent der Fälle von Internetkriminalität nicht aufgeklärt werden könnten. Angesichts der vielfältigen und immer komplexer werdenden Erscheinungsformen hat der Justizminister von Nordrhein-Westfalen, Thomas Kutschaty, Cyberkriminalität im vergangenen Jahr als „größte Herausforderung für Strafverfolgungsbehörden“ bezeichnet. Cyberkriminelle agieren hochprofessionell – häufig in bandenmäßig organisierten Strukturen –, sind innovativ, anpassungsfähig und nutzen die neuesten Technologien auf der Suche nach immer neuen Einfallstoren. Sie handeln global, nationale Grenzen spielen keine Rolle. Tatorte, Taterfolgsorte und Aufenthaltsort der Cyberkriminellen sind unabhängig voneinander.

Eine effektive strafrechtliche Verfolgung von Cyberkriminalität stellt in operativer, organisatorischer, technischer und rechtlicher Hinsicht an die Arbeit von Strafverfolgungsbehörden besondere Anforderungen.

Eine effektive strafrechtliche Verfolgung von Cyberkriminalität stellt daher in operativer, organisatorischer, technischer und rechtlicher Hinsicht an die Arbeit von Strafverfolgungsbehörden besondere Anforderungen. Traditionelle Arbeitsmethoden, Arbeitsabläufe und Organisationsstrukturen bei Polizei- und Justizbehörden, welche auf die Bekämpfung klassischer Kriminalität ausgerichtet sind, sind für die „Cyberwelt“ unpassend und stoßen wegen ihrer häufigen Schwerfälligkeit schnell an ihre Grenzen. „Zeit“ ist indes – auch wegen der Flüchtigkeit der von Cyberkriminellen hinterlassenen Spuren – für die Bekämpfung von Cyberstraftaten ein entscheidendes Momentum. Eine Chance, Verbesserungen in der Erfolgsquote bei der Bekämpfung von Cyberkriminalität zu erreichen, besteht überhaupt nur dann, wenn die Strafverfolgungsbehörden in Bezug auf Professionalität, Innovationsfähigkeit, Flexibilität und technische Ausstattung mit den Cyberkriminellen „auf Augenhöhe“ agieren können. Auch bei Polizei und Justizbehörden scheint sich diese Erkenntnis durchzusetzen.

SPEZIALEINHEITEN BEI POLIZEI UND JUSTIZ

Die Europäische Union hat Anfang 2013 das Europäische Zentrum zur Bekämpfung der Cyberkriminalität, kurz EC3, eröffnet. Es verbessert

die Zusammenarbeit zwischen den Behörden in den Ländern. Im September 2014 folgte mit der Joint Cybercrime Action Taskforce (J-CAT) der europäischen Polizeibehörde Europol eine neue, länderübergreifende Einsatzgruppe für den Kampf gegen Internetkriminalität. Sie koordiniert internationale Untersuchungen der beteiligten Länder – darunter neben europäischen Vertretern auch Kanada und die USA.

Auch in Deutschland sind in den vergangenen Jahren bei Polizei und Justiz auf Bundes- und Landesebene Spezialeinheiten für die Bekämpfung von Cyberkriminalität aufgestellt worden. Neben einer speziellen Ermittlungsgruppe Cybercrime, die beim Bundeskriminalamt als Bundespolizeibehörde besteht, wurde auf Landesebene im Jahre 2011 beim Landeskriminalamt Nordrhein-Westfalen ein Cybercrime-Kompetenzzentrum als zentrale landesweite Ansprechstelle für Cyberkriminalität geschaffen. Im Juni vergangenen Jahres hat eine entsprechende Spezialeinheit beim Landeskriminalamt Sachsen ihre Arbeit aufgenommen.

Im Hinblick auf die besonderen Anforderungen, die eine effektive Bekämpfung von Cyberkriminalität insbesondere auch an die Zusammenarbeit von Polizei und Staatsanwaltschaften stellt, sind auch Landesjustizbehörden aktiv geworden. Die Vorreiterrolle nahm hier die Generalstaatsanwaltschaft Frankfurt im Jahre 2013 mit der Einrichtung der hessischen Zentralstelle für die Bekämpfung von Internetkriminalität (ZIT) in der Außenstelle Gießen ein.

Die Generalstaatsanwaltschaft Köln hat im Januar vergangenen Jahres als staatsanwaltschaftliche „Komplementäreinheit" zum Cybercrime-Kompetenzzentrum des Landeskriminalamts in Nordrhein-Westfalen die spezialisierte Einheit „Zentralstelle und Ansprechpartner für Cybercrime (ZAC)" ins Leben gerufen. Noch handelt es sich bei diesen spezialisieren Einheiten auf Landesebene um Pilotprojekte. Da eine Aufstellung solcher Sondereinheiten bei Polizei- und Justizbehörden jedoch alternativlos erscheint, um Cyberkriminalität erfolgreich zu bekämpfen, ist zu wünschen, dass andere Bundesländer dem Beispiel von Nordhein-Westfalen, Hessen und Sachsen bald folgen.

ENGE VERNETZUNG MIT SONDEREINHEITEN

Was im Bereich Cyberkriminalität für die Arbeitsmethoden und Arbeitsabläufe innerhalb der Polizei- und Justizbehörden gilt, gilt in gleichem Maße für die Interaktion und Kommunikation zwischen betroffenen Unternehmen und Strafverfolgungsbehörden: Für ein betroffenes Unternehmen, das sich erst zu einem kompetenten und zuständigen Ansprechpartner bei Polizei oder Staatsanwaltschaft „durchtelefonieren" muss oder gar bei der räumlich nächstgelegenen Dienststelle einer Polizei oder Staatsanwaltschaft schriftlich eine Strafanzeige wegen einer Cyberstraftat erstattet, die dann behördenintern in den normalen „Geschäftsgang" gegeben wird, dürften kaum hinreichende Erfolgsaussichten bestehen, dass die Strafverfolgungsbehörden Beweismittel rechtzeitig sichern und Cyberstraftäter „dingfest" machen können.

Um die Chancen für eine erfolgreiche Aufklärung von Cyberstraftaten bestmöglich zu nutzen – mögen diese im Einzelfall wegen tatsächlicher oder rechtlicher Gegebenheiten auch bisweilen gering sein –, ist es für Unternehmen von erheblicher Bedeutung, Zurückhaltung in der Zusammenarbeit mit Polizei und Staatsanwaltschaften abzubauen, sich mit den bestehenden Sondereinheiten zur Bekämpfung von Cyberstraftaten insbesondere auch auf Landesebene eng zu vernetzen und sich bereits im Vorfeld eines Cyberangriffs oder einer Gefahrenlage über Bedingungen, Möglichkeiten und Methoden einer strafrechtlichen Verfolgung sowie einer diesbezüglichen zielführenden Kooperation zwischen Strafverfolgungsbehörden und betroffenen Unternehmen intensiv auszutauschen.

In Ergänzung zu dem regelmäßigen Informationsaustausch, der zwischen dem Bereich Group Cyber- und Datasecurity der Telekom und den mit Fragen der Informationssicherheit befassten Bundesbehörden – Bundeskriminalamt, Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Verfassungsschutz, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – zum Thema Cybersicherheit besteht, hat der Telekomintern für Angelegenheiten des Strafrechts und der Strafverfolgung zuständige Bereich Group Criminal Law seit 2013 mehrere Workshops zum Thema Cyberkriminalität durchgeführt, an denen Behördenvertreter des Cybercrime-Kompetenzzentrums des Landeskriminalamts Nordrhein-Westfalen, der ZAC der Generalstaatsanwaltschaft Köln sowie der Staatsanwaltschaft Bonn teilgenommen haben. Die positive Resonanz aus dem Teilnehmerkreis und das große Interesse gerade auch der Behördenvertreter gibt uns Anlass, den Informations- und Erfahrungsaustausch mit Strafverfolgungsbehörden auf dem Gebiet der Cyberkriminalität weiter zu intensivieren und im Rahmen unserer Kontakte zu Justiz- und Polizeibehörden für den verstärkten Auf- und Ausbau entsprechender Sonderermittlungseinheiten zu werben.

ZUR PERSON

Hans-Lucas Bauer

leitet seit November 2004 den Bereich Group Criminal Law bei der Deutschen Telekom. Zuvor war der Rechtswissenschaftler unter anderem im Justizdienst des Landes Baden-Württemberg als Richter in Zivilsachen und später als Staatsanwalt in einer Schwerpunktabteilung für Wirtschaftskriminalität tätig.

SECURITY IS FOR SHARING – GEMEINSAM STÄRKER

Der Kampf gegen Cyberangriffe gleicht dem Wettrennen von Hase gegen Igel. Damit Unternehmen nicht immer als Verlierer vom Feld gehen, müssen sie kooperieren.

229 Tage. Mehr als 7 Monate. So lange dauert es heute im Durchschnitt, bis Unternehmen einen Cyber-Angriff auf ihre IT-Systeme entdecken. Alle Karten liegen damit beim Angreifer, der seinen Zeitvorsprung ausnutzen und in aller Ruhe wertvolle Geschäftsinformationen stehlen oder Geschäftsprozesse manipulieren kann.

Warum dauert es so lange, Cyberangriffe zu identifizieren? Bisherige Verteidigungsmodelle stoßen an ihre Grenzen, da die wirklich gefährlichen Angreifer unter dem Radar durchfliegen und sich unbemerkt in IT-Systeme einnisten. Natürlich leisten Firewalls und Antiviren-Software noch immer wertvolle Dienste – und werden auch in Zukunft als Basisschutz benötigt – da sie standardisierte Massenangriffe abfangen. Doch sie halten nur die Angriffe und Schadprogramme ab, deren Angriffsmuster bekannt sind.

BEOBACHTEN UND ANALYSIEREN

Daher gleicht die Abwehr von Massenattacken einem Hase-und-Igel-Rennen. Anbieter von Antiviren-Software beobachten und analysieren rund um die Uhr Art und Weise der Angriffe, entwickeln in möglichst kurzer Zeit Filterprogramme und spielen sie sofort in ihre Software ein. Geht alles schnell, sind die Nutzer solcher Antiviren-Programme nach wenigen Stunden gegen die neuen Angriffe gewappnet.

Mit zunehmender „Qualität" der Cyberangriffe gestaltet sich die Abwehr zu einer zunehmend schwierigen Aufgabe. Inzwischen leisten sich Großunternehmen ganze Teams von Sicherheitsspezialisten, die ständig auf Spurensuche sind und bei Angriffen Gegenmaßnahmen einleiten – und ihre wertvollen Erkenntnisse nicht teilen. Denn wie in der Wirtschaft üblich, lassen sich Unternehmen ungern in ihre Karten schauen. Dies gilt auch für die IT-Sicherheit.

Daher findet der Austausch von Informationen eher auf Kongressen statt als im täglichen Einsatz gegen die Cyberattacken.

INFORMATIONSAUSTAUSCH IN ECHTZEIT

Das soll sich ändern. Die Telekom hat im November 2014 eine Initiative ins Leben gerufen, die Sicherheitsexperten von Großunternehmen miteinander fachlich vernetzen soll. Die Ziele des „Cyber Security Sharing and Analytics CSSA e. V.": Über eine branchenübergreifende Plattform teilen die IT-Sicherheitsabteilungen der Mitgliedsunternehmen Informationen zu Cyberattacken in Echtzeit. Weiterhin tauschen sich die CIOs und Sicherheitsexperten der Unternehmen regelmäßig zu aktuellen Erkenntnissen über Angriffsmuster und strategische Fragestellungen zur Abwehr von Cyberangriffen aus.

Bisher tun sich Unternehmen schwer, Cyberangriffe auf ihre IT-Systeme offen zu legen. Erst wenn es zu erfolgreichen Attacken gekommen ist – zum Beispiel das Lahmlegen von Webseiten oder IT-Systemen, die sich auf Geschäftsprozesse mit Kunden auswirken – gehen Unternehmen an die Öffentlichkeit. Zu groß ist nach wie vor die Angst vor Reputationsverlust und Imageschäden. Um die Hemmschwelle für den Informationsaustausch zu senken, können die CSSA-Mitglieder die Daten auf der Plattform anonym teilen.

Die Vorteile einer Austauschplattform für Cybersecurity: Durch den transparenten Austausch von exklusiven Informationen verbessern die teilnehmenden Unternehmen ihre Schlagkraft im Kampf gegen Cyberkriminalität – und setzen das um, was der Bundesinnenminister mit dem Inkrafttreten eines IT-Sicherheitsgesetzes plant: mehr Transparenz und mehr Zusammenarbeit für mehr Sicherheit im Cyberraum.

ZUR PERSON

Dr. Jürgen Kohr
ist Leiter des Geschäftsfelds 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.

INDUSTRIE 4.0 NUR MIT DATENSICHERHEIT

Die Digitalisierung der Industrie verändert die Märkte. Die Ausgangsposition für Deutschland ist hervorragend: Seit jeher stark in den klassischen Ingenieurdisziplinen, punktet Europas stärkste Wirtschaftsmacht zusätzlich mit einem hohen Datenschutz- und Datensicherheitsniveau.

Es ist ganz einfach. Eine frei zugängliche Software aus dem Internet. Eine mobile Verbindung zum Roboter. Und schon lässt er sich mit einem Smartphone aus der Ferne steuern. Die Teilnehmer am Cyber Security Summit 2014 waren verblüfft, wie leicht eine computergesteuerte Maschine manipulierbar ist. Der Live-Hack eines Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI) zeigte eindrucksvoll, welche Hausaufgaben zu erledigen sind, bevor die vierte industrielle Revolution – Industrie 4.0 – ihren Siegeszug antreten kann.

Telekom Vorstand Reinhard Clemens: „Für den Industriestandort Deutschland bedeutet die Vernetzung der industriellen Produktion eine Chance."

Für den Industriestandort Deutschland bedeutet die Vernetzung der industriellen Produktion eine Chance. Kaum einer anderen Nation wird mehr Kompetenz rund um Produktion und Industrie zugeschrieben. Das Ingenieurwissen der vielen traditionsreichen Konzerne und vor allem die Innovationskraft des Mittelstands genießen weltweit einen hervorragenden Ruf. Dagegen ist der Zug der Internetwirtschaft bis auf wenige Ausnahmen fast völlig an Deutschland vorbeigerauscht.

SICHERHEIT „MADE IN GERMANY"

Die Digitalisierung der traditionellen Fertigung könnte eine Wende bedeuten. Sie steht vor einem gewaltigen Umbruch. Die produzierenden Unternehmen müssen das Qualitätsversprechen „Made in Germany" in digitale Geschäftsmodelle umwandeln. Bald wird sich also zeigen, wer die künftigen Player der Industrie 4.0 sind. Die bisherigen Internetgiganten oder die erfolgreichen Industrietitanen?

Einiges spricht dafür, dass in der zweiten Halbzeit der Digitalisierung Europa höhere Spielanteile bekommen könnte. Zwei Drittel der eingebetteten Systeme, die Maschinen steuern, kommen heute schon aus den Ländern der Europäischen Union – Deutschland ist sogar federführend in der Steuerungstechnik. Wie aber lassen sich die vernetzten Automatisierungssysteme gegen Risiken aus dem unsicheren Internet schützen?
Wie wichtig IT-Sicherheit für Industrie 4.0 ist, zeigen die zunehmenden Cyberangriffe auf Industrieanlagen und kritische Infrastrukturen, die für die Versorgung eines Landes zentral sind. Dazu gehören Kraftwerke oder Telekommunikationsnetze. Schwachstellen in Steuerungssystemen von Industrieanlagen sowie unentdeckte Sicherheitslücken können sich fatal auswirken. Ein erfolgreicher Angriff auf lebenswichtige Infrastrukturen hätte Folgen für das gesamte Wirtschaftsgeschehen – nicht nur auf einzelne Unternehmen. Der aktuelle BSI-Bericht zur „Lage der IT-Sicherheit in Deutschland 2014" beschreibt einen gezielten Angriff auf ein deutsches Stahlwerk. Die Angreifer manipulierten das Produktionsnetz, was zu Ausfällen von Steuerungskomponenten oder ganzer Anlagen führte. Eine Anlage wurde massiv beschädigt.

POLEPOSITION FÜR EUROPA

Angst ist allerdings kein guter Ratgeber für Fortschritt und Innovation. Industrie 4.0 bedeutet für Deutschland und ganz Europa eine echte Chance. Zu sehr haben die USA und die bisherigen Stars der digitalen Wirtschaft an Vertrauen eingebüßt: durch nahezu ungebremstes Abschöpfen von Informationen sowie Geschäftsmodellen, die auf das Sammeln, Auswerten und Verkaufen von Daten der eigenen Kunden beruhen. Das Killerkriterium ist deshalb: Sicherheit der Daten. Von den Unternehmen und Verbrauchern über Jahre eher vernachlässigt, haben sich Datenschutz und Datensicherheit inzwischen zu wichtigen Grundpfeilern im fairen Miteinander entwickelt.
Noch braucht es einige Jahre, bis Industrie 4.0 flächendeckend in der Produktion Einzug hält, bis komplette Produktlebenszyklen vernetzt sind. Darin liegt unsere Chance. Mit Cloud- und Machine-to-Machine-Technologie sind die technischen Grundlagen gelegt. Europa hat als Faustpfand das Wissen aus dem Maschinenraum, steht auf der Poleposition. Aber wir alle wissen: Wer von ganz vorn startet, ist der Gejagte und nicht immer der Sieger. Wir müssen uns also ranhalten. Die Fähigkeit der deutschen Wirtschaft, Industrie 4.0 schnell und mit einem angemessenen Sicherheitsniveau einzuführen, wird über die Wettbewerbsfähigkeit des Industriestandorts Deutschland entscheiden.

ZUR PERSON

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

BIG DATA – ANONYMISIERUNGSVERFAHREN

Das Berliner Start-up Motionlogic GmbH entwickelt und vertreibt selbstlernende Analysesysteme, die aus großen Datenmengen – Big Data – Muster und Zusammenhänge erkennen, um damit Prozesse und Abläufe in Unternehmen zu optimieren. Die Telekom ist zu 100 Prozent an Motionlogic beteiligt.

Big-Data-Lösungen haben zum Ziel, große Datenmengen in Echtzeit auszuwerten und mit anderen Daten zu verknüpfen. Aus Datenschutzsicht wird das oft kritisch bewertet. Die Telekom hat daher für eigene Big-Data-Projekte Leitsätze entwickelt, welche die ungefilterte Analyse von personenbezogenen Daten verhindern sollen. Dort heißt es unter anderem: Die Deutsche Telekom verarbeitet Daten für Big-Data-Lösungen grundsätzlich in anonymisierter Form, sodass Rückschlüsse auf einzelne Personen ausgeschlossen sind.

ANONYMISIERTE DATEN

Der Konzerndatenschutz unterstützt Motionlogic dabei, marktfähige Geschäftsmodelle auf Basis von anonymisierten Telekommunikationsdatensätzen zu realisieren. Die Telekom plant die Verknüpfung von anonymisierten Signalisierungsdaten aus der Netztechnik mit anonymisierten Attributen aus der Kundendatenbank. Die daraus erstellten anonymisierten Datensätze sollen an Motionlogic übermittelt werden. Ein Rückschluss auf Einzelpersonen ist nicht möglich. Dazu haben die Datenschützer verschiedene Sicherheitsmechanismen im Verfahren eingefügt. Das Start-up nutzt diese anonymen Daten zum Beispiel für Verkehrswegeanalysen für städtebauliche Entwicklung oder Unternehmen.

Die Telekom hat das Anonymisierungsverfahren im Februar 2014 der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vorgestellt. Die BfDI hat das Verfahren grundsätzlich positiv bewertet, jedoch stand Anfang 2015 eine finale Bewertung noch aus. Erst wenn die BfDI das Anonymisierungsverfahren ebenfalls als rechtlich zulässig bewertet hat, wird die Motionlogic GmbH ihre Analyselösungen vermarkten und die Telekom das Verfahren für andere Big-Data-Lösungen einsetzen.

ZERTIFIZIERTER DATENSCHUTZ

Kunden- und Mitarbeiterdaten sind bei der Telekom in besten Händen. Die Datenschutzorganisation und -mechanismen des Konzerns zeigen Wirkung. Damit ist die Telekom mit ihrem Datenschutz-Compliance-Management-System als erstes Unternehmen weltweit nach dem IDW PS 980 auf seine Wirksamkeit hin zertifiziert worden.

Wissen ist besser als glauben: Mit dieser Maxime hat die Telekom im Sommer 2014 rund drei Monate lang ihre Datenschutzorganisation konzernweit auf den Prüfstand stellen lassen. Wirtschaftsprüfer von Deloitte haben die vorhandenen Systeme und Prozesse analysiert und geprüft, ob sie wirksam sind.

Dafür wurde das gesamte Datenschutz- Compliance-Management-System mit seinen Abläufen, Prüfprotokollen und Audits auf seine Ausgestaltung und Umsetzung im Konzern begutachtet. Prozesse wurden analysiert und entlang ihrer Maßnahmenkette nachvollzogen. Die Prüfung der notwendigen Implementierung in IT-Systemen erfolgte ebenso wie eingehende Interviews mit den Mitarbeitern, die an den Prozessen beteiligt sind.

Die Wirtschaftsprüfer haben für die Zertifizierung den Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer in Deutschland, kurz IDW PS 980, angewandt. Er definiert die „Grundsätze ordnungsgemäßer Prüfung von Compliance-Management-Systemen“ und bietet eine Grundlage zur Prüfung von Datenschutzorganisationen auf Einhaltung von Gesetzen, Regelungen und Selbstverpflichtungen.

Ein Kurzbericht über die Zertifizierung ist im Internet unter www.telekom.com/verantwortung/datenschutz/datenschutz-im-unternehmen/22790 veröffentlicht.

STANDARD FÜR SICHERE E-MAILS

Seit dem 29. April 2014 kommunizieren die rund 50 Millionen deutschen Privatkunden im Mailverbund „E-Mail made in Germany“ (EmiG) von Telekom, freenet, GMX und WEB.DE unabhängig vom genutzten E-Mail-Programm automatisch auf allen Transportwegen verschlüsselt.

Darüber hinaus garantieren die beteiligten Provider, Daten nur gemäß deutschem Datenschutz in sicheren Rechenzentren zu speichern und zu verarbeiten. Ein grüner Haken als Kennzeichen in den Webmailservices zeigt direkt an, ob der Provider die jeweilige Mail nach den Sicherheitsstandards des Verbunds zustellen kann. Dies hängt davon ab, ob der Empfänger einer E-Mail eine Adresse bei einem der Provider des Verbunds hat. Rund zwei Drittel der privaten E-Mail-Anwender in Deutschland nutzen E-Mail-Dienste von Telekom, United Internet – GMX, WEB.DE – oder freenet und nehmen somit automatisch an der Initiative „E-Mail made in Germany“ teil. Das Versenden von E-Mails an andere Anbieter wie Google, Yahoo oder Microsoft ist weiter möglich, aber weder die sichere Übertragung noch die Datenverarbeitung in Deutschland sind dann sichergestellt.

SICHERE E-MAIL AUCH FÜR UNTERNEHMEN

Auch die beiden größten deutschen Hostingunternehmen 1&1 und Strato und deren rund drei Millionen Firmenkunden ohne eigene Mailserver können an dem sicheren Verbund teilnehmen, wenn sie dies per Mausklick für ihre Domain aktivieren. Außerdem bietet der TÜV Rheinland allen Unternehmen und Institutionen mit eigener E-Mail-Infrastruktur die Möglichkeit, sich für „E-Mail made in Germany“ zertifizieren zu lassen, um mit Endkunden und Geschäftspartnern verschlüsselt kommunizieren zu können. „In puncto sicherer Kommunikation ist das auf jeden Fall ein Gewinn“, erklärte Björn Haan, Geschäftsführer der TÜV Rheinland i-sec, anlässlich des EmiG-Starts. „Wer eine Nachricht mit dem Signet ‚E-Mail made in Germany‘ versendet oder erhält, kann sicher sein, dass für Übertragung und Verarbeitung ein höheres Niveau in Datenschutz und Datensicherheit gilt als bei herkömmlichen E-Mails mit Speicherung außerhalb Deutschlands.“

DEUTSCHE VERSCHLÜSSELUNGSZERTIFIKATE

Die erfolgreiche Verschlüsselung durch „E-Mail made in Germany“ ist ein wichtiger Baustein der Telekom Sicherheitsstrategie. Die Akzeptanz der gemeinsam von Telekom und United Internet gestarteten Initiative ist sehr hoch. Dies zeigt eine Untersuchung des Marktforschungsinstituts YouGov, nach der rund 58 Prozent der Befragten die Initiative als sehr hilfreich bewerten: Sie wollen nicht, dass unbefugte Dritte ihre E-Mails mitlesen.

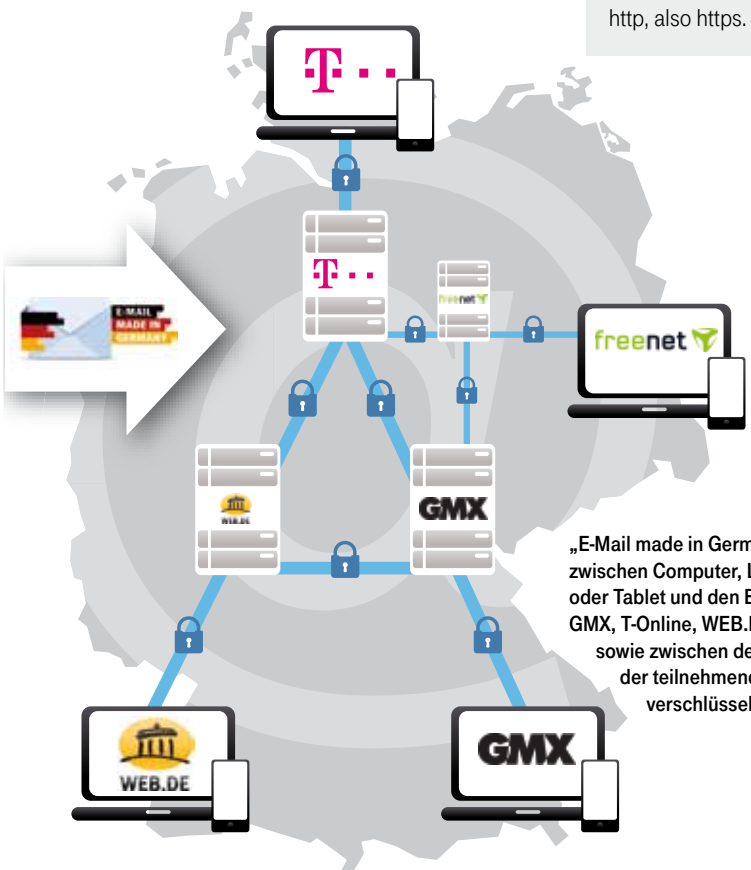
Mit Umsetzung der 100-prozentigen TLS-Verschlüsselung (Transport Layer Security) hat die Initiative auch die Sicherheitsstandards erweitert: Zum Einsatz kommen nur deutsche TLS-Zertifikate. Darüber hinaus haben alle Partner im Verbund Perfect Forward Secrecy implementiert, was einen zusätzlichen Schutzmechanismus gegen das nachträgliche Entschlüsseln von Daten bietet.

IDENTITÄTSPRÜFUNG

Ferner haben die Provider ein neues Verfahren zur Zertifikatsvalidierung und Identitätsprüfung eingerichtet. Bei jeder Datenübertragung werden Zertifikat und Identität des Providers überprüft, um zu verhindern, dass sich Dritte in die Kommunikation einschalten. Auch die verwendeten Schlüssel wurden auf einen der derzeit sichersten Standards (AES 256 Bit) aufgerüstet.

KURZ ERKLÄRT

TLS: Transport Layer Security
Das TLS-Übertragungsprotokoll – Nachfolger von Secure Sockets Layer (SSL) – ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet, von E-Mails oder beim Zugriff auf Websites. Es transportiert Inhalte nur verschlüsselt, die Identität des Servers steht fest und es wird geprüft, ob Daten vollständig und unverändert ihren jeweiligen Empfänger erreichen. Erkennbar ist die TLS-Verschlüsselung bei Websites an dem s hinter http, also https.



„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.

VERTRAUEN SICHERN

Die Zahl der Angriffe aus dem Internet steigt weiter an. Die Methoden der Angreifer ändern sich ständig. Sie lassen sich nur mit großem Aufwand analysieren und abwehren.

70
Mitarbeiter des Konzern-datenschutzes prüfen IT-Systeme, -Prozesse und neue IT-Produkte der Telekom

1,16
Millionen Kreditkartendaten haben Hacker zwischen Juli und September 2014 von der US-Büroartikelkette Staples erbeutet

10.000
Anfragen zum Datenschutz gingen an datenschutz@telekom.de

170
nationale Datenschutzkoordina-toren unterstützen im Konzern bei Aufgaben rund um den Datenschutz

400.000
neue Viren überschwemmen täglich das Netz

40
Prozent der Internetnutzer in Deutschland wurden 2013 mit Schadsoftware angegriffen und deren Computer infiziert

575
Milliarden Dollar wirtschaftlichen Schaden hat im Jahr 2013 die Internetkriminalität verursacht

2.500
Entwicklungsprojekte durchlaufen pro Jahr das Privacy-and-Security-Assessment-Verfahren (PSA)

5
gezielte Angriffe täglich registriert das verschlüsselte Regierungsnetz

1.000.000

Angriffe registriert die Telekom pro Tag auf ihre Netze

Audits – national und international – haben interne und externe Prüfer bei der Telekom durchgeführt

27

580

Teilnehmer registriert die Allianz für Cybersicherheit

9

von 10 Firmen in Deutschland sind schon Ziel von Angriffen aus dem Netz gewesen

2

Millionen Hinweise zu missbrauchten Kundensystemen hat das Abuse-Team allein im Oktober 2014 verarbeitet

35.000

Kunden monatlich schreibt das Abuse-Team an, um sie über schadcode-infizierte Rechner zu informieren

180

Honeypots betreibt die Telekom, um die Methoden der Angreifer zu analysieren

54

Data Protection Officer gibt es insgesamt an den internationalen Standorten der Telekom

1.444

Sicherheitswarnungen und Handlungsempfehlungen sowie 43 Incidents veröffentlichte das Telekom CERT

HUNTER TEAMS GEGEN WIRTSCHAFTSSPIONE

Im April 2014 nahm die neue Spionageabwehr der Telekom ihren Dienst auf: Das Cyber Defense Center (CDC) geht mit einer Analystenelite, einem SIEM-System (Security Information and Event Management), Angriffsmodellierung und korrelierten Logdatenauswertungen gegen Spione vor, die das Netz des Konzerns penetrieren.

Viele Cyberkriminelle betreiben heute gezielte Wirtschaftsspionage. Sie suchen nicht nach beliebigen Daten, sondern haben es gezielt auf Patente, Hochtechnologie und anderes wertvolles Firmen-Know-how abgesehen. Dabei steht ihnen mitunter ein nahezu unbegrenztes Maß an Zeit und Ressourcen zur Verfügung. Ähnliches gilt für Nachrichtendienste, die im Regierungsauftrag spionieren.

„Wenn ein Geheimdienst oder ein hoch motivierter professioneller Wirtschaftsspion ein Unternehmensnetzwerk infiltrieren will", erläutert Bernd Eßer, Leiter des Cyber Defense Centers, „ist er früher oder später erfolgreich." Entweder er bricht über die Netze ein oder nutzt andere Methoden, etwa einen mit Schadsoftware infizierten USB-Stick, der auf dem Firmenparkplatz ausgelegt wird. Oder er schleust einen Mitarbeiter ein, der einen Arbeitsplatz mit Malware infiziert.

EINDRINGLINGE AUFSPÜREN

Von einem mit Malware infizierten Arbeitsplatzrechner kann sich ein Krimineller immer weiter vorarbeiten, bis er sich Zugriff auf wertvolle Informationen verschafft hat. „Das dauert allerdings", weiß Bernd Eßer, „denn er muss sich erst einmal im Netz orientieren und mühsam vorarbeiten." Bis er ein Netz von der Größe eines DAX-Unternehmens kartografiert und die gewünschten Informationen lokalisiert hat, können Wochen und Monate vergehen.

Wirklicher Schaden entsteht erst, wenn der Spion die Daten ausfindig gemacht und ins Internet übertragen hat. Darum lautet die Aufgabe der Cyberspionageabwehr, einen Eindringling so schnell wie möglich ausfindig zu machen und die Sicherheit wiederherzustellen, bevor er Wissen stehlen konnte.

Bernd Eßer und sein Team schützen den Konzern und seine Kunden vor Gefahren aus dem Internet. Im Angriffsfall schreiten sie sofort ein, damit alle Informations- und Netzwerktechnologien zuverlässig weiterarbeiten und schnellstmöglich von Schadsoftware bereinigt werden. Die IT-Forensiker des CDC gehen pragmatisch vor, um ihre Aufgabe zu erfüllen. Sie führen komplexe Daten aus verschiedenen Quellen zusammen und werten sie aus, um Unregelmäßigkeiten zu entdecken, die regulären Sicherheitslösungen entgehen. Zu ihren Quellen zählen unter anderem die Firewall des Konzerns, die Intrusion-Prevention-Systeme, die Proxyserver, die Exchangeserver, die Antiviruslösung der Telekom und die Active-Directory-Server.

SCHADEN VERHINDERN

Aufgrund ihrer jahrelangen Erfahrung können die Sicherheitsspezialisten die Vorgehensweise der Täter in Use Cases zerlegen und die Logquellen gezielt nach Indikatoren für diese Angriffe durchsuchen. Ein SIEM-System (Security Information and Event Management) unterstützt sie dabei, indem es die verschiedenen Logdaten sammelt und sofort nach den von den Analysten festgelegten Kriterien auswertet. Wird eine Korrelation von Ereignissen festgestellt, die im Rahmen eines Use Cases definiert wurde, alarmiert das System ein „Hunter Team" – einsatzbereite Experten, die den Vorfall prüfen und die Sicherheit im Falle eines korrekten Alarms schnellstmöglich wiederherstellen.

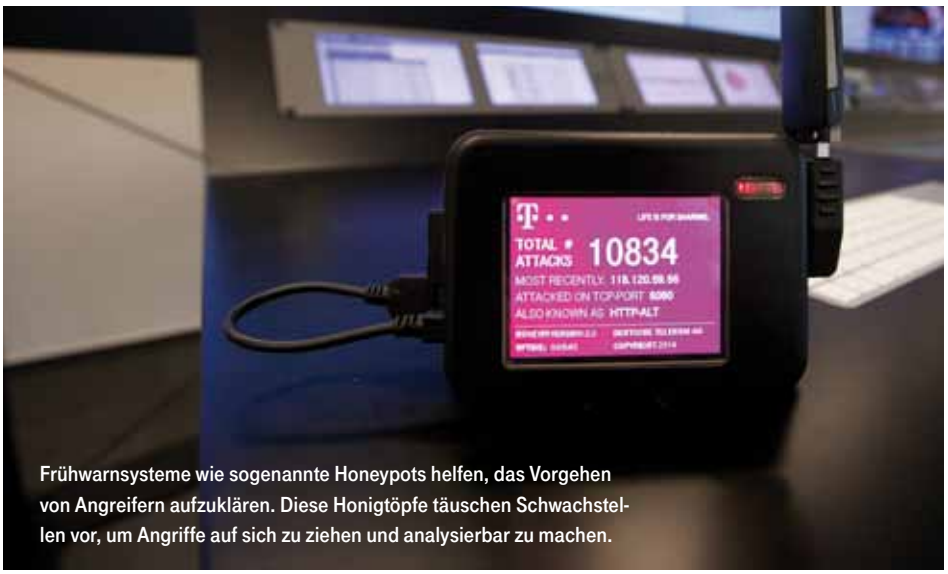
Die komplexen Use Cases machen den Telekom Ansatz besonders, da sie Informationen aus unterschiedlichen Quellen miteinander verknüpfen. Dadurch erhalten die Hunter Teams des Cyber Defense Centers eine überschaubare Zahl von Notifikationen mit sehr hoher Trefferquote. Üblicherweise generiert ein SIEM-System eine hohe Zahl von False Positives – Fehlalarme, die hohen Aufwand erzeugen. Die Telekom wertet vergleichsweise wenige Ereignisse aus einer geringen Zahl von Quellen aus, erzielt durch die Korrelation der Daten jedoch kaum Beifang. Erreicht ein Use Case nicht die erforderliche signifikante Trefferquote, wird er aus dem System gelöscht, damit nicht unnötigerweise Daten erhoben und ausgewertet werden.

ANGRIFFSTRENDS ERKENNEN

Einige Analysten des CDC führen kontinuierlich das Wissen der Kollegen zusammen, um die Use Cases weiterzuentwickeln, aktuellen Angriffstrends anzupassen und neue Szenarien zu modellieren. Zunächst arbeiten die Spezialisten des Cyber Defense Centers ausschließlich für die interne Sicherheit der Telekom. In Kürze bietet T-Systems die Leistungen auch als Managed Service für Kunden an.

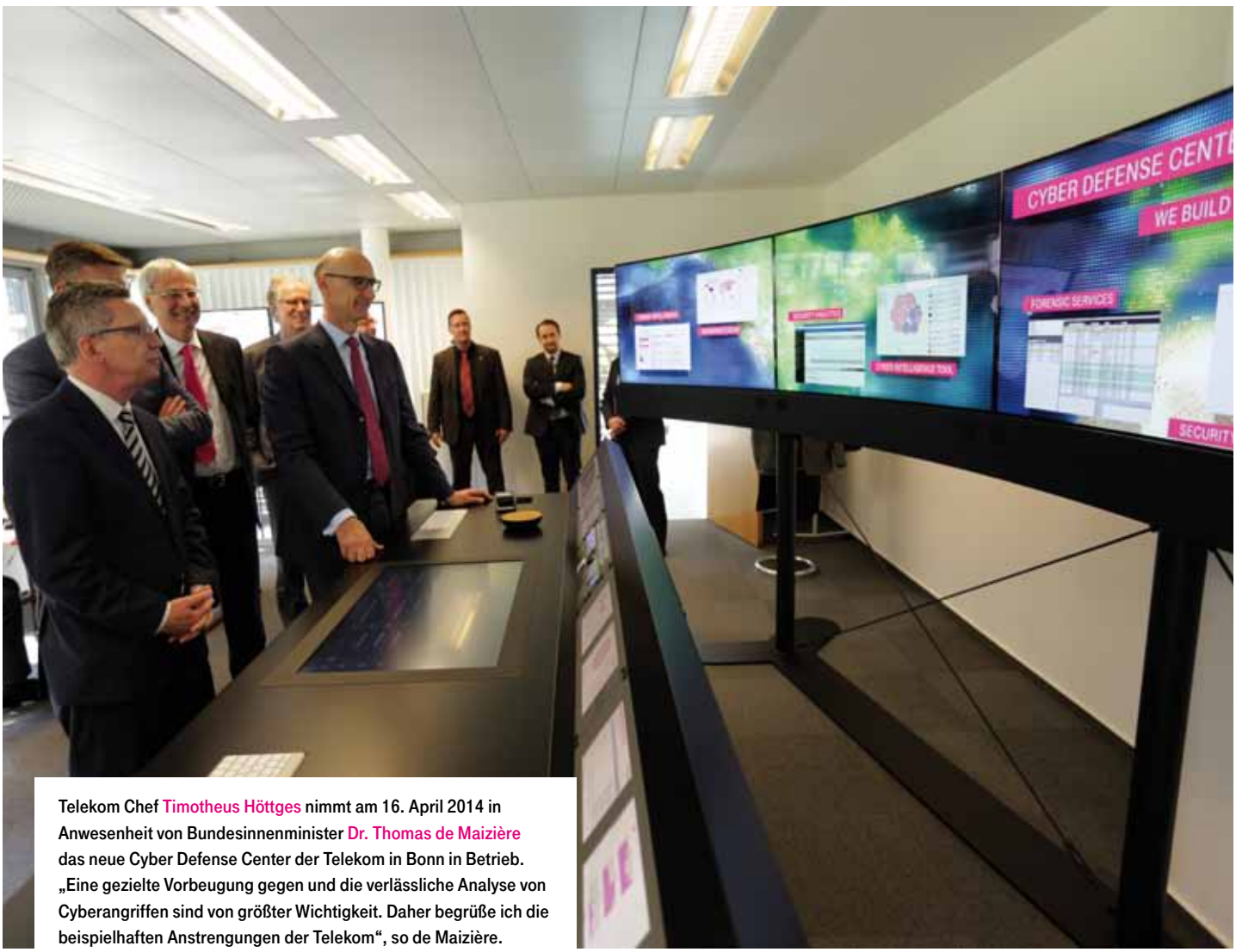
KURZ ERKLÄRT

SIEM
SIEM steht für Security Information and Event Management. Diese Systeme sind in der Lage, sicherheitsrelevante Ereignisse in Echtzeit zu identifizieren, zu bewerten und zu alarmieren. SIEM-Systeme nutzen hierfür Millionen von Meldungen von IT-Systemen und setzen sie miteinander in Beziehung.



Frühwarnsysteme wie sogenannte Honeypots helfen, das Vorgehen von Angreifern aufzuklären. Diese Honigtöpfe täuschen Schwachstellen vor, um Angriffe auf sich zu ziehen und analysierbar zu machen.

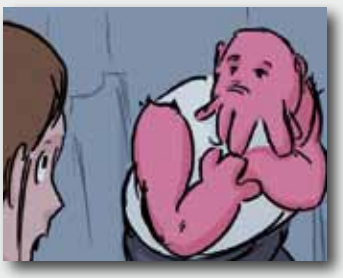
Das Cyberabwehrzentrum setzt auf verhaltensbasierte Analysemethoden: Mittels spezieller Sensoren werden gezielt Verhaltensmuster erkannt, die auf einen Cyberangriff verweisen



Telekom Chef Timotheus Höttges nimmt am 16. April 2014 in Anwesenheit von Bundesinnenminister Dr. Thomas de Maizière das neue Cyber Defense Center der Telekom in Bonn in Betrieb. „Eine gezielte Vorbeugung gegen und die verlässliche Analyse von Cyberangriffen sind von größter Wichtigkeit. Daher begrüße ich die beispielhaften Anstrengungen der Telekom“, so de Maizière.

HAB ACHT, DATENSCHLONZ!

Hollywood im Telekom Intranet: Mit einem kurzen Filmtrailer als Vorgeschmack hat der Konzerndatenschutz im Dezember eine weltweite Awareness-Kampagne eingeleitet.



Wer kennt das nicht? Der Schreibtisch voll mit Unterlagen, darunter auch das ein oder andere Schreiben, das nicht unbedingt in fremde Hände geraten sollte. Dann ist Feierabend und der Weg zum abgesicherten Aktenschrank oder zum Papierschredder zu weit. Schnell alles zusammengerafft, höchstens noch in der unverschlossenen Schublade verstaut und raus aus der Tür.

Solche alltäglichen Szenarien – die in Eile schon jeder persönlich erlebt hat – passieren ohne böse Absicht, sind aber aus Sicht des Datenschutzes problematisch. Denn auf diese Weise können personenbezogene und oft vertrauliche Informationen ungewollt in falsche Hände geraten. Darauf soll ab Januar 2015 die Telekom Mitarbeiter der Datenschlonz als Hauptdarsteller einer Filmserie aufmerksam machen und ihr Verhalten aus Sicht des Datenschutzes verändern. Unterstützt wird die interne Kommunikationskampagne durch einen Wettbewerb. Hier können die Beschäftigten weltweit ihre Ideen zu solchen Alltagssituationen einbringen und vorstellen, wie man sie (nicht) löst.

SICHERHEIT WIRD FÜHRENDES MESSETHEMA

Ganz gleich, ob auf CeBIT, Internationaler Funkausstellung (IFA) oder it-sa – Datenschutz und Datensicherheit zählten 2014 zu den Themen, bei denen die Telekom den größten Zuspruch der Messebesucher fand.

Fach- und Publikumsmessen sind für die Deutsche Telekom ein zentrales Mittel, um das öffentliche Bewusstsein für Datenschutz und Datensicherheit zu stärken. Dabei konzentriert sich das Unternehmen auf die CeBIT als führende ITK-Fachmesse, die IFA als weltgrößte Messe für Unterhaltungselektronik und die it-sa als wichtigste Fachmesse für Informationssicherheit im deutschsprachigen Raum. Das umfassende Informationsangebot reicht vom Schutz privater Daten über den sicheren Betrieb mobiler Endgeräte bis zur Sicherheit im Cloud Computing.

GROSSES INTERESSE

Wie wichtig die Aufklärung der Internetnutzer über die Risiken ist, zeigen die Ergebnisse des Sicherheitsreports 2014, einer repräsentativen Befragung des Instituts Allensbach im Auftrag der Telekom. Danach glauben 74 Prozent der Befragten, dass die Gefahr vor Datenbetrug im Internet zunehmen wird. Auch die messebegleitende Marktforschung ergab, dass Sicherheitsthemen im Zentrum des Publikumsinteresses angekommen sind: In der Gunst der Standbesucher belegten Datenschutz und Datensicherheit stets die vordersten Plätze. Zudem zeigten die Untersuchungen, dass die Mehrzahl der Besucher Sicherheit als wichtigen Bestandteil der Marke Telekom sieht.

Auf der Internationalen Funkausstellung wurde das Standpersonal von Mitarbeitern des Bürger-CERT unterstützt, mit dem sich das Bundesamt für Sicherheit in der Informationstechnik an Endverbraucher und kleinere Unternehmen wendet. Eines der wesentlichen Ziele des IFA-Auftritts bestand darin, die Besucher in die Lage zu versetzen, selbst zu entscheiden, auf welchem Datenschutz- und Datensicherheitsniveau sie sich bewegen wollen. Um die Messeinformation zu vertiefen, brachte die Telekom rechtzeitig zum Beginn der IFA den multimedialen Onlineratgeber sicherdigital.de an den Start. Kinder, Jugendliche, Eltern, Erwachsene und Kleinunternehmer erhalten dort praktische Hinweise (inklusive Selbsttests), wie sie sich und ihre Privatsphäre vor Cyberbedrohungen durch veränderte Einstellungen besser schützen können.

ANGRIFFSVERSUCHE MITVERFOLGEN

Im Mittelpunkt des CeBIT-Auftritts stand das neue Cyberabwehrzentrum der Deutschen Telekom. Messebesucher erhielten Einblick in die Leitzentrale des Zentrums. Deren Herzstück bildet eine Analyseumgebung, die Verhaltensmuster sichtbar macht, welche auf Cyberangriffe hinweisen.

Am Messestand hatten die Besucher Gelegenheit, aktuelle Angriffsversuche mitzuverfolgen und mit Securityexperten über passende Antworten zu sprechen. Auf diese Weise war es der Telekom möglich, die Messegäste für relevante Bedrohungen zu sensibilisieren und Anknüpfungspunkte für individuelle Beratungsgespräche zu finden.

SICHER LEBEN IN DER DIGITALEN WELT

Cyberkriminelle, Schadsoftware und Phishingbetrug? Mit dem Onlineratgeber [sicherdigital] bietet die Telekom nützliche Tipps und Hilfestellungen rund um Sicherheit und Datenschutz in der digitalen Welt.

Unter www.sicherdigital.de finden Jugendliche, Erwachsene und Unternehmen nützliche Hinweise und konkrete Hilfe rund um die Themen Sicherheit und Datenschutz bei allen Berührungspunkten mit der digitalen Welt. Der Ratgeber orientiert sich an den Informationswünschen des Nutzers: „Welche Risiken habe ich und wie kann ich mich schützen?“ Er bietet den Besuchern der Site einen explorativen Zugang zu sicherheitsrelevanten Themen, die der Lebenswirklichkeit der Zielgruppen entsprechen. Repräsentiert werden die Zielgruppen über die Jugendlichen Lena und Lukas, die Mutter Sandra mit ihrem Sohn Max und den Unternehmer Matthias.

Zu jeder Person wird ein fiktiver Tagesablauf dargestellt, der typische Situationen enthält, bei denen Sicherheit und Datenschutz eine Rolle spielen. Für Lena und Lukas etwa beginnt der Tag auf dem Weg zur Schule, bei dem sie über ihre Smartphones mit Freundinnen und Freunden chatten. Später besuchen sie soziale Netzwerke, surfen vor den Hausaufgaben im Internet, bis sie schließlich vor dem Zubettgehen noch eine App herunterladen.

SICHERHEIT SPIELERISCH ENTDECKEN

Die intuitive Benutzerführung lädt den Besucher ein, sich spielerisch mit diesen Szenarien und den damit verbundenen Sicherheitsrisiken auseinanderzusetzen. In Detailbeiträgen erklärt die Telekom, worauf die Nutzer achten sollten und wie sie sich effektiv vor Bedrohungen schützen können – zum Beispiel mit den richtigen Grundeinstellungen im Betriebssystem des Smartphones oder mit speziellen Benutzerkonten für Kinder und Jugendliche. Neben informativen Artikeln bietet der Leitfaden eine Reihe von Checklisten, in denen die wichtigsten Tipps zu einem Thema übersichtlich zusammengefasst sind. Darüber hinaus kann der Nutzer seine Sicherheit mit interaktiven Fragebogen selbst überprüfen oder sich in einer Reihe von Filmbeiträgen ansehen, wie die unterschiedlichen Charaktere mit dem Thema Sicherheit umgehen.

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

WISSEN MIT ANDEREN TEILEN

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

Der Sicherheitsratgeber wird kontinuierlich weiterentwickelt und aktualisiert. Inhalte lassen sich über das Onlineformat leicht austauschen und ergänzen, um mit dem Tempo in der digitalen Welt Schritt zu halten. Social-Media-Funktionalitäten bieten dem Nutzer zudem Gelegenheit, Beiträge und Filme zu teilen. Frei nach dem Motto „Security is for Sharing.“

DA IST DATENSCHUTZ DRIN

Das Privacy Icon der Telekom zeigt Kunden, wo sie Datenschutzhinweise oder Einstellungsmöglichkeiten zum Datenschutz finden. Wiedererkennungswert garantiert.

Überall, wo Kunden der Telekom auf das Privacy Icon stoßen, geht es um das Thema Datenschutz. Seit Sommer 2014 findet es sich etwa auf der Firmware-Benutzeroberfläche der Speedport-Router und in der DSL-Hilfe-App. Unter dem Icon geht es zu den Einstellungsmöglichkeiten, mit denen ein Kunde seine IP-Adresse ändern kann, um mehr Anonymität im Internet zu erreichen.

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

Als Sinnbild für Datenschutz mit hohem Wiedererkennungswert findet es sich auch überall dort, wo die Telekom Datenschutzhinweise bietet, etwa bei Auftragsbestätigungen oder im Business Marketplace. Dort finden sich sogar noch weitere Icons, die Aufschluss über den Hostingstandort von Cloud-Applikationen bieten und erklären, wer Zugriff auf Kundendaten hat.

Im neuen Telekom Browser 7 dient das Privacy Icon als Symbol für den privaten Modus, der mehr Anonymität im Internet gewährt. Bei einer der Connected-Car-Lösungen der Telekom ermöglicht ein Privacy Button, Privatfahrten bei Geschäftsfahrzeugen zu markieren, bei denen keine Daten erfasst werden. Künftig kommt das Symbol auch in den Telekom Shops auf Austauschgeräten zum Einsatz und erinnert den Kunden daran, seine Daten vor Rückgabe des Geräts zu löschen.

40 MILLIONEN DOKUMENTE QUALIFIZIERT SIGNIERT

Die Telekom setzt seit elf Jahren auf die elektronische Personalakte. 2011 forderte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) den Konzern auf, die Akten der Beamten qualifiziert zu signieren. Das Personalwesen passte die Akten der Arbeitnehmer gleich mit an. Mehr als 40 Millionen Dokumente erhielten eine qualifizierte elektronische Signatur.

2004 läutete die Telekom das Ende der papiergebundenen Personalakte ein. Seither hat der Konzern in Deutschland rund 115.000 elektronische Personalakten für seine Beamten und etwa 130.000 für seine Angestellten erstellt. Elektronische Personalakten machen die mitarbeiterbezogenen Unterlagen zentral verfügbar. Zusätzlich zu den Personalern haben auch die Mitarbeiter die Möglichkeit, sich ihre Akten über ein besonders gesichertes Intranetportal anzuschauen. Wer welche Zugriffsrechte hat, regelt eine Konzernbetriebsvereinbarung, welche die Telekom gemeinsam mit dem Sozialpartner abgeschlossen hat.

VERÄNDERTE RISIKOLAGE

Um die Integrität der elektronischen Dokumente zu schützen, nutzte die Telekom bis 2013 das kryptografische MD5-Checksummenverfahren. Dieser weltweit verbreitete Verschlüsselungsstandard galt unter Datenschützern und Sicherheitsexperten bis dahin als sicher. Da potenzielle Angreifer jedoch über immer leistungsstärkere Rechner verfügen, entstehen mehr und mehr Risiken für das Schutzniveau, das sich mit dem MD5-Verfahren erreichen lässt. Vor diesem Hintergrund forderte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Telekom auf, alle Dokumente ihrer elektronischen Beamtenakten nur noch qualifiziert signiert abzulegen. Dies bedeutet, dass jedes Dokument eine elektronische Signatur erhält, welche die hohen Anforderungen des deutschen Signaturgesetzes erfüllt.

Die veränderte Maßgabe galt sowohl für die neu aufzunehmenden Dokumente als auch für die bereits in den Personalakten enthaltenen Unterlagen. Nach Ansicht aller Projektbeteiligten lag darin eine Herausforderung, die in ihrer Größenordnung in Deutschland bis dahin noch ohne Beispiel war. Zumal sich die Telekom dazu entschlossen hatte, nicht nur die Beamtenakten, sondern auch die Akten der sozialversicherungspflichtig Beschäftigten auf das höhere Schutzniveau zu bringen. Insgesamt ging es somit um über 40 Millionen Dokumente in rund 245.000 elektronischen Personalakten. Dass die Zahl der Personalakten mehr als doppelt so hoch ist wie die aktuelle Zahl der Mitarbeiter in Deutschland, liegt an den gesetzlichen Aufbewahrungsfristen sowie an der hohen Anzahl beamteter Versorgungsempfänger.

SOZIALPARTNER EINBINDEN

Um die elektronischen Signaturen nicht nur rechtskonform, sondern auch kostenschonend zuzuweisen, entwickelte die Telekom ein Blocksignaturverfahren, mit dem sich die manuelle Bearbeitung auf ein Minimum beschränken lässt. Das Vorgehen stimmte der Konzern mit dem BfDI und dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) ab. Zudem waren auch der Konzernbetriebsrat und der Konzerndatenschutz in die gesamte Prozessgestaltung aktiv eingebunden. Zusätzlich zur qualifizierten Signatur haben sich die Beteiligten auch schon über das nächste Großvorhaben abgestimmt: Im Frühjahr 2015 wird die Telekom alle noch vorhandenen Beamtenpapierakten vernichten. Mit diesem Schritt geht das Zeitalter der papiergestützten Personalakte dann auch im physischen Sinn zu Ende.

HOHES DATENSCHUTZNIVEAU ATTESTIERT

Das Basisdatenschutzaudit gibt Auskunft darüber, wie ausgeprägt das Wissen der Telekom Mitarbeiter in puncto Datenschutz ist und wie sie dieses Know-how im Tagesgeschäft umsetzen. 2014 hielten die Kennzahlen das hohe Niveau und legten international weiter zu.

Wissen Sie, wie sich E-Mails mit personenbezogenen Daten 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. 2014 wurden 30 Prozent repräsentativ ausgewählte Mitarbeiter in Deutschland und aus 34 Landesgesellschaften zur Teilnahme eingeladen.

Die Ergebnisse zeigen für alle Landesgesellschaften, dass das Datenschutzniveau die hohen Vorjahreswerte erneut erreicht und international noch einmal übertroffen hat. Dies belegt die Hauptkennzahl, mit der die Prüfer die zahlreichen Einzelergebnisse des Audits in einem einzigen Wert zusammenfassen. Während die Hauptkennzahl in Deutschland im Jahresvergleich auf dem sehr hohen Niveau von 9,6 Punkten stabil blieb, ergab sich international ein weiteres Wachstum. Nach 7,6 im Jahr 2013 kamen die Landesgesellschaften 2014 auf einen neuen Spitzenwert von 7,9. Auch die Teilnahmequote konnte noch einmal gesteigert werden.

ENTSCHEIDERINFORMATIONSSYSTEM

2013 stoppte die Telekom das SAP Business Warehouse EIS (Entscheiderinformationssystem). Es bestand der Verdacht, das EIS hätte unerlaubt personenbezogene Informationen von Beschäftigten ausgewertet. Eine unabhängige externe Wirtschaftsprüfungsgesellschaft hat den Vorfall geprüft. Der Verdacht hat sich nicht bestätigt.

Eine vom Konzerndatenschutz durchgeführte Prüfung hatte ergeben, dass entgegen den Angaben des verantwortlichen Bereichs die Software personenbezogene Daten der Telekom Mitarbeiter enthält. Dies ist nur dann erlaubt, wenn datenschutzrechtliche Vorgaben eingehalten und die Daten für einen legitimierten Zweck verwendet werden. Auf Basis der vorgefundenen Informationen ergaben sich aber keine Hinweis darauf, dass die Daten in irgendeiner Weise aus datenschutzrechtlicher Sicht missbraucht wurden.

KLARE VERANTWORTLICHKEITEN

Trotzdem zeigte sich Verbesserungsbedarf bei den IT-Systemen im Personalbereich. Daher einigten sich alle Beteiligten auf Vorschlag der Wirtschaftsprüfer darauf, fünf konkrete Maßnahmen anzugehen und umzusetzen. So haben die Fach- und IT-Abteilung gemeinsam mit dem Datenschutz klare Verantwortlichkeiten für alle HR-Systeme vereinbart, die in einer Konzernrichtlinie festgelegt werden. Jeweils zwei Vertreter der Fach- und IT-Seite kontrollieren nach dem Vieraugenprinzip sämtliche Maßnahmen bezüglich der Systeme und verantworten die weitere Entwicklung.

Ein weiterer wichtiger Schritt ist die enge Verzahnung der verschiedenen Audits der Bereiche IT-Security, Revision und Datenschutz. So sollen künftig Prüfer Auffälligkeiten, die beispielsweise die Revision feststellt, an den Datenschutz weitergeben, damit eine datenschutzrechtliche Prüfung erfolgen kann. Weitere Maßnahmen rund um die HR-Systeme sind: exakte Dokumentation der Konzepte und Vereinbarungen sowie Abgleich von Betriebsvereinbarungen und Datenschutzkonzepten. Und schließlich wird der Datenschutz ein spezielles Schulungs- und Sensibilisierungsprogramm für Führungskräfte und Nutzer von Personalsoftware aufsetzen.

PERSONALSOFTWARE AUS DER CLOUD

Die Telekom setzt für die Personalwirtschaft bereits seit vielen Jahren auf eine HR Management Software von SAP. Nun erweitert sie in einem internationalen Großprojekt die bestehenden Module um eine Cloud-Lösung von SAP – und musste dafür datenschutzkonforme Anpassungen vornehmen.

Die Vorteile von Software-as-a-Service-Lösungen sind bekannt: geringe Anfangsinvestitionen, Nutzen nach Bedarf und Bezahlen nach Verbrauch. Doch viele Unternehmen scheuen Cloud-Lösungen, besonders wenn sie personenbezogene Daten verarbeiten müssen. Das gilt ganz besonders für den Personalbereich.

Daher war der Konzerndatenschutz der Telekom von Beginn an involviert, die Personalfachabteilung bei der Einführung einer ergänzenden Software-as-a-Service-Lösung für den Personalbereich zu begleiten. Zwei wesentliche Anforderungen galt es zu prüfen: Wo müssen die personenbezogenen Daten gespeichert und verarbeitet werden? Bildet die Standardlösung aus der Cloud die unterschiedlichen Datenschutzanforderungen aus den zahlreichen internationalen Telekom Standorten ab? Herausgestellt hat sich, dass ein Telekom Rechenzentrum in Deutschland für das Hosting der HR-Cloud alle Datenschutzanforderungen erfüllt. Auch die personenbezogenen Daten aus anderen Staaten dürfen laut den länderspezifischen Datenschutzgesetzen in einem deutschen Rechenzentrum verarbeitet werden. Der Konzerndatenschutz hat dafür die Verträge zur Auftragsdatenverarbeitung eingehend geprüft und wo notwendig angepasst.

HOSTING IN DEUTSCHLAND

Schwieriger gestaltete sich das Anpassen der Software selbst. Cloud-Lösungen ziehen ihre Stärke unter anderem daraus, dass sie weitgehend standardisiert sind und Sonderwünsche der unterschiedlichen Nutzer nicht unbedingt erfüllt werden können. Es gibt nur begrenzte Möglichkeiten, die Lösung individuellen Anforderungen anzupassen. Diese wurden vom Projekt in Absprache mit dem Datenschutz geplant und von T-Systems umgesetzt. So variieren unter anderem die Löschfristen von Daten, da sie länderspezifisch sind. Die unterschiedliche Datenschutzgesetzgebung lässt wenig Spielraum für Kompromisse.

Daher wird SAP auf Basis eines ausführlichen Datenschutzkonzepts länderspezifische Anforderungen umsetzen. Seit Mitte 2014 rollt die Telekom nun die neue SAP SuccessFactors Business Execution Suite (BizX) Schritt für Schritt in allen Ländergesellschaften aus. Den Anfang machten unter anderem Deutschland und Polen.

PRIVACY BY DESIGN

Datenschutzaspekte schon frühzeitig in der Entwicklungsphase eines Produkts einbringen: Mit diesem Ziel haben die Datenschützer der Telekom das Privacy-and-Security-Assessment-Verfahren (PSA) um eine frühzeitige Projektberatung mit zusätzlichen Kontrollelementen ergänzt.

Es ist wie in jedem Entwicklungsprojekt: Wenn Fehler erst spät – kurz vor der Inbetriebnahme – entdeckt werden, wird es zeitaufwendig und teuer, sie zu bereinigen. Das gilt auch für den Datenschutz und die Datensicherheit. Daher beginnen die Datenschützer der Telekom ihre Beratungsleistung seit 2014 in einer noch früheren Phase eines Projekts. „Wir gehen frühzeitig proaktiv auf unsere Kunden zu“, erklärt Jan Lichtenberg, der das Konzept mitentwickelt hat. „Sie nehmen unsere Beratungsleistung gern an. So konnten wir schon im ersten Jahr vielfach Projekte mit unserer neuen Arbeitsweise begleiten und haben den Projektleitern sicher Kosten gespart.“

STANDARDCHECKLISTE

Für das neue Erstberatungsgespräch hat das Datenschutzteam eine Standardcheckliste entwickelt, mit der sich die Basisvorgaben einheitlich prüfen lassen. In den Beratungsgesprächen werden dann projektspezifische Anforderungen herausgearbeitet (Rahmenvorgaben), die über die Standardanforderungen hinausgehen. In anschließenden Fokus-Audits können sich dann die Datenschützer und Projektleiter auf kritische Datenschutzaspekte eines Entwicklungsprojekts konzentrieren. „So konnten wir schon in verschiedenen Projekten frühzeitig den Umfang der Verarbeitung personenbezogener Daten reduzieren und direkt wirksame Anonymisierungsverfahren implementieren“, erklärt Lichtenberg. Die Datenschützer konzentrieren sich jetzt weniger auf die Prüfung der Dokumentation, sondern führten vor Ort oder per Webmeeting einen Systemcheck durch. Lichtenberg: „Weg vom Papier, hin zum Realitätscheck und nach der Inbetriebnahme mit weiteren Fokus-Audits den Datenschutz praktisch kontrollieren.“

MAUTSYSTEM FÜR BELGIEN

Satellic NV hat im Juli 2014 den Zuschlag für den Aufbau eines satellitengestützten Mautsystems erhalten. Vertragspartner von Satellic ist auf belgischer Seite Viapass, eine eigens für das Mautprojekt gegründete Behörde.

Bereits im Rahmen der Einführung des Mautsystems in Deutschland spielten Datenschutzfragen eine wichtige Rolle. Datenschützer befürchteten, dass mit automatisch erfassten Mautdaten Bewegungsprofile von Fahrern erstellt werden

könnten. In Deutschland hat der damalige Bundesbeauftragte für den Datenschutz das Lkw-Mautsystem von Toll Collect, an der auch die Telekom beteiligt ist, geprüft und freigegeben. Damals wurde bereits als Bestandteil der Ausschreibung ein Datenschutz- und Sicherheitskonzept erarbeitet, das später fortgeschrieben und konkretisiert wurde. Die Erlaubnis zur Datenverarbeitung ergibt sich für das deutsche Mautsystem primär aus dem Bundesfernstraßenmautgesetz und der Lkw-Maut-Verordnung. Die Daten werden vom Betreiber streng und gemäß den datenschutzrechtlichen Vorgaben

TELEKOM FÜHRT KONZERNRICHTLINIE DATENSCHUTZ WELTWEIT EIN

21 EU-Mitgliedstaaten haben die von der Telekom neu entwickelte Konzernrichtlinie Datenschutz genehmigt. Seit Juli 2014 läuft die Einführung in allen Landesgesellschaften. Telekom Kunden und Mitarbeiter werden von einem weltweit einheitlichen Schutzniveau profitieren, das in vollem Einklang mit europäischem Recht steht.

Im Mai 2014 wurde die neue Konzernrichtlinie Datenschutz von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) genehmigt. Zuvor hatte die BfDI die Richtlinie mit 21 am Verfahren teilnehmenden europäischen Aufsichtsbehörden abgestimmt. Die Deutsche Telekom ist das erste Telekommunikationsunternehmen, welches das europaweite Genehmigungsverfahren erfolgreich abgeschlossen hat.

Die Konzernrichtlinie Datenschutz löst den Privacy Code of Conduct aus dem Jahr 2004 ab. Die neue Richtlinie – auch Binding Corporate Rules Privacy (BCRP) genannt – regelt, wie personenbezogene Daten innerhalb der Telekom Gruppe erhoben, gespeichert und weiterverarbeitet werden dürfen. Die BCRP sind eine gesetzliche Voraussetzung für den weltweiten Datenaustausch innerhalb der Telekom Gruppe. Sie enthalten alle nach EU-Recht geltenden Anforderungen an den Schutz personenbezogener Daten und gehen teilweise sogar darüber hinaus.

Auf diese Weise stellen die BCRP die Datentransfers mit Nicht-EU-Ländern auf ein rechtssicheres Fundament. Sie bestätigen, dass innerhalb der Telekom

ausschließlich für die gesetzlich vorgesehenen Zwecke der Mauterhebung verarbeitet. In Belgien nimmt Satellic eine andere Rolle bei der Erfassung der Mautdaten ein. Sie ist ausschließlich für den Aufbau und Betrieb der Lösung zuständig. Die Verarbeitung der Daten verantwortet der belgische Staat allein. Mit den Modulen der Satellic Telematic Platform lassen sich die Daten der Straßenbenutzung automatisch erfassen und die Gebühren abrechnen. Die On-Board-Unit (OBU) erfüllt Datenschutzanforderungen, da sie nur die für die Mautabrechnung relevanten Daten überträgt. Die personenbezogenen Bewegungsdaten verbleiben in der OBU. In Belgien sollen voraussichtlich ab 2016 einheimische und ausländische Lkws Maut entrichten.

Gruppe ein angemessenes Datenschutzniveau besteht. Zusätzlich zu den Kunden profitiert davon auch das Unternehmen selbst: Nach Maßgabe der Binding Corporate Rules Privacy werden die europäischen Landesgesellschaften personenbezogene Daten an ausländische Schwesterunternehmen übermitteln können, ohne entsprechende Einzelfallgenehmigungen bei ihren nationalen Aufsichtsbehörden einholen zu müssen. Auf dieser Grundlage kann die Telekom in kürzerer Zeit internationale Geschäftsmodelle entwickeln und datenschutzkonform umsetzen.

Der konzernweite Datenschutzgipfel der Telekom mit Datenschutz-Vorstand Dr. Thomas Kremer fand 2014 in Berlin statt.

GLOBAL PRIVACY SUMMIT – DER KONZERNWEITE DATENSCHUTZGIPFEL

Ende August kamen Mitarbeiter aus fünf Kontinenten zum ersten konzernweiten Datenschutzgipfel nach Berlin. Ziel des zweitägigen Spitzentreffens: das grenzüberschreitende Verständnis für die Anforderungen stärken, denen sich die Datenschützer der Telekom weltweit stellen müssen.

Sie waren aus Südafrika angereist, aus den Vereinigten Staaten, aus Singapur und 20 weiteren Ländern – die 90 Datenschutzbeauftragten und -verantwortlichen der Telekom Gruppe. Den Sinn und Zweck des Gipfels brachte Gastgeber Dr. Claus-Dieter Ulmer gleich zu Beginn auf den Punkt. In seiner Begrüßung sprach sich der Konzerndatenschutzbeauftragte dafür aus, die stark steigende Bedeutung des Datenschutzes zu nutzen, um länderübergreifend noch enger zusammenzuarbeiten.

In zahlreichen Workshops und Paneldiskussionen waren sich die Teilnehmer darin einig, dass der Schlüssel zu einer erfolgreichen Kooperation im wechselseitigen Verständnis der Datenschutzanforderungen liegt, die in den Ländern bestehen, in denen die Telekom tätig ist. Das Rüstzeug hierfür liegt vor, so zum Beispiel die einheitlichen Rollendefinitionen für die Datenschutzbeauftragten oder die neue Konzernrichtlinie Datenschutz (Binding Corporate Rules Privacy), die seit Juli 2014 weltweit eingeführt wird.

Zudem gibt es bereits eine Reihe von Projekten, die zeigen, wie eine enge internationale Zusammenarbeit in der Praxis funktioniert. Im Kern kommt es darauf an, die Kollegen aus Produktentwicklung, Vertrieb, Systemintegration und Betrieb von Anfang an aktiv zu begleiten. Auf diese Weise ist der Datenschutz integraler Bestandteil der Marke Telekom.

ALTERNATIVEN ZU GOOGLE, FACEBOOK UND CO.

Die NSA-Bespitzelungsaffäre hinterlässt in Unternehmen und Politik deutliche Spuren: Fast zwei Drittel der Führungskräfte halten den Aufbau von europäischen Alternativen zu den großen amerikanischen Internet- und IT-Unternehmen für geboten.

So lautet das Ergebnis einer repräsentativen Befragung von Abgeordneten sowie Topführungskräften in mittleren und großen Unternehmen, durchgeführt im Sommer 2014 vom Institut für Demoskopie Allensbach im Auftrag der Deutschen Telekom. Das Meinungsbild vor und nach dem NSA-Skandal hat sich vollständig umgekehrt. Noch vor zwei Jahren waren die meisten Führungskräfte der Meinung, Europa bräuchte keine Gegenspieler zu den außereuropäischen Technologiegiganten. Fast zwei Drittel der 621 befragten Topentscheider wünschen sich sogar ein innereuropäisches Internet, halten dies jedoch für nicht realisierbar.

Fast zwei Drittel der Topentscheider wünschen sich ein innereuropäisches Internet

Der Cyber Security Report 2014 zeigt zudem, dass IT-Angriffe auf deutsche Unternehmen weiter gestiegen sind. Neun von zehn Firmen haben 2014 Angriffe von außen registriert – 14 Prozent täglich, 18 Prozent einmal oder mehrmals in der Woche. Trotzdem fühlen sich nur noch 39 Prozent der Führungskräfte aus Großunternehmen durch Hackerangriffe stark oder sehr stark bedroht. 2013 waren es noch 53 Prozent.

ANGRIFFE ANSTEIGEND, ANGST ABNEHMEND

60 Prozent der Unternehmen sehen sich gut gegen IT-Gefahren geschützt. Diese Aussage überrascht, denn gleichzeitig sind vier von fünf Führungskräften davon überzeugt, dass IT-Angriffe jedes Jahr einen großen volkswirtschaftlichen Schaden verursachen. Und 69 Prozent der befragten Entscheider aus mittleren und großen Unternehmen sehen die Gewährleistung von IT-Sicherheit als erfolgskritischen Faktor für das eigene Geschäft – direkt hinter den Klassikern Kundennähe und Kosteneffizienz.

Daher tauschen sich fast drei Viertel der Unternehmen als Teil einer globalen Wertschöpfungskette mehr oder weniger regelmäßig mit Zulieferern oder Partnern über Fragen der IT-Sicherheit aus. Fragen der IT-Sicherheit stehen besonders dann regelmäßig auf der Agenda, wenn die Unternehmen Daten untereinander weitgehend automatisiert austauschen, wie es durch den Megatrend Industrie 4.0 mehr und mehr der Fall sein wird.

90 Prozent der Internetnutzer haben kein gutes Gefühl, wenn sie im Internet Kreditkartendaten eingeben sollen

GROSSE ANGST VOR CYBERRISIKEN

Datenbetrug im Internet, Missbrauch persönlicher Daten durch Unternehmen, Computerviren und Missbrauch persönlicher Daten durch andere Nutzer in sozialen Netzwerken: Diese Cyberrisiken steigen laut Sicherheitsreport 2014 weiter an.

Im Auftrag der Telekom hatte das Institut für Demoskopie Allensbach im Frühjahr 2014 einen repräsentativen Querschnitt der Bevölkerung ab 16 Jahren befragt. Machten sich 2013 noch 44 Prozent der Bevölkerung und 47 Prozent der Internetnutzer große Sorgen bezüglich Risiken im Zusammenhang mit dem Internet, sind es aktuell 47 Prozent der Bürger und 54 Prozent der Internetnutzer, die sich hinsichtlich mindestens eines der Cyberrisiken große Sorgen machen. Jeweils 74 Prozent, also knapp drei Viertel aller Bürger, gehen von einer Zunahme dieser Risiken aus.

59 Prozent der Internetnutzer haben ein ungutes Gefühl, wenn sie im Internet – zum Beispiel bei der Bestellung in Onlineshops, bei E-Mail-Anbietern oder sozialen Netzwerken – aufgefordert werden, persönliche Daten anzugeben. Nur 26 Prozent haben damit grundsätzlich kein Problem. Zwischen den Altersgruppen gibt es dabei erhebliche Unterschiede. Je jünger die Internetnutzer sind, desto mehr reduzieren sich die Vorbehalte.

SKEPSIS BEI EINGABE VON BANKDATEN

Nicht alle Daten sind aus Sicht der Internetnutzer in gleichem Maß sensibel. Als besonders kritisch gelten Kreditkartennummer und Bankverbindung, bei denen über 90 Prozent der Internetnutzer ein ungutes Gefühl haben, wenn sie im Internet diese Daten eingeben sollen. Bei mehr als zwei Dritteln der Internetnutzer besteht Skepsis, wenn sie Kontaktdaten in Form von Telefonnummer oder genauer Adresse mit Straßenanschrift eingeben sollen. Als weniger sensibel stufen die Befragten die eigene E-Mail-Adresse ein.

Trotz der Skepsis lesen gerade einmal 17 Prozent der Internetnutzer Datenschutzbestimmungen von Onlineshops oder anderen Angeboten im Internet, 26 Prozent zumindest ab und zu. Die Begründung: Datenschutzbestimmungen sind zu ausführlich und damit zu mühsam zu lesen. 55 Prozent führen an, dass sie in der Regel so kompliziert sind, dass man sie ohnehin nicht verstehe. Jeder Dritte ist der Ansicht, dass diese häufig versteckt platziert und deshalb nicht auf Anhieb zu finden seien.

JE ÄLTER, DESTO UNVORSICHTIGER

Besonders ältere Nutzer von Computern, Laptops, Tablets oder Smartphones laufen Gefahr, Opfer digitaler Attacken zu werden. Zu diesem Resultat kommt eine Umfrage des Marktforschungsinstituts TNS Emnid im Auftrag der Deutschen Telekom.

An der Mehrheit der Nutzer scheinen Warnungen vor Phishingmails, Spyware, Viren oder Hackerangriffen jedoch nicht spurlos vorbeizugehen. Die meisten der 1.000 Befragten geben an, mindestens eine der gängigsten Sicherheitsvorkehrungen an ihren technischen Geräten vorzunehmen. Dazu zählen vor allem das Verwenden und Aktualisieren von Antivirensoftware, das Verschlüsseln von Daten oder das regelmäßige Ändern von Passwörtern.

Zwölf Prozent der Befragten verzichten allerdings komplett auf die Sicherung ihrer Daten und Endgeräte. Bei Nutzern ab 50 Jahren sind es 22 Prozent und bei den über 60-Jährigen ist es fast jeder Dritte. 36 Prozent der Befragten schätzen ihr Wissen als schlecht bis sehr schlecht ein. Von diesen 36 Prozent treffen 30 Prozent ebenfalls keine Sicherheitsmaßnahmen.

HILFE VON FREUNDEN UND FAMILIE

Die Zahlen korrespondieren mit der Einschätzung der eigenen IT-Kenntnisse der Befragten. Je älter die Nutzer, desto schlechter schätzen sie das eigene Wissen ein: 39 Prozent der 50- bis 59-Jährigen und zwei Drittel der über 60-Jährigen halten ihre IT-Kenntnisse für schlecht oder sehr schlecht, bei den 14- bis 29-Jährigen sind es nur 14 Prozent.

Wenn das eigene Know-how zur Lösung von technischen Problemen nicht ausreicht, greifen fast zwei Drittel der Nutzer auf Freunde, Bekannte oder Familienmitglieder zurück. 23 Prozent nehmen aber auch kostenpflichtige Dienstleistungen von IT-Fachleuten in Anspruch. Die Gründe dafür sind unterschiedlich: Für die meisten steht das Vertrauen in das Expertenwissen im Vordergrund. Häufig ist aber auch ausschlaggebend, dass ein Fachmann das Problem wesentlich schneller löst als man selbst.

Fast jeder Dritte der über 60-Jährigen verzichtet komplett auf die Sicherung von Daten und Endgeräten

TELEKOM BROWSER MIT VIRENSUCHFUNKTION

Eine Million Mal wurde der Telekom Internet Browser 7 bisher heruntergeladen. Um es Hackern so schwer wie möglich zu machen, verfügt er seit November 2014 über eine in Deutschland bisher einzigartige Sicherheitsfunktion.

Während Sicherheitsoptionen bei vielen Browsern oft in den komplizierten und schwer verständlichen Submenüs der Internetoptionen vergraben liegen, finden Nutzer des Telekom Browsers ihre Sicherheitsoptionen gut sichtbar in der Symbolleiste. Ein Klick auf den Button „Sicherheit“ öffnet eine Liste, die es ermöglicht, Cookies und Verlaufslisten schnell zu löschen sowie den Stand der persönlichen Anschlusssicherheit zu prüfen. Eine Infoseite weist den Nutzer automatisch darauf hin, dass der Internetzugang akut missbräuchlich genutzt wird, und empfiehlt die weitere Vorgehensweise, beispielsweise das Ändern aller Passwörter oder die Installation eines Sicherheitspakets. So vermeiden Nutzer, dass ein Virus oder Trojaner unbemerkt auf ihrem Computer bleibt und Schaden anrichtet.

BLOCKINGLISTE FÜR UNERWÜNSCHTE WEBSITES

Ausgewählte Websites öffnet der Browser automatisch in einer privaten Sitzung und verhindert so die Aufzeichnung von Surfspuren. Außerdem bietet der Browser eine Blockingliste für Websites. Damit lässt sich verhindern, dass der Browser unerwünschte Websites aufruft. Darüber hinaus können Nutzer auch Wildcards für diese Blockingliste einsetzen. Dies unterbindet den Aufruf von Websites mit bestimmten Inhalten, ohne die genaue Adresse der betreffenden Seiten zu kennen.

Die Informationen für das neue Feature stammen vom www.sicherheitstacho.eu der Telekom. Ausführliche Daten und Statistiken zu aktuellen Cyberangriffen sind über dieses Onlinetool einsehbar. Weltweit mehr als 180 Sensoren, sogenannte Honeypots, zeigen auf einer digitalen Weltkarte die Herkunft der Cyberangriffe an.

Der Browser 7 der Telekom basiert auf dem Firefox-Browser der Mozilla-Stiftung und steht zum kostenlosen Download zur Verfügung: **www.t-online.de/browser**

DATENSCHUTZFREUNDLICHE SMARTPHONES

Personenbezogene Daten auf Handys zu schützen ist eine Kunst. Wirksame Einstellungen sind rar und ohne Hintergrundwissen nur schwer zu durchschauen. Mozilla und die Telekom wollen dies ändern. Ab 2015 statten sie Firefox-Handys mit Schutzmechanismen aus, die auch für Normalnutzer leicht zu bedienen sind.

Wenn es darum geht, Handynutzern Mittel an die Hand zu geben, um ihre persönlichen Daten zu schützen, üben sich die marktführenden Betriebssysteme in Zurückhaltung. Einstellungen für den Datenschutz sind als solche kaum erkennbar und greifen angesichts der wachsenden Bedrohungen nur selten weit genug. Das Handybetriebssystem Firefox OS bildet derzeit die einzige Ausnahme. Sein Urheber, die Open-Source-Organisation Mozilla, bietet den Nutzern eine Reihe von Möglichkeiten, um externe Zugriffe auf die Dienste und Daten ihrer Handys zu kontrollieren.

MEHR DATENHOHEIT FÜR NUTZER

In enger Zusammenarbeit mit der Telekom wird Mozilla dieses Angebot noch einmal deutlich erweitern. Auf dem Mobile World Congress 2014 in Barcelona präsentierten die beiden Entwicklungspartner einen ersten Prototyp. Messebesucher hatten Gelegenheit, im Mobilfunkmarkt bislang noch völlig einzigartige Datenschutzeinstellungen kennenzulernen. Beispielsweise erlaubt es die Funktion Ortungsgenauigkeit (Location Accuracy), zu entscheiden, wie exakt eine App den aktuellen Standort eines Smartphones ermitteln darf. Somit lässt sich zum Beispiel die Übermittlung der GPS-Daten auf die Navigations-App beschränken. Die Wetter-App wiederum erhält nur die Koordinaten der Stadt, in der sich der Handynutzer gerade aufhält.

Deutlich mehr Datenhoheit bietet auch die neu entwickelte Fernschutzfunktion (Remote Privacy Protection). Im Gegensatz zu den Lösungen aller anderen Betriebssysteme verzichtet Firefox darauf, die Ortsdaten der Smartphones an eine zentrale Stelle zu schicken, an die sich der Handynutzer im Verlustfall dann wendet. Stattdessen wird auf dem Firefox-Smartphone ein Lokalisierungspasswort hinterlegt. Schickt man das Passwort per SMS an das abhandengekommene Handy, antwortet dieses ebenfalls per SMS mit seinen Positionsdaten.

Mozilla wird die gemeinsam mit der Telekom entwickelten Datenschutzfunktionen ab 2015 schrittweise an den Markt bringen. Darunter wird dann auch die sogenannte Permission History sein, die Benutzer darüber aufklärt, welche Apps auf welche Daten und Dienste ihres Handys zugreifen. Die neue Funktion dient als Hilfe, um die Zugriffsrechte allzu datenhungriger Apps zu erkennen und einzuschränken.

BRANCHENWEITER ERFAHRUNGSAUSTAUSCH NIMMT ZU

Um den Datenschutz auf allen Smartphones zu verbessern, engagiert sich die Telekom in einem branchenweiten Erfahrungsaustausch. Zusammen mit dem World Wide Web Consortium (W3C) veranstaltete die Telekom einen internationalen Workshop zum Thema. Ende November kamen in Berlin hochrangige Datenschutzexperten fast aller Betriebssystemanbieter sowie Vertreter von Universitäten und Nichtregierungsorganisationen zusammen. Eines der wesentlichen Ziele des Workshops bestand darin, die Erfahrungen aus der Entwicklungspartnerschaft zu teilen. In der Privacy Interest Group des W3C wird die Diskussion weiter fortgesetzt.

SICHERHEITSLÜCKE IM MOBILFUNKNETZ GESCHLOSSEN

Ein Team von Berliner Sicherheitsforschern hat im Dezember 2014 Sicherheitslücken im SS7-Protokoll aufgedeckt. Diese Lücke erlaubt das Abhören von Verbindungen über das UMTS- und GSM-Netz. Betroffen sind weltweit alle Netzbetreiber. Die Telekom hat die Sicherheitslücke sofort geschlossen.

Die Telekom hatte bereits in den Monaten zuvor verschiedene Maßnahmen umgesetzt, um Angriffe gegen ihre Kunden im Rahmen der SS7-Problematik weiter einzuschränken. Nach Bekanntwerden des Risikos hat die Telekom zusätzliche Sicherheitsmaßnahmen ergriffen und die Umsetzung beschleunigt. Darüber hinaus sucht die Telekom den engen Austausch mit externen Fachleuten wie dem Chaos Computer Club (CCC).

Ein Mobilfunkexperte des CCC zeigte auf dem Jahreskongress des Chaos Computer Clubs, wie Angreifer eine Funktion des SS7-Protokolls nutzen können, mit der sie Anrufe umleiten. Ein Telefonat wird dann im Hintergrund an ihn weitergeleitet, bevor es an das ursprüngliche Ziel weitergeschickt wird. Mit dem zuvor von den Sicherheitsexperten aufgezeigten Szenario können Hacker die Verschlüsselung innerhalb des Netzes überwinden und so Telefonate mithören und SMS mitlesen. Die notwendigen Informationen zum Entschlüsseln von Nachrichten werden über SS7 ausgetauscht. Das gezielte Ausspionieren von Einzelpersonen ist nur mit einem hohen Expertenwissen und krimineller Energie möglich. So muss sich der Täter in der Nähe des Opfers aufhalten oder wissen, wo dieses sich aufhält. Weiterhin benötigt das Abhören spezielle technische Vorrichtungen, die nicht am Markt erhältlich sind.

Die Maßnahmen der Netzbetreiber sind allerdings nur eine vorübergehende Lösung, da ein dauerhaftes Beheben solcher Risiken nur die gesamte Industrie entwickeln kann. Dazu gehören Netzbetreiber, die Hersteller von Netzinfrastruktur und Endgeräten, die Branchenverbände und die Standardisierungsgremien wie ETSI und die GSMA.

SPIONAGESCHUTZ FÜR JEDES SMARTPHONE

Mit der Mobile Encryption App verschlüsselt die Telekom Voice-over-IP-basierte Telefonate und Kurznachrichten auf jedem Android- und iOS-Smartphone – weltweit sowie netz- und geräteunabhängig.

Die Verschlüsselungslösung der Telekom in Kooperation mit dem Entwicklungspartner GSMK ermöglicht abhörsichere Telefonie auf jedem handelsüblichen Smartphone mit Android- oder iOS-Betriebssystem. Im Gegensatz zu anderen Lösungen funktioniert sie in jedem Telefonnetz und sogar ohne SIM-Karte über WLAN oder eine Satellitenverbindung. Sie ermöglicht sogar verschlüsselte Kommunikation in Ländern, in denen die Internettelefonie blockiert wird.

Da die App mit 4,8 Kilobit pro Sekunde Datendurchsatz äußerst geringe Anforderungen an die Bandbreite stellt, eignet sie sich außerdem für den Einsatz in Gebieten mit schlechter Netzabdeckung. Sie funktioniert etwa auch in GSM-Netzen in Entwicklungsländern. Beide Gesprächspartner müssen die App auf ihrem Gerät installiert haben. Sie müssen jedoch nicht Kunden desselben Mobilfunkanbieters sein. Weitere Software oder Systeme sind nicht erforderlich, um die Applikation nutzen zu können.

SCHÜTZT GEHEIMNISSE

Die Anwendungsgebiete der Lösung sind vielfältig. Sie ermöglicht etwa geheime Vertragsverhandlungen, vertrauliche Diskussionen über Unternehmenszusammenschlüsse, Informationsaustausch zu Forschung und Entwicklung oder kann bei Zeugenschutzprogrammen zum Einsatz kommen. Die Schlüssel für sichere Kommunikation werden auf den eingesetzten Smartphones selbst generiert und nach Gesprächsende gelöscht. Damit bleiben sie in der Hand des Nutzers und verhindern, dass sich Dritte per „Man-in-the-Middle-Attacke“ in eine Kommunikation einschalten, um zu spionieren. Kontaktdaten, Nachrichten und Texte in der App werden in einem sicheren Container verschlüsselt und separat auf dem Smartphone gespeichert. Um die vertraulichen Informationen zu lesen, muss der Nutzer ein Passwort eingeben.

Die Telekom hat sich bewusst entschieden, ein möglichst flexibles Produkt anzubieten, das insbesondere für internationale Kunden interessant ist. Zunächst als Lösung für größere Unternehmen gedacht, soll die App mittelfristig auch Privatkunden und kleineren Unternehmen abhörsichere Kommunikation zugänglich machen.

BOTNETZ: SOFORTHILFE NACH INFEKTION MIT ANDROID-VIRUS

60 Mobilfunkkunden der Telekom waren Anfang 2014 Teil eines Botnetzes, das spanische Ermittlungsbehörden aufgedeckt hatten. In einer telefonischen Blitzaktion klärte die Telekom ihre Kunden darüber auf, wie sie den Missbrauch ihrer Smartphones wirksam stoppen können.

Ein Botnetz ist ein illegal betriebenes Netzwerk, das internetfähige Rechner ohne das Wissen der Nutzer übernimmt. Hierzu installiert das Botnetz einen entsprechend programmierten Schadcode auf den Zielrechnern. Aufgrund ihrer hohen Leistungsfähigkeit geraten auch immer mehr Smartphones in das Visier der Angreifer. Endgeräte mit dem Betriebssystem Android sind das mit Abstand beliebteste mobile Angriffsziel. Sobald Smartphones in ein Botnetz eingebunden sind, lassen sie sich über den Command-and-Control-Server des Netzes fernsteuern. Beispielsweise kann der Server dann sämtliche Zugangsdaten der Nutzer ausspähen.

Im Januar 2014 informierte die Bundesnetzagentur die Telekom über einen laufenden Angriff. Spanische Behörden hatten gegen ein Android-Botnetz ermittelt und waren unter anderem auch auf die Daten von deutschen Mobilfunkkunden der Telekom gestoßen. Um den insgesamt 60 Kunden schnellstmöglich zu helfen, nahm das Serviceteam Konzerndatenschutz seine Arbeit auf.

In einer Blitzaktion riefen die Servicemitarbeiter alle betroffenen Kunden an. Wen sie nicht direkt erreichen konnten, dem schickten sie eine SMS mit der Bitte um Rückruf. In den anschließenden Beratungsgesprächen bekamen die Kunden eine Schritt-für-Schritt-Anleitung, wie sie die Schadsoftware von ihren Handys vollständig entfernen können. Zudem empfahl der Konzerndatenschutz den Kunden, eine Antivirensoftware zu installieren, um einer jederzeit möglichen Neuinfektion wirksam vorzubeugen.

KEIN TRACKING

Wissenschaftler haben im Sommer 2014 eine neue, hartnäckige Trackingtechnologie namens Canvas Fingerprinting nachgewiesen.

Sie hatten zuvor rund 100.000 Websites auf die Trackingmethode untersucht. Auch T-Online.de war vorübergehend betroffen. Mit Canvas Fingerprinting können Unternehmen über Cookies nachverfolgen, welche Internetseiten ein Nutzer besucht – ohne dass er das verhindern kann. Dies widerspricht den datenschutzrechtlichen Anforderungen der Telekom. Zudem ist das Verfahren nicht mit dem deutschen und europäischen Datenschutzrecht vereinbar.

Websitetracking ohne Zustimmung der Nutzer ist nicht datenschutzkonform.

Ein Dienstleister hatte das Tracking ohne Wissen der Telekom auf T-Online.de eingesetzt. Es seien keine personenbezogenen Daten erhoben worden, versicherte der Dienstleister. Dennoch war der Vorfall ein Vertrauensbruch. T-Online.de hat daraufhin die Zusammenarbeit direkt ausgesetzt. Eine effektive Methode, sich vor solchen Techniken zu schützen, wäre JavaScript abzuschalten. Aber dann würde quasi keine Seite aus dem Internet mehr richtig angezeigt werden. Die Telekom arbeitet derzeit an einer Lösung, zukünftig den unzulässigen Einsatz von Canvas Fingerprint auf eigenen Portalen zu erkennen und für die Einhaltung der Konzernvorgaben zu sorgen.

GLOBALE HERAUSFORDERUNGEN

Die Enthüllungen von Edward Snowden haben im Sommer 2013 ein Erdbeben in der digitalen Industrie ausgelöst, dessen Auswirkungen weiterhin zu spüren sind. Aber manchmal vergessen wir, dass auch die Cyberkriminalität immer weiter wächst. Beide Themen bedrohen die digitale Industrie.

Herr Petri, wie fällt Ihre Bestandsaufnahme zur globalen Sicherheitslage aus?
Axel Petri: Die geopolitischen Krisen in unserer Welt nehmen leider weiter stetig zu. Das hat auch erhebliche Auswirkungen auf die digitale Welt. Ließ sich die Diskussion um die Balance von kollektiver Sicherheit und individueller Freiheit im letzten Jahr noch relativ unbelastet führen, hat sich dies durch die neueren Entwicklungen zum Beispiel in der Ukraine oder um den „Islamischen Staat“ und nicht zuletzt natürlich die schrecklichen Ereignisse in Paris doch verändert.

Wie ist denn Ihre Sicht auf die Diskussion um die Sicherheit im Netz?
Axel Petri: Ich glaube, wir stehen hier einem Paradoxon gegenüber: Der völlige Verzicht auf (rechts-)staatliche Überwachung im Netz ist eine Wunschvorstellung, gerade angesichts der vielen Krisen in der Welt und der geopolitischen Sicherheitslage. Genauso stellt eine hundertprozentige und allumfassende Sicherheit in der digitalen Welt eine Illusion dar. Wir müssen lernen, mit dieser neuen Unsicherheit zu leben. Nichtsdestotrotz wird die Telekom weiter unermüdlich an der Sicherheit ihrer Netzte und Dienste arbeiten. Dabei gibt es keine „Silver Bullet“, die alle Herausforderungen auf einen Schlag löst. Wir werden weiter Schritt für Schritt vorgehen und den sprichwörtlichen Elefanten in Scheiben schneiden müssen.

Warum muss die Telekom kontinuierlich an der Sicherheit ihrer Netze und Dienste arbeiten?
Axel Petri: Die Bedrohungslage im Cyberraum verschärft sich. Auf der einen Seite stehen finanziell motivierte Hacker, die es auf Unternehmens- und Kundendaten abgesehen haben, auf der anderen Seite gibt es politisch angetriebene Hacktivisten und Cyberterroristen, die vor Sabotage nicht zurückschrecken und finanziellen oder materiellen Schaden anrichten wollen. Und auch Geheimdienste stellen eine Bedrohung dar, wenn es um die schützenswerten Daten unserer Kunden geht.

Was kann die Telekom gegen die Bedrohungen tun?
Axel Petri: Als international engagierter Netzbetreiber ist es unsere Aufgabe, derartige Bedrohungen abzuwehren, um die Kommunikation und die Daten unserer Kunden zu schützen. Der Verbraucher erwartet das von uns und schenkt uns viel Vertrauen. Aus dem Sicherheitsreport 2014, einer repräsentativen Befragung der Bevölkerung durch das Institut Allensbach, geht hervor, dass die Telekom als mit Abstand vertrauenswürdigstes Unternehmen gilt, wenn es um den Umgang mit persönlichen Daten geht. Wir tun alles, um diesen Vertrauensvorsprung zu rechtfertigen.

Mit welchen Mitteln verbessern Sie die Sicherheit Ihrer Kunden?
Axel Petri: Die Umstellung unserer Netze auf die IP-Technologie gilt als ein wichtiger Schritt bei der Verbesserung der Sicherheit. Ein geschlossenes europaweites Datennetz bietet einen höheren Schutz vor Spähangriffen, mehr Verlässlichkeit und ermöglicht vollständige Verschlüsselung der Voice-over-IP-Kommunikation von Festnetz über Mobilfunk. Die analoge Technik hingegen ist veraltet und störanfällig. Darüber hinaus arbeiten wir eng mit Behörden wie der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen, um unsere Kunden zu schützen. Als gesamteuropäischer Telekommunikationsanbieter müssen wir uns dabei mit staatlicher Regulierung und Rechtsprechung der unterschiedlichen Nationalstaaten

FÜR DIE TELEKOMMUNIKATIONSINDUSTRIE

Ein geschlossenes europaweites Datennetz ermöglicht vollständige Verschlüsselung der Voice-over-IP-Kommunikation

auseinandersetzen, die verschiedene rechtliche Rahmenbedingungen bieten. Neben den national voneinander abweichenden Rahmenbedingungen zur Vorratsdatenspeicherung und der national unterschiedlich ausgeprägten Auskunftspflicht gegenüber Behörden ist hier insbesondere das ungleiche Sicherheitsniveau für kritische Infrastrukturen wie Telekommunikationsbetreiber und die IT-Branche zu nennen. Deutschland hebt sich im Feld der europäischen Mitgliedstaaten hinsichtlich der Sicherheit der Netzinfrastruktur und der IT-Netze bereits sehr positiv ab. Die Telekom setzt sich dafür ein, das Sicherheitsniveau in Europa signifikant zu erhöhen.

Was wünschen Sie sich von den europäischen Nationalstaaten?

Axel Petri: Die Staaten sollten sich auf die technischen Neuerungen einstellen und mehr Transparenz zulassen, wenn es um die Zusammenarbeit mit den Behörden geht. Sie müssen die Internationalisierung unterstützen und gemeinsame rechtliche Rahmenbedingungen schaffen, damit die Bürger alle Vorteile paneuropäischer Netze nutzen können. Wir brauchen eine staatenübergreifende Lösung, die es insbesondere Unternehmen, aber auch Behörden und Regierungen ermöglicht, grenzüberschreitend sicher und verschlüsselt miteinander zu kommunizieren. Mit einzelstaatlichen Lösungen und voneinander getrennten Netzen ist das nicht möglich.

Welche Voraussetzungen müssen erfüllt werden?

Axel Petri: Aus Perspektive der Sicherheit ist eine wesentliche Voraussetzung für die erfolgreiche Implementierung paneuropäischer Netze, dass Behörden anerkennen, dass Netzstrukturen zukünftig international und damit grenzüberschreitend beschaffen sein werden. Das dürfte die Arbeit der nationalen Behörden beeinflussen. In der Zusammenarbeit mit den Behörden müssen wir herausstellen, welche gesellschaftlichen und wirtschaftlichen Vorteile internationale Netze im Vergleich zu ausschließlich nationalen Netzen für die einzelnen Staaten und die dort lebenden Nutzer haben werden. Dies bedeutet aber nicht, dass die jeweiligen legitimen nationalen Sicherheitsinteressen depriorisiert werden. Hier werden Wirtschaft und Staat weiter aufeinander zugehen müssen, um Lösungen zu finden. Wir stehen hierfür jederzeit bereit.

KURZ ERKLÄRT

Kritische Infrastrukturen
Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Das Bundesministerium des Inneren gliedert kritische Infrastrukturen in neun Sektoren. Dazu gehören unter anderem Energie, Informationstechnik und Telekommunikation, Transport und Verkehr oder Gesundheit.

ZUR PERSON

Axel Petri

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

WISSEN SCHÜTZEN MIT EIGENER CLOUD

Im Markt für thermoplastische Kunststoffe zählt das Familienunternehmen Ensinger zu den weltweit führenden Anbietern. Um seine 28 Produktions- und Vertriebsstandorte sicher zu vernetzen, hat der Mittelständler eine Cloud-Lösung geschaffen, die getrennt vom öffentlichen Internet arbeitet.

„Neue Werkstoffe spielen eine entscheidende Rolle für den industriellen Fortschritt." Mit diesem Credo hat es Ensinger in fünf Jahrzehnten vom Garagenunternehmen zu einem der weltweit gefragtesten Hersteller von Hochleistungskunststoffen gebracht. Industriekunden zahlreicher Branchen kommen vor allem dann auf den Mittelständler aus Schwaben zu, wenn sie Halbzeuge, Präzisionsbauteile und Profile brauchen, die an die Grenzen des technisch Machbaren gehen sollen. Um den hohen Erwartungen gerecht zu werden, hat Ensinger das Innovationsmanagement ins Zentrum seines Geschäfts gerückt.

KNOW-HOW-SCHUTZ

„Mit unseren Produkten und Fertigungsverfahren differenzieren wir uns von anderen Marktteilnehmern. Know-how-Schutz zählt daher zu den Kernanforderungen meines Aufgabengebiets", erklärt CIO Erwin Schuster, der die Verantwortung für Ensingers IKT-Systeme weltweit trägt. Eine Verantwortung, deren Gewicht von Jahr zu Jahr zunimmt. Hauptgrund ist die weiter fortschreitende Internationalisierung des Unternehmens. Inzwischen ist der Mittelständler in mehr als 20 Ländern rund um den Globus tätig. Entsprechend komplex stellt sich der Grad der Vernetzung dar. Doch damit nicht genug: Zusätzlich zur Internationalisierung steht die IT vor der Herausforderung, Lösungen für neue Arbeitsformen zu schaffen. Aktuell zählen mobiles und kollaboratives Arbeiten sowie die weltweite Steuerung von Produktionsanlagen zu den drängendsten Themen.

Mit jeder neuen Anforderung nimmt die Zahl der potenziellen Einfallstore in die Informations- und Kommunikationssysteme zu. Um die steigende Komplexität sicher managen zu können, hat Ensinger daher eine eigene Cloud-Lösung aufgebaut. Diese sogenannte Private Cloud stützt sich auf drei Rechenzentren, die der Kunststoffverarbeiter an seinen deutschen Produktionsstätten in Cham, Nufringen und Rottenburg-Ergenzingen betreibt. Gemeinsam mit der Telekom hat Ensinger die drei Rechenzentren in einem Weitverkehrsnetzwerk (engl. Wide Area Network, WAN) gekoppelt.

ZWEI ZUGANGSPUNKTE ZUM INTERNET

„Das Entscheidende dabei ist, dass unsere Geschäftsdaten nur noch über die dedizierten Leitungen der Telekom und somit getrennt vom öffentlichen Internet fließen", erläutert IT-Leiter Schuster. „Für die darüber hinausgehende Webkommunikation bietet unsere Cloud exakt zwei Zugangspunkte zum Internet, die wir von den Sicherheitsexperten der Telekom rund um die Uhr schützen lassen." Die Private Cloud befindet sich seit Ende 2014 im Grundbetrieb. Nach und nach bindet Ensinger nun auch seine übrigen Standorte und Landesgesellschaften darin ein. Im Tagesgeschäft sind die IKT-Verantwortlichen fortwährend mit der Frage konfrontiert, wie sich das hohe Schutzniveau aufrechterhalten lässt, ohne die Kommunikationsprozesse über Gebühr einzuschränken. Für Erwin Schuster ist dies ein Spagat, dessen Bedeutung zukünftig noch einmal deutlich zunehmen wird.
Als wesentliche Triebfeder sieht er den sich weiter fortsetzenden Trend zu hochintegrierten Produktions- und Logistiksystemen, die über das Netzwerk kommunizieren. „Ein gutes Beispiel sind unsere Produktionsanlagen. Die kommende Generation dieser Anlagen wird zum Teil über fünf bis sechs Netzwerkports verfügen. Daraus resultieren völlig neue Anforderungen an die technische Vernetzung und Sicherheit, das heißt, die horizontale Integration nimmt zu. Darüber hinaus steigt der Grad der vertikalen Integration aller betrieblichen Anwendungssysteme."

DETAILLIERTES REGELWERK

Um die Interessen der Anwender und der Sicherheitsmanager ins Gleichgewicht zu bringen, hat Ensinger ein detailliertes Regelwerk aufgesetzt. Für jeden einzelnen Anwendungsfall ist präzise festgelegt, wer innerhalb welcher Zeit zu welchem Zweck in die Administration der Firewall eingreifen darf. Die Betriebsverantwortung liegt durchgängig – technisch wie inhaltlich – bei der Telekom. CIO Schuster rät allen Unternehmen, die Ähnliches vorhaben, sich für die Ausarbeitung eines solchen Regelwerks hinreichend Zeit zu nehmen. „In unserem Fall lief die konzeptionelle Arbeit über ein Dreivierteljahr. Zweifellos ein hoher Aufwand, der jedoch absolut sinnvoll ist, wenn man zu einer tragfähigen Lösung kommen will, die den Anforderungen der Sicherheit und des Business gleichermaßen gerecht wird."

SPREU VOM WEIZEN TRENNEN

Das geplante IT-Sicherheitsgesetz soll unter anderem dazu beitragen, besonders gefährdete Infrastrukturen wie Energie- oder Telekommunikationsnetze besser vor Hackerangriffen zu schützen. Die Lebensmittelversorgung soll dazugehören.

Hackerangriffe auf Websites sind alltäglich. Nur noch die spektakulärsten Fälle schaffen es auf die Nachrichtenseite der Medien: Weihnachten 2014 die Onlineplattformen Playstation Network und Xbox Live oder im Januar 2015 die Internetseiten von Angela Merkel und Bundestag. Sind durch Hacker lahmgelegte Internetseiten wie die der Bundeskanzlerin für die Allgemeinheit noch zu verkraften, könnten gehackte IT-Systeme von Energieunternehmen fatale Folgen haben: Ohne Strom würde ein ganzes Land in wenigen Stunden stillstehen. Das Bundesinnenministerium will daher im Rahmen des geplanten IT-Sicherheitsgesetzes kritische Infrastrukturen definieren, die besondere Verpflichtungen in puncto IT-Sicherheit erfüllen müssen. Die Betreiber dieser Infrastrukturen müssen dann IT-Sicherheitsvorfälle zwingend melden und Mindeststandards für die IT-Sicherheit einhalten. Riccardo Sperrle, CIO der Unternehemnsgruppe Tengelmann und des Lebensmittelhändlers Kaiser's Tengelmann, kann nachvollziehen, warum die Lebensmittelsparte zu den kritischen Infrastrukturen zählt. Bezogen auf Ausfälle durch Cyberattacken sei das Risiko eines Versorgungsengpass jedoch geringer als bei kritischen Infrastrukturen: „Auch wir werden wie alle Unternehmen täglich von Hackern angegriffen. Aber bei einem Ausfall unserer IT-Systeme durch einen Hackerangriff sind wir zumindest kurzfristig arbeits- und lieferfähig."

Die Unternehmensgruppe Tengelmann schützt ihre IT-Systeme mit einem aktuellen Information Security Management System

Damit geht der IT-Chef von Tengelmann konform mit dem EHI Retail Institute, das die Gefährdungslage und Sicherheitsstandards des Lebensmittelhandels untersucht hat. Ergebnis: „Die Sicherheitsstandards sind bereits sehr hoch, die Risiken angesichts einer enormen Vielfalt von unterschiedlichen Unternehmenseinheiten und IT-Systemen in dieser Branche überschaubar und die Wahrscheinlichkeit, dass die Versorgung der Bevölkerung durch Cyberattacken auf den Lebensmittelhandel flächendeckend gefährdet wird, ist sehr gering." Allein die große Vielfalt an einzelnen Unternehmenseinheiten führe dazu, dass eine flächendeckende Gefährdung aller Unternehmen durch Cyberattacken sehr unwahrscheinlich sei.

2013 stellte das EHI fest, die Handelsunternehmen hätten in Bezug auf IT-Sicherheit ihre Hausaufgaben gemacht. Die Verantwortlichkeit für IT-Sicherheit sei klar geregelt und alle Unternehmen hätten ein Information Security Management System eingeführt oder befänden sich damit im Aufbau. Ebenso hätten die Unternehmen Risikobeurteilungen für ihre IT durchgeführt und entsprechende Sicherheitskonzepte entwickelt.

Für Tengelmann kann Riccardo Sperrle diese Einschätzung des Handelsinstituts bestätigen. „Wir haben mithilfe von IT-Sicherheitsexperten der Telekom unsere Sicherheit geprüft, und wo notwendig, den aktuellen Angriffsmethoden der Hacker angepasst", erklärt der CIO und empfiehlt anderen Unternehmen, eine wichtige Maßnahme an den Anfang eines Sicherheitschecks zu stellen: „Jedes Unternehmen muss wissen, in welchen IT-Systemen sich die Kronjuwelen befinden. Es ist utopisch, zu glauben, man könnte sich auf Dauer zu 100 Prozent gegen massive und gezielte Angriffe schützen. Daher sollte man zunächst das Schutzbedürfnis einzelner Systeme und Daten genau definieren und den maximalen Schutz auf geschäftskritische Prozesse und Daten fokussieren."

So muss ein Händler, der den Großteil seines Umsatzes im Onlinehandel erwirtschaftet, alles daransetzen, seine Webshops zum Beispiel gegen den Missbrauch von Kundendaten oder DDoS-Attacken (Distributed Denial of Service) zu schützen. Mit dieser Angriffsmethode versuchen Hacker, Internetseiten lahmzulegen – beispielsweise die Website der Bundeskanzlerin. „Wenn Webshops eines Onlinehändlers über Tage nicht erreichbar sind, dann richtet das erheblichen finanziellen Schaden an und kann das Image nachhaltig zerstören", sagt Sperrle. Zwar verkaufe der Lebensmittelhändler Kaiser's Tengelmann selbst relativ wenig Ware im Netz, aber in anderen Tochtergesellschaften der Unternehmensgruppe Tengelmann mache E-Commerce einen nicht unerheblichen Anteil am Gesamtumsatz aus.

Auch Wirtschaftsspionage sei für einen Lebensmittelhändler mit überschaubarem Risiko verbunden, weiß Sperrle: „Wir verkaufen Produkte, die andere entwickeln und herstellen. Wir haben also wenig schützenswerte Patente, wie sie zum Beispiel die Lebensmittelhersteller selbst haben." Welche Kronjuwelen der CIO für Tengelmann identifiziert hat, verrät er allerdings nicht.

MEHR SICHERHEIT FÜR ALLE

Die Telekom hat ihre 1.800 Sicherheitsanforderungen an IT-/NT-Systeme überarbeitet und stellt sie jedem Interessierten frei zur Verfügung.

Bereits seit über zehn Jahren schreiben die Securityspezialisten der Telekom Sicherheitsanforderungen für IT-/NT-Systeme. Sie geben vor, worauf interne Entwickler und externe Dienstleister zu achten haben, wenn sie ein neues Produkt, ein System wie etwa eine Website erstellen. Die Sicherheitsanforderungen bilden das Rückgrat des Privacy-and-Security-Assessment(PSA)-Verfahrens, mit dem die Telekom das gleiche hohe Sicherheits- und Datenschutzniveau für alle Neuentwicklungen und Aktualisierungen gewährleistet, die sie selbst nutzt oder ihren Kunden anbietet. Seit 2011 gilt das sogar weltweit für alle Landesgesellschaften des Konzerns.

KOSTENLOSER DOWNLOAD FÜR ALLE

Im Laufe der Jahre entstanden 55 umfangreiche Papiere, die allgemeingültig-funktionale, systemspezifisch-funktionale und umsetzungsorientierte Sicherheitsanforderungen, etwa für einen Apache Server, enthalten. Im Sommer 2014 haben Experten der Group Security Service (SEC) der Telekom jedes dieser Papiere mit insgesamt 1.800 Einzelanforderungen geprüft und überarbeitet. Seit deren Inkrafttreten zum 1. Juli 2014 stellt die Telekom sie erstmals über www.telekom.com/sicherheit für jeden Interessierten frei zugänglich zum Download zur Verfügung.

„Diese Anforderungen“, sagt Markus Schmall, Vice President für Sicherheit in IT und Anwendungen und Testing bei der Telekom, „sind für jeden relevant, der das Sicherheitsniveau seiner Entwicklungen erhöhen möchte – und natürlich auch für jedes Unternehmen, das selbst Sicherheitsanforderungen für sich und seine Dienstleister definieren möchte.“ Die Idee hinter der Veröffentlichung ist klar: „Wenn jeder Entwickler unsere Anforderungen berücksichtigen würde, läge der Sicherheitsstandard bei IT-/NT-Produkten deutlich höher als jetzt.“ Mehr Sicherheit für alle also.

UNTERNEHMENSSICHERHEIT 2030: FAKTOR MENSCH IM FOKUS

Topmanager von Bayer, Daimler, Deutsche Post DHL, Deutsche Telekom und RWE haben mit Unterstützung des Verbands für Sicherheit in der Wirtschaft Nordrhein-Westfalen die Entwicklung von Sicherheitsthemen bis zum Jahr 2030 analysiert. Dabei betrachteten die Teilnehmer insbesondere die Herausforderungen der Informations- und Datensicherheit.

Initiatoren der branchenübergreifenden Studie „Corporate Security 2030: Challenges & Opportunities“ waren das Strascheg Institute for Innovation and Entrepreneurship (SIIE) der EBS Business School und das Beratungsunternehmen Z_punkt The Foresight Company. Das SIIE und Z_punkt brachten Sicherheitsexperten, Datenschutzverantwortliche und Topmanager von Bayer, Daimler, Deutsche Post DHL, Deutsche Telekom und RWE an einen gemeinsamen Tisch. Hinzu kamen Vertreter des Verbands für Sicherheit in der Wirtschaft Nordrhein-Westfalen (VSW NW).

HANDLUNGSSTRATEGIEN ABLEITEN

Das Hauptziel der Untersuchung bestand darin, zukünftige Herausforderungen für die Sicherheit der Konzerne zu ermitteln und zu bewerten. Daraus leiteten die Studienteilnehmer Handlungsstrategien für ihre Unternehmen und das Sicherheitsmanagement insgesamt ab. Es herrscht Einigkeit darüber, dass der Schutz von Know-how, Informationen und Daten eine zentrale unternehmerische Herausforderung bleiben wird.

Mit Blick auf die Handlungsstrategien empfehlen die Studienteilnehmer, sich nicht zu einseitig auf rein technologische Lösungen zu konzentrieren. Mindestens genauso wichtig sei es, den Faktor Mensch in das Sicherheitsmanagement noch stärker einzubeziehen. So gelte es, Wissensträger langfristig an das eigene Unternehmen zu binden. Gleichzeitig müssten die Mitarbeiter darin befähigt werden, verantwortungsvoll mit kritischen Daten und Informationen umzugehen – Stichwort: Human Firewall. Darüber hinaus gelte es, den physischen und logischen Zugriff auf unternehmensinterne Informationen gegenüber externen Dienstleistern zu definieren und strikt zu überprüfen. Angesichts der Tragweite dieser Aufgaben müsste Sicherheit noch intensiver im Bewusstsein eines jeden Mitarbeiters verankert werden.

ZUSAMMENARBEIT MIT SICHERHEITSBEHÖRDEN

Telekommunikationsunternehmen sind gesetzlich verpflichtet, mit staatlichen Stellen zu kooperieren, wenn die rechtlichen Voraussetzungen dazu erfüllt sind. Für Deutschland veröffentlicht die Telekom seit 2014, wie viele Überwachungsmaßnahmen sie ermöglichen musste und welche Auskünfte sie wie oft erteilt.

Im vergangenen Jahr belief sich die Zahl der überwachten Anschlüsse auf insgesamt 47.958. Richter oder Staatsanwälte haben die Mehrzahl der Maßnahmen auf Basis des Paragrafen 100a der Strafprozessordnung angeordnet. Nur ein geringer Teil ging auf das Artikel-10-Gesetz und die Landespolizeigesetze zurück. 2013 lag die Zahl der Überwachungen bei 49.796. Somit hat sich das Maßnahmenaufkommen nur unwesentlich verringert.

STEIGENDES INTERESSE AN VERKEHRSDATEN

Demgegenüber nahm das staatliche Interesse im Bereich der Verkehrsdaten weiter zu. 2014 griff die Telekom insgesamt 502.847 Mal auf ihre Verkehrsdatenbank zu, um den an sie gerichteten Auskunftsverpflichtungen nachzukommen. 2013 hatte die Vergleichszahl bei 436.331 Datensätzen gelegen. Die Menge der pro Datensatz übermittelten Kundenkennungen liegt noch einmal deutlich höher, wird jedoch nicht separat erfasst. Der Grund für die Abweichung wird vor allem im Mobilfunk erkennbar. Hier enthalten die zu beauskunftenden Verkehrsdatensätze sämtliche Kennungen, die in einer Funkzelle in einem bestimmten Zeitraum aktiv waren. Vor allem in Ballungszentren bewegt sich die Zahl der erfassten Kennungen dann rasch im drei- bis vierstelligen Bereich.

Bei den Teilnehmerbestandsdaten betrug die Zahl der Auskünfte 27.957. Im Wesentlichen handelte es sich dabei um die Übermittlung folgender Kundendaten: Name, Geburtsdatum, Rufnummer, Anschlussadresse, Rechnungsanschrift und Kontoverbindung. Darüber hinaus gab die Telekom zur Durchsetzung von Urheberrechtsansprüchen in insgesamt 733.377 Fällen die Daten von IP-Adressinhabern weiter.

VORGEHEN UNTERLIEGT STRIKTER KONTROLLE

In allen Fällen achtet die Telekom streng auf die Einhaltung des Fernmeldegeheimnisses und des Datenschutzes. Insbesondere ist gewährleistet, dass die Telekom nur dann tätig wird, wenn die rechtlichen Voraussetzungen dafür erfüllt sind. Bestehen Zweifel an der Wirksamkeit einer Anordnung, wird sie beanstandet und nicht umgesetzt. Unterstützungsleistungen für Überwachungsmaßnahmen werden dabei strikt nach dem Vieraugenprinzip erbracht. Hierbei sind immer zwei Mitarbeiter eingebunden, die sich gegenseitig kontrollieren. Jeder Bearbeitungsschritt wird ausführlich dokumentiert und unterliegt der regelmäßigen Kontrolle durch den Sicherheitsbevollmächtigten und die Bundesnetzagentur. Zusätzlich können der Datenschutzbeauftragte und die interne Revision der Deutschen Telekom jederzeit Prüfungen durchführen.

VERBINDLICHE LIEFERFRISTEN FÜR SICHERHEITSPATCHES

In puncto Sicherheit nimmt die Telekom ihre Zulieferer stärker in die Pflicht. 2014 hat der Konzern damit begonnen, Fristen für die Übermittlung von Sicherheitspatches zu vereinbaren.

Kritische Schwachstellen zeitnah zu beheben zählt zu den größten Herausforderungen des IKT-Sicherheitsmanagements überhaupt. Vor allem Softwarehersteller haben dies erkannt und ihre Entwicklungsprozesse bereits stark beschleunigt. Demgegenüber dauert das Patchmanagement im Bereich der Netzwerkausrüster oftmals noch deutlich länger. Um den Prozess zu verkürzen, stellt die Telekom sämtliche Rahmenverträge mit ihren Zulieferern um. Je nach Schweregrad der Schwachstellen werden die Hersteller darauf verpflichtet, innerhalb weniger Tage angemessene Sicherheitspatches auszuliefern. Für den Fall, dass sich die Fristen aus Komplexitätsgründen nicht einhalten lassen, müssen die Lieferanten eine funktionierende Übergangslösung (engl. Workaround) zur Verfügung stellen.

Um die Kritikalität der Schwachstellen zu bemessen, nutzen die Vertragspartner den Industriestandard CVSS (Common Vulnerability Scoring System). Auf einer Skala von 1 bis 10 beschreibt der CVSS das Gefährdungspotenzial, das von einer Schwachstelle ausgeht. Den CVSS-Wert 7 definiert die Telekom als Schwelle, die zu einem schnelleren Handeln aufseiten der Hersteller führen muss. Andererseits können Lieferanten Schwachstellen mit Werten zwischen 1 und 6 auch weiterhin über Standardupdates beheben.

WASCHMASCHINE FÜR MOBILFUNK

Ein neuer Sicherheitsservice sorgt dafür, dass Mitarbeiter von Unternehmen mobil sicher kommunizieren und keine Schadsoftware in Smartphone und Tablet eindringt.

Nur jedes fünfte deutsche Unternehmen achtet genau auf die Internetsicherheit seiner Smartphones, Tablets und Laptops. Dabei tauchten allein im Jahr 2013 fast 2,5 Millionen neue Schadprogramme für mobile Geräte auf. Mit einem neuen Service der Telekom bestimmen Unternehmen selbst, wie umfangreich die Schutzmaßnahmen ausfallen sollen. Wie eine Waschmaschine im Netz filtert ein Cloud-Dienst Schadcodes aus dem Internet heraus, bevor sie Smartphones und Tablets erreichen. Damit erübrigt sich der Einsatz von Virenschutz und Firewallfunktionen auf jedem einzelnen mobilen Endgerät.

Nutzer der Waschmaschine können einzelne Quell- und Zieladressen im Internetverkehr zulassen oder sperren. Darüber hinaus bestimmen sie, welche Ports sie erlauben, um etwa bekannte Botnetze zu blockieren. Zusätzlichen Schutz bietet die Verschlüsselung der Kommunikation über eine gesicherte Verbindung, den sogenannten SSL-VPN-Tunnel. Wählen sich Mitarbeiter dann über einen unsicheren Hotspot in das Internet ein, verhindert dies Fremdzugriffe und das unbemerkte Einklinken und Mitlesen der Kommunikation – Session Hijacking.

Was bereits in der Cloud „gereinigt“ wurde, richtet auf mobilen Endgeräten keinen Schaden an

Die Firmengeräte lassen sich über ein Webportal registrieren und konfigurieren. Auf Knopfdruck erhält man für jedes einzelne Gerät einen Überblick über alle Attacken. Die Anzahl der Nutzer ist frei wähl- und veränderbar und Sicherheitsstandards sind stets aktuell. Die Lösung leitet den gesamten Datenverkehr über deutsche Rechenzentren der Telekom, in denen der Verkehr in Echtzeit auf Gefahren geprüft und von diesen befreit wird.

SICHERHEIT VON INDUSTRIE 4.0

Auf dem Nationalen IT-Gipfel 2014 in Hamburg haben Infineon und die Telekom eine Sicherheitslösung zum Schutz der vernetzten Produktion vorgestellt.

Beim Nationalen IT-Gipfel wurde gezeigt, wie Unternehmen sensible Produktionsdaten über einen lückenlos sicheren Kommunikationskanal zwischen zwei deutschen Standorten übermitteln können. Insbesondere kleine und mittelständische Unternehmen, zum Beispiel aus dem Maschinen- und Anlagenbau oder der Fahrzeugzulieferindustrie, können davon profitieren. Denn Labore, Fabriken und Lager von Lieferanten, Produzenten und Kunden tauschen zunehmend größere Datenmengen aus. Sie werten diese Daten aus, um die Produktivität und Flexibilität in der industriellen Fertigung kontinuierlich zu steigern.

An der in Hamburg vorgestellten Sicherheitstechnologie „made in Germany“ sind auch die Unternehmen Fraunhofer SIT, TRUMPF, Wibu-Systems und Hirschmann beteiligt. Infineon liefert Sicherheitschips, die als Identitätsausweis für Computer, Router und Maschinen dienen und nur autorisierten Personen sowie nicht manipulierten Geräten Zugriff auf IT-Netzwerke gewähren. Erst nach erfolgreicher Prüfung werden die Daten verschlüsselt über sichere Telekommunikationsnetze übermittelt.

Die Telekom stellt eine sichere und hochverfügbare Netzinfrastruktur als wesentliches Bindeglied für die Echtzeitkonnektivität zur Verfügung. Dazu gehören gesicherte Cloud-Leistungen sowie mobile Endgeräte und deren Integrierbarkeit in Prozesse und Applikationen. Das Cyber Defense Center der Telekom ist ein wesentliches Element, um die sichere Ende-zu-Ende-Kommunikation der gezeigten Lösung sicherzustellen.

Ein Identitätsausweis gewährt nur autorisierten Personen Zugriff auf vernetzte Maschinen

FRITZ!BOXEN GESICHERT

Erstmals im Februar 2014 hatte die Telekom ihre Kunden auf eine Sicherheitslücke in Fritz!Boxen der Firma AVM hingewiesen. Mitte Dezember hatten von 4.000 nur noch 40 Kunden die angreifbaren WLAN-Router in Betrieb.

Im Oktober 2014 identifizierten die Telekom und AVM die hochgefährdeten Fritz!Boxen, deren Nutzer noch immer kein Update zur Behebung der Schwachstelle installiert hatten. Die Betroffenen wurden angeschrieben und vom Telekom Kundenservice angerufen. Wer Hilfestellung benötigte, dem stand eine spezielle Hotline zur Verfügung. 99 Prozent der von der Sicherheitslücke gefährdeten Telekom Kunden hatten bis zum 12. Dezember 2014 die notwendigen Softwareupdates heruntergeladen oder die Boxen ausgetauscht.

Die ungesicherten WLAN-Router erlaubten es Kriminellen, die Kontrolle über die Anschlüsse per Fernzugriff zu übernehmen. Die Hacker hätten die Schwachstelle dafür nutzen können, um auf Kosten ihrer Opfer teure Telefondienste im Ausland anzurufen. Erfährt die Telekom von möglichen Bedrohungen wie im Falle der Fritz!Boxen, informiert sie Kunden zügig über potenzielle Gefahren und Lösungsansätze. Dies gilt auch für den Fall, dass Experten IP-Adressen identifizieren, von denen aus Spamnachrichten verschickt werden. Die Telekom Kunden können dann das Passwort ihres E-Mail-Kontos ändern, um den Versand der unerwünschten Post zu unterbinden.

FireEye
SECURITY REIMAGINED

ABWEHR IN ECHTZEIT

Mit FireEye holte die Telekom im November 2014 einen Partner an Bord, der auf die Abwehr von hochkomplexen Cyberangriffen spezialisiert ist.

Die Cybersecurityexperten von FireEye sind auf die Abwehr von hochkomplexen Cyberangriffen spezialisiert. Die Lösungen ergänzen herkömmliche Abwehrsysteme wie Firewalls und Antivirenprogramme, welche zielgerichtete Angriffe nicht entdecken und abwehren. Cyberangriffe bleiben bisher durchschnittlich 229 Tage unentdeckt in Unternehmen und richten in dieser Zeit ungehindert Schaden an. FireEye dagegen erkennt Angriffe innerhalb weniger Minuten und leitet unverzüglich Abwehrmaßnahmen ein.

FireEye und T-Systems bieten gemeinsam einen durchgängig gemanagten Service, der Unternehmen schnell und wirkungsvoll vor IT-Spionage und Cyberattacken schützt. So entdeckten Fachleute von FireEye im Jahr 2013 elf bis dato unbekannte Schwachstellen, sogenannte Zero-Day-Sicherheitslücken, zumeist in Standardprogrammen wie Internet Explorer oder Adobe.

Die Lösungen ergänzen das von T-Systems entwickelte Securityportfolio „Advanced Cyber Defense by Telekom“ (ACD), das auf die Sicherheitsanforderungen von internationalen Großkonzernen zugeschnitten ist. Bei Cyberangriffen „unter dem Radar“, beispielsweise mit fingierten Dateianhängen in E-Mails oder mit Schadsoftware, die auf Webseiten hinterlassen wird (Drive-by Downloads), spielt ACD seine Stärken aus. Verdächtige E-Mail-Anhänge werden isoliert und erst danach geöffnet, um das „Verhalten“ der verdächtigen Datei in einer kontrollierten Umgebung zu analysieren.

SAFE FÜR UNTERNEHMENS-APPS

Mitarbeiter nutzen private Smartphones oftmals auch für dienstliche Zwecke. Dies öffnet Hackern Tür und Tor in die Unternehmens-IT. Safe Mobile Business Apps! Bietet einen sicheren Container für Apps.

Bring Your Own Device (BYOD) – die berufliche Nutzung privater Endgeräte – ist laut einer BITKOM-Studie inzwischen bei sieben von zehn Mitarbeitern in Deutschland üblich. In diesen Fällen steigt das Risiko, dass Hacker geschäftlich genutzte Apps als Einfallstor in die Unternehmenssysteme nutzen. Die Telekom hat mit Safe Mobile Business Apps eine Lösung entwickelt, die Business-Apps in einen sicheren Safe packt. Die IT-Abteilung muss damit nur noch den Container statt einer Reihe einzelner Apps steuern. Die Beschäftigten arbeiten damit auf ihren privaten Tablets oder Smartphones sicher mit Unternehmensdaten. Der Container gewährleistet, dass alle Apps reibungslos miteinander kommunizieren. Neue Sicherheitsrichtlinien für einzelne Apps, Updates oder das Einspielen neuer Programme geschehen minutenschnell und voll automatisiert über Funk. Geht ein Gerät verloren, lässt es sich aus der Ferne sperren und die Daten können gegebenenfalls komplett gelöscht werden. Ein App-Management organisiert zentral die Sicherung von Apps und Inhalten: Die Administratoren können Rechte rollenspezifisch vergeben, jeder Mitarbeiter erhält also nur Zugang zu jenen Daten und Anwendungen, die er für seine Tätigkeit braucht.

HACKER MADE BY TELEKOM

Anstatt sich nur auf dem Arbeitsmarkt auf die Suche nach hoch qualifizierten IT-Sicherheitsspezialisten zu machen, bildet die Deutsche Telekom gemeinsam mit der Industrie- und Handelskammer (IHK) Köln ihre eigenen Securityprofis aus: Im Jahr 2014 haben die ersten zehn Mitarbeiter eine Weiterqualifizierung zum „Cyber Security Professional“ begonnen.

Sandra Rutkowska ist alles andere als eine blutige Anfängerin. Gerade erst hat sie ihre Ausbildung als Fachinformatikerin für Systemintegration erfolgreich abgeschlossen. Doch für die 22-Jährige geht das Lernen direkt weiter. Denn sie ist eine von zehn Telekom Beschäftigten, die das neue Weiterbildungsprogramm „Cyber Security Professional“ durchlaufen. In zweieinhalb Jahren lernen fertige Azubis und Absolventen dualer Studiengänge, worauf es beim Thema IT-Sicherheit ankommt. Dabei wird ihnen auch beigebracht, sich als Hacker in vermeintlich sichere IT-Systeme einzuschleichen. Für Rutkowska eine spannende Herausforderung. „Ich habe mich zwar schon mit der Sicherheit von IT-Systemen auseinandergesetzt, aber in dieser Komplexität und Tiefe der Materie ist das Thema Datensicherheit für mich neu.“

MODULARES LERNEN

Für die Telekom ist die Qualifizierung im eigenen Hause ein wichtiger Baustein, um den zunehmenden Bedrohungen von außen entgegenzuwirken. „Trotz der gestiegenen Anforderungen im Bereich Cyber Security gibt es leider hierzulande noch nicht genügend und geeignete Ausbildungs- und Studiengänge für Abwehr und Sicherheitsexperten“, weiß Inge Rader, Leiterin HR Business Partner Datenschutz, Recht & Compliance und Group Security Services bei der Deutschen Telekom. „Indem wir unsere Experten selbst ausbilden, schaffen wir bedarfsgerechte Entwicklungschancen für unsere Mitarbeiter. Wir investieren damit in die Zukunft der Beschäftigten und stellen gleichzeitig den Schutz unserer Kunden und die Wahrung ihrer Interessen sicher.“

Im Rahmen der berufsbegleitenden Ausbildung durchlaufen die Teilnehmer zahlreiche Workshops und Onlineseminare zu technischen Themen wie digitaler Forensik, IT-Sicherheitsuntersuchungen und -konzepten, Testing sowie Programmiertechniken. Weiterhin gehören auch Soft Skills, etwa interkulturelles Projektmanagement, Präsentationstechniken oder das Argumentieren unter Stressbedingungen zu den Lerninhalten.

SCHWACHSTELLE MENSCH

Die Struktur und Abfolge der Lernmodule sind nicht fest vorgegeben. Jeder Teilnehmer hat so die Chance, seine Ausbildung selbst zu gestalten und das Erlernte in den jeweiligen Fachbereichen on the Job zu vertiefen. Unter anderem dürfen sich die Auszubildenden dabei auch als „Hacker“ versuchen, um Sicherheitslücken in den Systemen der Telekom aufzudecken und entsprechende Gegenmaßnahmen zu entwickeln. Zur Unterstützung stellt die Telekom den künftigen Sicherheitsexperten während der gesamten Qualifizierungsmaßnahme einen speziell dafür ausgebildeten Lernprozessbegleiter zur Seite.

Am Ende der Ausbildung steht im Frühjahr 2017 eine Prüfung durch die Industrie- und Handelskammer (IHK) Köln. Ulf C. Reichardt, Hauptgeschäftsführer der IHK Köln, erklärt, worauf es seiner Ansicht nach beim Thema IT-Sicherheit besonders ankommt. „Digitalisierung ist ein Thema, das nicht nur die Prozesse in Unternehmen betrifft, sondern die gesamte Unternehmenskultur beeinflussen wird“, so Reichardt. „An der wichtigen Schnittstelle Sicherheit ist gute Kommunikation für den Betrieb existenziell. Bei der Ausbildung zum Cyber Security Professional legen wir neben den technischen Skills daher großen Wert auf Fähigkeiten wie das Erarbeiten und Präsentieren von Konzepten sowie das Management komplexer Projekte.“

Auch die Abschlussarbeit, welche die Teilnehmer am Ende der Ausbildung vorlegen müssen, zielt in diese Richtung. Gefordert werden die Bearbeitung eines realen Falls aus dem direkten Tätigkeitsumfeld und die Präsentation der Ergebnisse vor der Prüfungskommission. So sollen die Absolventen zeigen, dass sie neben den technischen Lösungen auch die Umsetzung in die Unternehmens-praxis beherrschen.

DIGITALER WANDEL

Ein weiterer wichtiger Baustein der Ausbildung ist das Verhalten der Mitarbeiter im Umgang mit sensiblen Informationen. Ulf Reichardt: „Der Mensch spielt beim Thema IT-Sicherheit eine ebenso wichtige Rolle wie die Technik. Auch das soll im Rahmen der Ausbildung zum Cyber Security Professional vermittelt werden. Diese Ausbildung ist ein gutes Beispiel dafür, wie wir als IHK Köln unsere Mitgliedsunternehmen beim digitalen Wandel praxisnah unterstützen. Neue Herausforderungen brauchen eben auch neue Berufe.“

„Es hilft nicht, immer nur über den Fachkräftemangel zu klagen. Man muss aktiv werden und selbst gestalten“, erklärt Rader. „Mit unseren neuen Weiterbildungsangeboten in den Bereichen IT-Sicherheit und Datenschutz entwickeln wir eine Fortbildung, welche die Qualifizierung vom Azubi oder Studenten bis zum erfahrenen Profi viel stärker verzahnt. Das ist ein Gewinn für beide Seiten: Wir als Unternehmen verfügen so über die dringend notwendigen hoch qualifizierten Arbeitskräfte, und unsere Mitarbeiter profitieren sowohl von einem kontinuierlichen Lernprozess als auch interessanten Karriereperspektiven.“

Die Telekom bildet gemeinsam mit der Industrie- und Handelskammer Köln eigene Mitarbeiter zu Experten für Cybersicherheit aus

NEUER LEHRSTUHL FÜR DIE HOCHSCHULE LEIPZIG

Zusätzlich zur Qualifizierung zum Cyber Security Professional hat die Telekom eine neue Professur für Datenschutz und Sicherheit in der Informatik an der konzerneigenen Hochschule für Telekommunikation in Leipzig (HfTL) eingerichtet. Für zunächst fünf Jahre sollen die Dozenten und Studenten der HfTL Antworten auf folgende Fragen finden: Wie lässt sich die Gesellschaft für Datenschutz und Datensicherheit im Berufs- und Privatleben sensibilisieren? Wie können die Risiken, welche durch die Arbeit mit großen Mengen sensibler Daten entstehen, auf ein Mindestmaß reduziert werden? Und wie lassen sich Computerprogramme sicherer machen, ohne dabei Bedienungsfreundlichkeit und Barrierefreiheit einzuschränken? Ziel des Lehrstuhls ist es zudem, neue Lernmodule zu konzipieren, um die Weiterbildung rund um die Themen IT-Sicherheit und Datenschutz kontinuierlich zu verbessern. Schließlich startet die HfTL zum Wintersemester 2015/16 einen neuen Bachelorstudiengang, unter anderem mit den Schwerpunkten Datenschutzsensibilisierung, IT-Recht und -Forensik.

Hochschule für Telekommunikation Leipzig
University of Applied Sciences

KUNDENDATEN SCHÜTZEN

Alexander Schmitz ist einer der ersten Mitarbeiter, welche die Telekom zum „Cyber Security Professional“ ausbildet.

Herr Schmitz, Sie gehören zu den ersten zehn Mitarbeitern der Telekom, die sich zum „Cyber Security Professional“ weiterbilden lassen. Welche Vorkenntnisse bringen Sie mit?
Ich habe zunächst bei der Telekom eine Ausbildung zum Fachinformatiker Systemintegration absolviert. Durch eine Ausschreibung in einer internen Jobbörse bin ich dann auf die neue Qualifizierung zum IT-Sicherheitsexperten gestoßen.

Warum haben Sie sich beworben?
Es reizt mich, dass ich als Cyber Security Professional künftig einen wesentlichen Anteil daran habe, die Telekom Welt ein Stück sicherer zu machen und die Daten unserer Kunden wirkungsvoll zu schützen. Und natürlich macht mir das Thema IT-Sicherheit grundsätzlich großen Spaß.

War IT-Security immer schon Ihr Steckenpferd?
Nein, die Beschreibung der Ausbildung und die ersten Tätigkeiten in der Abteilung haben dazu geführt, dass mich das Thema so richtig gepackt hat.

Welche Erwartungen haben Sie an die Ausbildung?
Ich freue mich darauf, mir ein breites Wissen rund um das Thema IT-Sicherheit zu erarbeiten und dieses dann auch anzuwenden. Dabei interessieren mich vor allem die Themen Cloud, Virtualisierung und Storage. Und natürlich reizt es mich sehr, als „Hacker“ auch die andere Seite kennenzulernen.

Wie geht es nach der Ausbildung für Sie weiter?
Sicher ist, dass diese Qualifikation ein wichtiger Meilenstein auf meinem beruflichen Weg ist. Als nächsten Schritt stelle ich mir ein Studium und den Erwerb weiterer Securityzertifikate vor.

DIGITALE DREHSCHEIBE FÜR INFORMATIONSSCHUTZ

Die App InfoSecWheel zeigt Mitarbeitern der Telekom, wie sie sensible Informationen klassifizieren und verarbeiten dürfen.

Verschlüsseln oder nicht? Die Präsentation zum neuen Produkt ist fertig. Vor der Markteinführung soll ein Prototyp entwickelt werden, dessen Funktionalität die Präsentation detailgenau erklärt. Der Mitarbeiter aus der Produktentwicklung ist unschlüssig. Sein Vorgesetzter wartet auf die Folien, um sie bei einem internen Meeting auf Leitungsebene vorzustellen. Die Informationen sind sensibel und sollten nicht an die Öffentlichkeit gelangen. Soll er die Datei einfach als E-Mail-Anhang verschicken?

KLASSIFIKATION VON INFORMATIONEN

Um sicherzugehen, startet er die App InfoSecWheel auf seinem Smartphone, die der Bereich Group Security Governance (GSG) für die Mitarbeiter der Telekom erstellt hat. Die App ist wie eine Drehscheibe aufgebaut. In der ersten Ansicht zeigt sie dem Nutzer verschiedene Beispiele geschäftlicher Informationen wie Revisionsbericht, Managementreport und Vertragsentwurf. Per Wischbewegung wählt der Mitarbeiter das Beispiel aus, das seinen schützenswerten Informationen am meisten entspricht. Die App klassifiziert die entsprechende Präsentation daraufhin als vertraulich und gibt den Hinweis aus, dass der Mitarbeiter sie entsprechend kennzeichnen muss.

Nun wechselt der Nutzer zur Funktion „Umgang mit Informationen“. Die App zeigt ihm, dass er die Präsentation verschlüsselt per E-Mail an Berechtigte weitergeben darf. Unverschlüsselt oder etwa als Scan-to-E-Mail über einen Multifunktionsdrucker darf er die Folien nicht verschicken. Wenn der Mitarbeiter nicht genau weiß, wie er die Verschlüsselung einrichten soll, wechselt er zur Funktion „Verwendbare Produkte“. Hier sind alle Geräte, Dienste und Applikationen des Unternehmens gelistet, die für die Speicherung, Verarbeitung und den Austausch von Informationen zur Verfügung stehen. Per Filter wählt er nur diejenigen Produkte aus, die für die Schutzklasse „Vertraulich“ infrage kommen.

KOSTENLOSER DOWNLOAD

Die Funktion „Zusatzinformationen“ erklärt, wie er das gewählte Produkt einsetzen kann. Die Frage „Verschlüsseln oder nicht?“ kann der Mitarbeiter mithilfe der App nun einfach entscheiden und die Präsentation adäquat weitergeben – ganz ohne aufwendige Recherche in dicken Regelwerken.

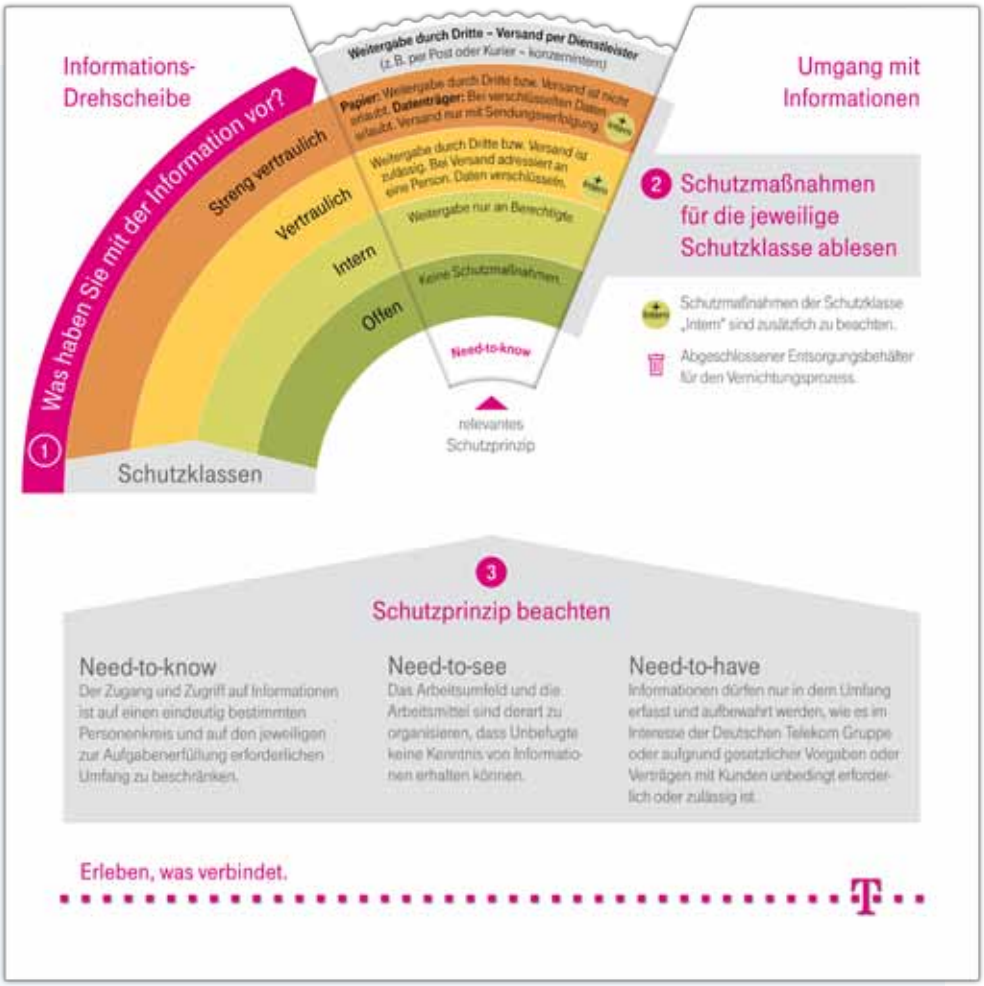
IN DER CHAMPIONS LEAGUE DER INFORMATIONSSICHERHEIT

Die Prüfgesellschaft DQS hat das Informationssicherheits-Managementsystem (ISMS) des Telekom Security Managements unter die Lupe genommen. Mit ihrem Überwachungsaudit bestätigen die Zertifizierer, dass der Konzern seine Risiken im Griff hat und den Vorgaben der ISO-Norm 27001 gemäß zu managen weiß.

Das von der DQS bestätigte Zertifikat belegt, dass die Telekom konzernweit qualifizierte Prozesse aufgesetzt hat, um ein einheitlich hohes Sicherheitsniveau zu erzielen. Im ISMS haben die Sicherheitsverantwortlichen definiert, welche Informationswerte welchen potenziellen Risiken ausgesetzt sind. Zudem sind die Prozesse des Sicherheitsmanagements hinterlegt. Hierbei vernetzt die Telekom sämtliche Handlungsfelder in einem einzigen Regelungsrahmen. Dieser reicht von der IT-/NT-Sicherheit über den Gebäude- und Objektschutz bis zum Kontinuitäts- und Lagemanagement. Da das ISMS alle Prozesse ganzheitlich betrachtet, dient es dem Management als solide Basis für sicherheitsrelevante Entscheidungen.

Ihr besonderes Augenmerk haben die Auditoren auf den in das ISMS eingebetteten kontinuierlichen Verbesserungsprozess gelegt. Dieser bietet den verantwortlichen Mitarbeitern eine systematische Handhabe, um die bestehenden Restrisiken fortlaufend zu minimieren. Laut internem DQS-Benchmark spielt das ISMS der Telekom damit in der obersten Liga vergleichbarer Lösungen. Dank einheitlicher Sicherheitsstandards erreicht der Konzern ein weltweit gleich hohes Sicherheitsniveau, das den relevanten Risiken angemessen ist. Der Reifegrad des ISMS spiegelt wider, dass die Telekom das Bestmögliche tut, um die ihr anvertrauten Informationswerte nachhaltig zu schützen.

Das InfoSecWheel basiert auf einer Informationsdrehscheibe aus Papier, die von GSG im Jahr 2012 entwickelt wurde. Rund 20.000 Beschäftigte des Konzerns nutzen diese Scheibe. Im Herbst 2014 hat die Telekom die Drehscheibe als App umgesetzt, um Informationen leichter aktualisieren und die Produkte des Konzerns mit Zusatzinformationen hinterlegen zu können. Mitarbeiter finden die App im unternehmenseigenen App Store. Die Telekom stellt das InfoSecWheel auch externen Unternehmen zum kostenlosen Download über die öffentlichen App Stores von Google und Apple zur Verfügung. Auf Wunsch können diese das InfoSecWheel auch individualisiert nutzen – mit eigenem Design und unternehmensspezifisch hinterlegten Produkten. Individualisierte Versionen bietet die Telekom allerdings kommerziell an.



NEUER SPITZENWERT FÜR SICHERHEITSBEWUSSTSEIN

Die Telekom misst jährlich, wie groß das Sicherheitsbewusstsein ihrer Mitarbeiter für die Anforderungen der Informationssicherheit ist. Als Kennzahl dient der Security Awareness Index (SAI) des Steinbeis Beratungszentrums. 2014 hält die Telekom im SAI-Benchmarkvergleich die Bestmarke.

Der SAI macht das Sicherheitsbewusstsein der Mitarbeiter von Autoherstellern, Banken und IT-Unternehmen vergleichbar. Er ist eine verdichtete Kennzahl aus zehn Sicherheitsthesen. Das durchschnittliche Sicherheitsbewusstsein aller Beschäftigten wird als Punktwert ausgewiesen. Als Erhebungsmethode dient eine Onlineumfrage, zu der die Telekom im vergangenen Jahr rund 40.500 Mitarbeiter und Führungskräfte aus insgesamt 57 Unternehmenseinheiten per Zufallsstichprobe ausgewählt und befragt hatte. Mit einer Rücklaufquote von 45 Prozent erzielte die Telekom die bislang höchste Beteiligung im Konzern.

Auch qualitativ gesehen hat die Telekom 2014 alles in allem ein hohes Niveau mit Blick auf das Sicherheitsergebnis erreicht – wobei zum Beispiel die Mitarbeiter der Telekom in Deutschland 77,6 Punkte auf der bis 100 reichenden SAI-Skala erzielt haben. Damit nimmt die Telekom branchenübergreifend einen Spitzenplatz ein. Auch unternehmensintern zeigt der SAI auf, wie sicherheitsbewusst die jeweilige Belegschaft ist, und erfasst die Effizienz von Awareness-Maßnahmen. Die Wirksamkeit wird in der zeitlichen Veränderung sichtbar und liefert den Verantwortlichen Hinweise, an welchen Stellen die Mitarbeiter zusätzliche Unterstützung brauchen.

Konzernweit hat die Telekom Sicherheitsexperten im Einsatz, deren Aufgabe es ist, die Sensibilität der Mitarbeiter für die Anforderungen des Sicherheitsmanagements zu steigern. Ein Schwerpunkt der aktuellen Maßnahmen liegt auf der Schulung von Führungskräften. Die Sensibilisierungsarbeit konzentriert sich auf Themen wie Informationssicherheit und Datenschutz, IT- und NT-Sicherheit, Zutrittsschutz, Social Engineering und den sicheren Umgang mit sozialen Netzwerken.

Impressum

Herausgeber

Deutsche Telekom AG
Vorstandsbereich Datenschutz,
Recht und Compliance
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 Telekom, BPA/Jesco Denzel (S. 8), Bundesregierung/ Kugler, Henning Schacht (S. 6), Fritz Schumann, Valentina Vos, Fotolia, iStockphoto

Stand: 1/2015

www.telekom.com/datenschutz

www.telekom.com/sicherheit