Erleben, was verbindet.

INHALT

„Es geht um nichts weniger als den Erhalt des hohen Datenschutzniveaus in Deutschland“, sagt Professor **Hansjörg Geiger**, Mitglied des Datenschutzbeirats, im Interview.

21

Schnelle Eingreiftruppe – Das Deutsche Telekom CERT koordiniert das Management von Sicherheitsvorfällen für alle Informations- und Netzwerktechnologien des Konzerns.

26

Mobile Endgeräte geraten immer mehr ins Visier von Cyberkriminellen. Unternehmen sollten von den Angreifern lernen.

42

Kundendienst an der Cyberfront. Das Abuse-Team der Telekom ist Ansprechpartner für jeden, der den Missbrauch von Internetdiensten melden will. 2012 gingen die Sicherheitsexperten mehr als einer Million Hinweisen nach.

44

Allianz für Cyber-Sicherheit

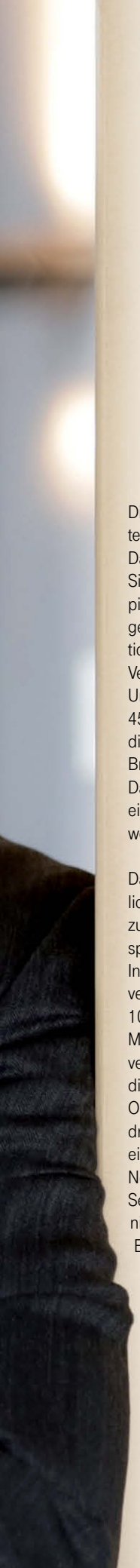
Allianz für Cybersicherheit – mehr Schutz durch Kooperation, fordert **Michael Hange**, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

46

„Wir müssen Mauern einreißen.“

In der Spitze verzeichnen die IT-Systeme der Deutschen Telekom 400.000 digitale Angriffe an einem Tag. Damit die Angreifer verlieren, entwickelt die Telekom ihr Datenschutz- und Datensicherheitsniveau konsequent weiter.

Dr. Thomas Kremer,
Vorstand Datenschutz,
Recht und Compliance



Dr. Thomas Kremer
gibt Tipps für sicheres Surfen im Netz und erklärt, wie sich Smartphones sichern lassen.

Die Kunden scheinen diesen Einsatz für Datenschutz und Datensicherheit zu honorieren. Das zeigen die repräsentativen Ergebnisse des Sicherheitsreports des Instituts für Demoskopie Allensbach aus dem Jahr 2012. Danach genießt die Telekom in der Telekommunikations- und Internetbranche einen deutlichen Vertrauensvorsprung in Bezug auf den Umgang mit persönlichen Daten. Immerhin 45 Prozent der Gesamtbevölkerung halten die Telekom für vertrauenswürdig. In einer Branche, die in hohem Maße mit persönlichen Daten ihrer Kunden umgehen muss, ist solch ein Ergebnis außerordentlich. Zumal Wettbewerber weit zurück auf den Plätzen liegen.

Das Engagement für Datenschutz und Datensicherheit wird die Telekom kontinuierlich ausbauen – was nicht nur angesichts der zunehmenden Bedrohung aus dem Cyberspace unabdingbar ist. So hat sich die Zahl der Internetangriffe innerhalb eines Jahres nahezu verdoppelt. Inzwischen gibt es täglich rund 100.000 neue Varianten von Schadsoftware. Mit immer intelligenteren digitalen Waffen versuchen die professionellen Angreifer in die IT-Systeme von Unternehmen, staatlichen Organisationen und Privatpersonen einzudringen. Wie weit dies gehen kann, belegt ein erfolgreicher Angriff von Hackern Ende November 2012. Ihnen ist es gelungen, in die Server der Internationalen Atomenergieorganisation (IAEA) einzudringen und vertrauliche E-Mail-Adressen zu stehlen und zu veröffentlichen.

Obwohl die Sicherheitsexperten der Deutsche Telekom Methoden entwickeln, mit denen sie Angriffe analysieren und bisher verhindern konnten, können wir uns darauf nicht ausruhen. Aber allein – und darin besteht Konsens im Vorstand – lässt sich der Kampf gegen die Cyberangriffe nicht gewinnen. Daher verstecken wir uns nicht hinter Mauern des Schweigens und setzen auf das Prinzip Hoffnung. Wir führen die Spitze einer Bewegung an, die gemeinsam mit anderen Unternehmen und staatlichen Sicherheitsbehörden alles dafür tun wird, den Gefahren einer vernetzten Gesellschaft zu begegnen. Wir machen wie kaum ein anderes Unternehmen die Attacken auf unsere Systeme transparent. Wir wollen so unser Wissen teilen und erreichen damit, dass andere schneller geeignete Gegenmaßnahmen einleiten können. Denn etwa 90 Prozent der Angriffe sind vermeidbar, wenn wir die Systeme auf dem aktuellen Stand halten.

„Vertrauen ist die Grundlage für ein erfolgreiches Geschäft!“

Doch noch hüllen sich die meisten Unternehmen aufgrund der Angst vor Imageverlusten in Schweigen. Welche Vorteile haben sie davon, wenn sie Informationen über Cyberangriffe auf eigene Systeme für sich behalten? Keine! Denn längst wissen alle, dass jeder von uns Opfer einer Cyberattacke sein kann. Daher müssen wir die Mauern des Schweigens einreißen! Die deutsche Industrie kann sich auf Dauer nur effizient gegen digitale Bedrohungen schützen, wenn sie zusammenarbeitet. Dies fängt mit ganz praktischen Maßnahmen an. So wollen wir mit anderen Unternehmen der IT- und Telekommunikationsindustrie – auch unseren Wettbewerbern – ein gemeinsames und unabhängiges Testzentrum einrichten. Darin könnten alle beteiligten Unternehmen kritische Netzkomponenten auf Sicherheit gegen digitale Angriffe überprüfen. Wenn sich das Bundesamt für Sicherheit in der Informationstechnik an einem solchen Testzentrum beteiligen würde, dann könnte dies sogar in ein offizielles Sicherheitssiegel für technische Produkte münden.

Technik für mehr Datensicherheit ist aber nur die eine Seite der Medaille. Auch der Datenschutz erfordert noch sehr viel mehr Aufmerksamkeit. Zwar ist das Datenschutzniveau in Deutschland und einigen Ländern Europas sehr hoch, doch wir brauchen dringend weltweit konsistente Rahmenbedingungen für den Datenschutz. Dies hat nicht nur etwas mit gleichen Wettbewerbschancen zu tun. Nur so gewinnen wir das Vertrauen der Kunden und verhelfen digitalen Geschäftsmodellen langfristig zum Erfolg.

Die Deutsche Telekom ist Vorreiter in Sachen Datenschutz und Datensicherheit. Doch wir werden nicht nachlassen, das Vertrauen unserer Kunden weiter zu stärken. Denn neue Geschäftsfelder wie Cloud-Dienste und intelligente Netze für die Stromversorgung oder die Gesundheitsbranche werden nur funktionieren, wenn Kunden auf sichere Lösungen vertrauen können.

Dr. Thomas Kremer
Vorstand Datenschutz, Recht und Compliance

Zur Person

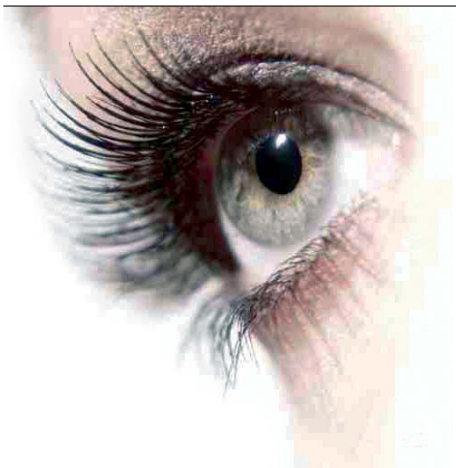
Dr. Thomas Kremer ist seit Juni 2012 Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom AG. Zuvor arbeitete er als Generalbevollmächtigter für die ThyssenKrupp AG, wo er 2003 die Leitung des Rechtsbereichs übernahm und 2007 zum Chief Compliance Officer des ThyssenKrupp Konzerns ernannt wurde.

Kundendatenschutz im Verkaufsraum

DEKRA zeichnet Telekom Shops zum dritten Mal in Folge aus.

Hohe Sensibilität und Kompetenz im Umgang mit Kundendaten zahlen sich aus. Wie bereits in den vorangegangenen Jahren hat die Prüfgesellschaft DEKRA die Telekom Shops auch 2012 erfolgreich auditiert. Sämtliche Verkaufsstellen dürfen das DEKRA-Siegel „Datenschutz und Datensicherheit gemäß dem Bundesdatenschutzgesetz“ ein weiteres Jahr nutzen. Erstmals besuchten die DEKRA-Experten rund 150 Shops ohne vorherige Ankündigung. Die Audits umfassten im Wesentlichen zwei Bereiche: Zum einen nahmen die Prüfer die Sicherheit im Ladengeschäft unter die Lupe. Beispielsweise klärten sie, ob Kundendaten ausreichend vor Diebstahl oder Verlust geschützt sind. Zum anderen prüfte die DEKRA den datenschutzkonformen Umgang mit den Kundendaten. Die Telekom Shops wollen das erreichte Datenschutzniveau weiter steigern.

Wie bereits in den vorangegangenen Jahren hat die Prüfgesellschaft DEKRA die Telekom Shops auch 2012 erfolgreich auditiert.



Mit einem engmaschigen Netz von Eigenkontrollen den Datenschutz auf den Prüfstand stellen.

Mit eigenen Augen

Interne Audits zeigen anhaltende Verbesserung des Datenschutzes weltweit.

Die Deutsche Telekom überprüft das Datenschutzniveau im Konzern durch ein engmaschiges Netz eigener Kontrollen. 2012 führte der Konzerndatenschutz insgesamt 60 interne Audits durch. Wie bereits in den vorangegangenen Jahren konzentrierte sich die Prüfarbeit auf geschäftskritische Anwendungen und Prozesse sowie auf den Datenschutz in einzelnen Landesgesellschaften und Tochterunternehmen.
Ziel der Prüfungen ist es, Schwachstellen zu erkennen und durch geeignete technische und organisatorische Maßnahmen auszuräumen. Darüber hinaus gewinnt die Telekom belastbares Wissen darüber, wie sich das Datenschutzniveau konzernweit entwickelt.

Das größte Spektrum von Kennzahlen liefert das Basisdatenschutzaudit. Hierbei handelt es sich um eine jährliche Befragung, an der 2012 mehr als 36.000 Mitarbeiter aus 35 Landesgesellschaften teilnahmen. Das Audit verdeutlicht, wie die Beschäftigten das Datenschutzniveau ihres Arbeitsumfelds einschätzen, ob sie die für ihre Tätigkeit relevanten Datenschutzprozesse kennen und inwieweit sie die vorgeschriebenen Werkzeuge anwenden.
Die 2012 ermittelten Kennzahlen zeigen, dass die Sensibilität und das Wissen im Umgang mit personenbezogenen Daten international im Konzern weiter gestiegen sind. Für Deutschland belegt das Audit einen Datenschutz auf hohem Niveau.

Geprüfte Qualität

TÜV NORD zertifiziert Abrechnungsprozesse der Deutschen Telekom.

Im Festnetz- und Mobilfunkgeschäft erstellt die Telekom etwa 65 Millionen Rechnungen pro Monat. Kunde für Kunde sind dabei je nach Tarif oft Hunderte, nicht selten sogar Tausende von Verkehrsdaten zeitgenau abzurechnen. Eine hochkomplexe Aufgabe, die vom Erheben und Vorverarbeiten der Daten über die eigentliche Rechnungslegung bis zum Schreiben, Ausliefern und Archivieren der Rechnungen reicht. Sowohl im Mobilfunk als auch im Festnetzbereich arbeiten hierzu zahlreiche unterschiedliche IT-Systeme zusammen. 2012 hat der TÜV NORD die gesamte Prozesskette und die darin eingebundenen Systeme auditiert. Die Prüfer bewerteten sowohl den Datenschutz als auch die IT-Sicherheit des Rechnungsprozesses. Während der Festnetzbereich sein Zertifikat aus dem Jahr 2010 erneuern konnte, erhält der Mobilfunk das TÜV-Siegel zum ersten Mal.

TÜV Rheinland zertifiziert externe Callcenter

Alle Telekom-Partner schließen Audits erfolgreich ab.

Die Callcenter-Dienstleister der Telekom haben laut TÜV Rheinland ihr hohes Datenschutzniveau auch 2012 bestätigt. Sämtliche Audits gingen positiv aus. Während die insgesamt 14 Hotline-Dienstleister ein neues TÜV-Siegel erhielten, erneuerten die 17 im Vertrieb eingesetzten Callcenter-Unternehmen das Siegel aus 2010. Der zweijährige Turnus ist Teil eines Prüfkonzepts, das der TÜV Rheinland gemeinsam mit der Telekom entwickelt hat. Das 2009 konzipierte Siegel ist das einzige seiner Art in der deutschen Callcenter-Branche. Die Telekom ergänzt die Arbeit der Prüfgesellschaft durch eigene Audits, sobald sich datenschutzrelevante Veränderungen bei den Partnern abzeichnen. Unter anderem schaltet das Risikomanagement im Vertrieb und Service Prüfungen zwischen, wenn neue Dienstleister ihre Arbeit aufnehmen. Gleiches gilt für Callcenter-Partner, die weitere Standorte gründen oder zusätzliche Services übernehmen. 2012 führte die Telekom 22 Prüfungen dieser Art durch.

Bundesnetzagentur auditiert Rechenzentrum Münster

Kundendatenschutz im Mobilfunk

Tut die Telekom alles Erforderliche, um die Daten ihrer Mobilfunkkunden zu schützen? Die Frage entscheidet sich keineswegs nur in Callcentern und Telekom Shops. Wesentlichen Anteil an einem optimalen Datenschutz haben auch die Rechenzentren, die Software für das Kundenbeziehungsmanagement (engl. CRM) betreiben. Im September 2012 prüfte die Bundesnetzagentur das Rechenzentrum Münster, in dem die Telekom CRM-Software für ihre Mobilfunksparte hostet.

Beim Datenschutz konzentrierte sich das Audit auf zwei große Themengebiete: Mit Blick auf das Tagesgeschäft kontrollierte die Bundesnetzagentur, ob die Telekom abrechnungsrelevante Gesprächsdatensätze rechtskonform verarbeitet, speichert und löscht. Zudem untersuchten die Auditoren, wie der administrative Bereich gegen Missbrauch abgesichert ist. Die Bundesnetzagentur zeigte sich mit dem Vorgehen des Rechenzentrums in Münster in allen Punkten einverstanden.

Mehr Lebensqualität für ältere Menschen durch den Einsatz von intelligenten Geräten und Systemen.

Selbstbestimmtes Leben im Alter

Telekom entwickelt datenschutzkonforme Kommunikationssysteme im Forschungsprojekt SmartSenior.

Technologien schaffen, die älteren Menschen ein längeres selbstbestimmtes Leben in den eigenen vier Wänden ermöglichen. Dafür haben sich 28 Partner aus Industrie und Wissenschaft in dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt SmartSenior zusammengetan. Ergebnis ist das Gesamtsystem SmartSenior. Mit leicht zu bedienenden Gesundheits-, Sicherheits-, Service- und Kommunikationslösungen schafft SmartSenior intelligente Lebenswelten für ältere Menschen. Als kommunikatives Zentrum dient der Fernseher, der durch Touchpad, Smartphone, Raumsensoren, Kamera, medizinische Messgeräte und eine intelligente Armbanduhr ergänzt wird. Die Telekom Innovation Laboratories haben das Gesamtvorhaben koordiniert und eine Reihe von Teilsystemen selbst entwickelt. So zum Beispiel eine Kommunikationslösung, welche die Mitarbeiter eines angeschlossenen Assistenzcenters alarmiert, wenn Sensoren eine Gefahrensituation in einer Wohnung erkannt haben und eine Reaktion des Bewohners darauf ausbleibt. Akzeptanz erhalten derartige Lösungen nur, wenn auch der Datenschutz berücksichtigt wird. Für ihren Zuständigkeitsbereich hat die Deutsche Telekom Verfahrensbeschreibungen und daraus gemeinsam mit den Partnern ein Datenschutzkonzept erstellt. Anwendung fanden alle aktuell geltenden Datenschutzbestimmungen der Länder Berlin/Brandenburg und des Bundes sowie die regulativen Anforderungen für klinische Studien. Die Datenschutzberater der Telekom begleiten auch zukünftige Projekte, die im Umfeld von SmartSenior entstehen.

Löschen für Fortgeschrittene

Telekom entwickelt revisionssichere Lösung zum Löschen von Beschäftigtendaten in SAP-Software.

Die Anforderungen an das Löschen personenbezogener Daten sind in der Personalwirtschaft besonders groß. Um regelkonform vorzugehen, muss ein Konzern wie die Deutsche Telekom zahlreiche gesetzliche Regelungen sowie eine Reihe betrieblicher Bestimmungen beachten. Keine triviale Aufgabe, zumal die Aufbewahrungs- und Löschfristen je nach betreffendem Gesetz zum Teil stark voneinander abweichen. 2012 hat die Telekom die relevanten Anforderungen analysiert und ein revisionssicheres Konzept für die Löschung personenbezogener Daten in SAP HR entwickelt.

SAP HR ist das zentrale Softwaresystem, mit dem das Personalwesen der Telekom seine Aufgaben steuert. Allein im Hauptmandanten verarbeitet die Personalwirtschaftssoftware die monatlichen Bezüge von mehr als 120.000 Mitarbeitern. Bei der Umsetzung des Löschkonzepts stieß das von SAP angebotene Löschmodul an seine Grenzen. Daher entschied sich die Telekom für den ergänzenden Einsatz eigener Lösungen.

Auf Konzernebene gilt das neue Löschkonzept als das erste seiner Art. Ein Erfahrungsaustausch fand bereits mit dem Bundesverkehrsministerium und einigen DAX-30-Unternehmen statt, deren Personalwesen vergleichbare Herausforderungen zu erfüllen hat. Zudem steht die Telekom mit Bundes- und Landesbehörden im Dialog, die für den Beschäftigtendatenschutz zuständig sind.

Startschuss für De-Mail

Sichere E-Mail-Infrastruktur für Bürger, Unternehmen und Behörden.

Im August 2012 hat die Deutsche Telekom den sicheren Maildienst De-Mail gestartet. Privatkunden und Firmen nutzen das neue Angebot, um digitale Dokumente vertraulich zu versenden. Grundlage bildet das De-Mail-Gesetz. Abgesicherte Anmeldeverfahren, verschlüsselte Transportwege sowie Sende- und Empfangsbestätigungen ermöglichen eine sichere und nachweisbare elektronische Kommunikation. Dritte können Nachrichten weder einsehen noch manipulieren. Da das De-Mail-Gesetz hohe Anforderungen an Sicherheit und Datenschutz stellt, müssen Anbieter einen strengen Akkreditierungsprozess durchlaufen. Erst danach werden die Unternehmen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) als De-Mail-Diensteanbieter zugelassen. Die Deutsche Telekom hat die Akkreditierung erfolgreich abgeschlossen. Seit März 2012 sind Telekom Deutschland und T-Systems International offiziell zugelassene De-Mail-Provider.

Schnelles Eingreifen

Telekom-Niederlassung vernichtet unzulässig gesammelte Gesundheitsdaten.

Im Januar erhielten Führungskräfte der Deutschen Telekom Technik in Bayreuth die interne Aufforderung, Informationen zu Gesundheit und Leistung ihrer Mitarbeiter festzuhalten. Diese Vorgabe widersprach den gesetzlichen Bestimmungen und den internen Vorgaben zum Umgang mit Beschäftigtendaten. Unmittelbar nach Bekanntwerden des Vorhabens wurden die bereits vorhandenen Listen vollständig vernichtet. Das schnelle Eingreifen erfolgte auf Intervention des örtlichen Betriebsrats. Gegen den Mitarbeiter, der die Liste initiiert hatte, hat die Telekom arbeitsrechtliche Maßnahmen ergriffen.

Klügeres Fernsehen

Telekom führt statistische Auswertung von Entertain-Nutzungsdaten ein.

Mit Web-TV, Mediatheken oder TV-Archiven können Zuschauer frei entscheiden, wann und auf welchem Endgerät sie das Format ihrer Wahl nutzen wollen. Je weiter der Wandel vorangeht, desto wichtiger wird es für Anbieter, die sich ändernden Konsumgewohnheiten zu verstehen. Dies gilt auch für das webbasierte Telekom-Angebot Entertain. Seit Juli 2012 erhebt die Telekom Nutzungsstatistiken, um die Produktqualität von Entertain weiter zu steigern. Im Zentrum des Interesses steht die Frage, welche Sendungen bevorzugt gesehen und welche Inhalte aus der Videothek abgerufen werden. Die Deutsche Telekom hat das Verfahren zur Nutzungsdatenauswertung den zuständigen Bundes- und Landesbeauftragten für Datenschutz und Informationsfreiheit vorgestellt und ist dabei auf die geltend gemachten kritischen Punkte eingegangen. Über technisch-organisatorische Rollenkonzepte ist sichergestellt, dass keine Rückschlüsse auf einzelne Kunden möglich sind. Zudem steht es jedem Kunden frei, die Auswertung seiner Daten jederzeit zu unterbinden. Bereits im Juni hatte die Deutsche Telekom ihre Kunden mit einer E-Mail und einer Bildschirmmeldung in Entertain über die geplante Datenerhebung und die Möglichkeit zum Widerspruch informiert. Dadurch war gewährleistet, dass die Kunden ihren Widerspruch einlegen konnten, bevor die statistische Nutzungsdatenauswertung begonnen hatte.

Trotz Analyse des Nutzungsverhaltens von Entertain, lassen sich keine Rückschlüsse auf einzelne Kunden ziehen.

„Es wird höchste Zeit.“

Ende Januar 2012 hat die Europäische Kommission den Entwurf einer Datenschutz-Grundverordnung für die Europäische Union (EU) vorgestellt. Sie soll Anfang 2014 in Kraft treten und wäre dann nach einer Übergangsfrist in allen EU-Ländern unmittelbar rechtlich bindend.

Dr. Claus Ulmer ist seit Juli 2002 Konzernbeauftragter für den Datenschutz der Deutschen Telekom Gruppe.

Wie immer, wenn Gesetzgeber neue Vorgaben machen, läuten auch bei der EU-Datenschutz-Grundverordnung einige Gegner die Warnglocken. Gerade in Ländern, in denen die Regierungen weniger strenge Datenschutzgesetze aufgelegt haben, reißt die Kritik an dem 91 Artikel umfassenden Entwurf nicht ab. Wie bewertet Dr. Claus Ulmer, Konzernbeauftragter für den Datenschutz der Deutschen Telekom, den Vorstoß aus Brüssel?

Herr Dr. Ulmer, können Sie die Kritik am Entwurf der EU-Datenschutz-Grundverordnung nachvollziehen?

Dr. Claus Ulmer: Zunächst einmal ist das Vorhaben der Europäischen Union sehr zu begrüßen und zudem dringend notwendig. Wir brauchen ein EU-weit einheitliches Datenschutzrecht. Gerade international tätige Konzerne wie die Deutsche Telekom benötigen Rechtssicherheit durch einheitliche und verlässliche Regeln. Im Großen und Ganzen ist der vorliegende Entwurf gelungen, weil er sowohl den aktuellen technischen Entwicklungen bei Datenverarbeitung im Internet als auch der internationalen Vernetzung Rechnung trägt. Sicherlich sehen wir bei einigen Punkten noch Diskussionsbedarf. Ein Beispiel: Sinnvoll ist zwar die im Entwurf beabsichtigte Regelung der Zuständigkeit bei den Aufsichtsbehörden im Sinne eines One-Stop-Shops. Hier muss der Regelungstext aber noch so angepasst werden, dass zweifelsohne auch multinational tätige „Unternehmensgruppen“ mit vielen Legaleinheiten unter die Regelung fallen und so davon profitieren können. In der Gesamtbetrachtung des jetzigen Verordnungsentwurfs überwiegen aber die Vorteile eines einheitlichen europäischen Datenschutzstandards bei weitem. Ich bin davon überzeugt, dass die EU mit der EU- Datenschutz-

Grundverordnung Standards setzt und alle anderen Staaten nach und nach ebenfalls ein höheres Niveau für ihren Datenschutz einschlagen werden. Beispiele dafür haben wir in jüngster Vergangenheit in Malaysia und Singapur gesehen.

Manche Unternehmen sind der Meinung, eine Selbstbindung würde ausreichen.
Dr. Claus Ulmer: Selbstbindung würde uns kaum weiterbringen, denn wer soll das kontrollieren? Auch würde bei einer Vielzahl von möglichen Selbstbindungen die Einheitlichkeit bei den Standards nicht in dem Maße erreicht, wie bei der geplanten Verordnung. Wir selbst können mit den strengen Datenschutzvorgaben aus dem deutschen Telekommunikationsgesetz sowie dem deutschen Datenschutzgesetz schon seit Jahren gut leben – teilweise gehen wir als Telekom sogar über die gesetzlich vorgeschriebenen Anforderungen hinaus. Zudem sind die Prozesse zur Selbstbindung nach den bisherigen Erfahrungen zu lang. Es setzt in der Regel erst einmal ein Diskussionsprozess ein, bevor überhaupt über verbindliche Inhalte gesprochen werden kann. Das behindert aber schnelle und flexible Geschäftsabschlüsse mit anderen Unternehmen, etwa bei Cloud-Angeboten. Zudem führt der Selbstbindungsansatz oft zur Verwirrung bei den Verbrauchern darüber, was denn nun wirklich gewollt oder gemeint ist. Klare, allgemein verbindliche Rahmenbedingungen halte ich daher als Grundlage für höchste Flexibilität der Unternehmen für besonders wichtig. Diese Chance kann uns die EU-Datenschutz-Grundverordnung geben.

Neu in einigen Ländern wird sein, dass Unternehmen ab 250 Mitarbeitern einen Datenschutzbeauftragten benennen müssen. Ist dies nicht längst überfällig?
Dr. Claus Ulmer: Unbedingt, da es zur Beurteilung von Fragestellungen aus dem Datenschutz in jedem Unternehmen eine neutrale und weisungsfreie Instanz geben sollte. Sie muss die Regeln für die Einhaltung der Datenschutzanforderungen vorgeben, deren Einhaltung prüfen und gegebenenfalls intervenieren können, ohne dadurch Nachteile im Unternehmen befürchten zu müssen. Die Deutsche Telekom nimmt die Rolle und die Befugnisse des Datenschutzbeauftragten sehr ernst. Der Datenschutzbeauftragte genießt in diesem Konzern auf seinem Fachgebiet eine weisungsfreie und unabhängige Stellung und nimmt insoweit unmittelbaren Einfluss auf unternehmerische Entscheidungen.

Die Regelungen im Verordnungsentwurf sollten sich an der deutschen gesetzlichen Regelung orientieren und zumindest dem internen Datenschutzbeauftragten auch die Position einer unabhängigen Kontrollinstanz zuschreiben, damit die Position sinnvoll ausgestaltet werden kann.

„Die Deutsche Telekom nimmt die Rolle und die Befugnisse des Datenschutzbeauftragten sehr ernst.“

Aus Sicht der Deutschen Telekom sollte die Einrichtung der Stelle eines Datenschutzbeauftragten für die Unternehmen auch auf Ebene der EU-Verordnung mit Privilegien einhergehen. Wir unterstützen daher den Vorschlag, Melde- und Konsultationsverpflichtungen bei der Bestellung eines Datenschutzbeauftragten entfallen zu lassen oder zumindest den Datenschutzbeauftragten anstatt der Aufsichtsbehörde als dafür zuständige Funktion auszuweisen.

Wie kann ein interner Datenschutzbeauftragter unabhängig sein? Als Angestellter gilt doch eher der Grundsatz: Wes Brot ich ess, des Lied ich sing.
Dr. Claus Ulmer: Gegen eine derartige Wahrnehmung wehre ich mich mit allem Nachdruck. Es gibt in Deutschland ein eindeutiges Datenschutzgesetz, das unsere Aufgaben und Rechte definiert, und an dieses Gesetz sind wir Datenschutzbeauftragte gebunden. Unsere Tätigkeit ist dabei natürlich auch an den Interessen des Unternehmens orientiert. Aber eben nicht nur an diesen, sondern darüber hinaus an den Interessen der von einer Datenverarbeitung betroffenen Personen. Hier gilt es eine für die Beteiligten tragfähige Lösung zu entwickeln.

Unser Rollenverständnis des Datenschutzbeauftragten hat der Entwurf der EU-Datenschutz-Grundverordnung in Ansätzen übernommen. Wie schon angedeutet, ist der Entwurf im Hinblick auf die Ausgestaltung als Kontrollinstanz und die Sicherstellung der zur Arbeit erforderlichen Ressourcen noch nachzubessern. Der Datenschutzbeauftragte muss unmittelbar der Unternehmensleitung unterstellt sein und auch nach Beendigung der Amtszeit ist ein erweiterter Kündigungsschutz zu gewähren, damit der Datenschutzbeauftragte unabhängig agieren und seine Aufgabe als betriebliche Kontrollinstanz wahrnehmen kann.

In Artikel 36 des Entwurfs der EU-Datenschutz-Grundverordnung heißt es: Das Unternehmen stellt sicher, „dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.“ Wie stellt die Deutsche Telekom dies heute schon sicher?
Dr. Claus Ulmer: Bei uns ist über das im Konzern eingeführte „Privacy & Security Assessment-Verfahren“ geregelt, dass wir als Datenschützer gemeinsam mit der IT-Sicherheit zwingend in Entscheidungs- und Entwicklungsprozesse einbezogen werden. Hierzu zählt zum Beispiel die Überprüfung neuer Produkte und Services auf ihre datenschutzrelevanten Aspekte. Erst wenn unsere datenschutzrechtliche Freigabe erteilt wurde, werden solche Projekte mit weiteren Budgets ausgestattet. Um die Freigabeprozesse leisten zu können, ist unsere Abteilung allein in der Zentrale in Bonn über 60 Mitarbeiter stark. Dazu kommen noch die Mitarbeiter, welche vor Ort – also auch an allen Standorten außerhalb von Deutschland – die Umsetzung von Datenschutzmaßnahmen beobachten und bewerten.

Der Entwurf der EU-Datenschutz-Grundverordnung sieht auch vor, dass Datenschutzverletzungen gemeldet werden müssen. Ist eine solche Regelung in Ihrem Sinne?
Dr. Claus Ulmer: Dies ist heute schon in Deutschland geltendes Recht und für uns Pflicht. Es ist zu begrüßen, dass die Regelung in allen Mitgliedsstaaten nun einheitliches Recht werden soll. Aber ich erwarte, dass die EU noch genaue Schwellenwerte festlegt, ab deren Überschreitung ein Unternehmen einen Vorfall melden muss. Ansonsten bleibt dieser Punkt zu allgemein.

Warum ein Schwellenwert? Sollte nicht jede datenschutzrechtliche Verletzung gemeldet werden?
Dr. Claus Ulmer: Wir selbst hinterlegen schon heute unter Beachtung der gesetzlichen Vorgaben im Internet, was alles passiert ist. Es stellt sich aber die Frage, ob weniger hier mehr sein könnte. Erfahrungen aus den USA zeigen, dass eine Ermüdung eintritt, wenn jeder noch so kleine Vorfall gemeldet und veröffentlicht wird. Früher oder später beachtet die Öffentlichkeit dann derartige Vorfälle nicht mehr. Dieser Gefahr einer Abnutzungserscheinung durch Informationsüberflutung müssen wir verantwortungsbewusst begegnen. Der Datenschutz lebt davon, dass er wahrgenommen wird und zu einem Umdenken beitragen kann.

„Die Telekom ist überzeugt davon, dass sie langfristig Wettbewerbsvorteile hat, wenn sie den geforderten Datenschutz achtet und vertrauensbildende Maßnahmen durchführt."

Bringen strenge Datenschutzgesetze unter Umständen auch Wettbewerbsnachteile?
Dr. Claus Ulmer: Die Telekom ist überzeugt davon, dass sie lang-fristig Wettbewerbsvorteile hat, wenn sie den geforderten Datenschutz achtet und vertrauensbildende Maßnahmen durchführt. Im Sinne unseres Leitbilds „Vertrauensräume schaffen" sind wir fest entschlossen, das Vertrauen der Kunden, der Öffentlichkeit und der Mitarbeiter in die Telekom zu stärken und stetig zu verbessern.Laut EU-Verordnung sollen alle Produkte und Dienstleistungen bei ihrer Auslieferung oder ihrer ersten Inanspruchnahme datenschutzfreundlich voreingestellt sein. Es werden dann nur so viele Daten erfasst, verarbeitet und weitergegeben, wie für die Nutzung unbedingt erforderlich ist.

Wie handhabt das die Telekom?
Dr. Claus Ulmer: Wir erfüllen die Forderung schon lange, da in Deutschland das Telekommunikationsgesetz und das Telemediengesetz klare Vorgaben machen. Wir begrüßen, dass Kunden aktiv auf Datenschutzaspekte hingewiesen werden und selbst ihre Bereitschaft zur Datennutzung erklären müssen. Nur dann können sie sich differenziert entscheiden. Ein Beispiel dafür sind die Apps. Schalten Sie die Ortungsdienste auf dem Smartphone aus, dann fragt diejenige App, welche die Lokalisationsdaten benötigt, bei der nächsten Nutzung, ob Sie den Ortungsdienst aktivieren wollen. Das ist praktizierter Datenschutz an einem ganz kleinen Beispiel.

Ein Unternehmen muss Verbraucheranfragen kostenlos und innerhalb eines Monats schriftlich beantworten ...
Dr. Claus Ulmer: ... und wir sind in der Regel sogar schneller als vier Wochen. Wir wollen aber auch das aktive Informieren weiter verbessern. Hierzu bietet uns das Internet zusätzliche Möglichkeiten – etwa mit der Einblendung von Begriffserklärungen. In diesem Zuge wird es auch kommen, dass wir auf das jeweilige Produkt abgestimmte spezifischere Datenschutzhinweise geben werden.

Es soll das Recht auf Löschung von Daten eingeführt werden. Dazu gehört die Pflicht, Dritte über den Löschwunsch zu informieren. Das dürfte der Telekom nicht schmecken.
Dr. Claus Ulmer: Damit haben wir kein Problem, denn auch das machen wir längst. Wenn Kunden zu einem Wettbewerber wechseln, löschen wir seine Daten. Wenn jemand aus dem elektronischen Telefonbuch gelöscht werden will, dann fordern wir beispielsweise auch Google auf, den Eintrag aus dem Cache zu löschen. Schwierig wird es erst dann, wenn der

„Wir erfüllen die Datenschutzanforderungen schon lange, da das Telekommunikationsgesetz und das Telemediengesetz klare Vorgaben machen.“

Anbieter verpflichtet würde, für die komplette Löschung aller Daten zu sorgen. Dies ist in manchen Fällen technisch nicht darstellbar. Hier müssen wirtschaftlich angemessene Anstrengungen ausreichen. Anders bewerte ich allerdings, wenn jemand selbst Einträge im Internet vornimmt. Dann können wir ihn in unserem Verantwortungsbereich zwar unterstützen, aber grundsätzlich bin ich der Meinung, dass sich der Urheber im Übrigen selbst um eine Löschung bemühen muss.

Artikel 20 der EU-Datenschutz-Grundverordnung besagt, dass Unternehmen Verhaltensprofile ihrer Kunden nur nach ihrer ausdrücklichen Zustimmung erstellen dürfen. Schlecht für die Telekom?

Dr. Claus Ulmer: Keineswegs, denn bei uns gibt es die Einwilligungsklausel für Werbe- und Marktforschungszwecke schon lange. Es gibt aber Unternehmen, die Cookies einsetzen, von denen Verbraucher nichts merken. Ein solches Vorgehen ist dann zwar irgendwo in der Datenschutzerklärung erwähnt, aber wer liest sich schon AGBs oder Datenschutzerklärungen durch. Cookies erfassen, auf welchen Seiten sich jemand im Internet bewegt. Anbieter lernen damit Interessen kennen, bringen sie in Zusammenhänge und nutzen das entsprechende Profil dann für gezielte Werbung. Hier sollte aus meiner Sicht mehr Transparenz für den Kunden geboten sein. Die Deutsche Telekom agiert auch in diesem Zusammenhang transparent und kundenfreundlich.

Wie wollen Sie Ihre Kunden konkret mitnehmen auf die Reise?

Dr. Claus Ulmer: Da gibt es viele Möglichkeiten, angefangen bei diesem Bericht zu Datenschutz und Datensicherheit. Eine konkrete Planung möchte ich aber ansprechen. Es fällt den Kunden immer schwerer, sich in der heutigen Online- und Smartphone-Welt zurechtzufinden. Die Datenschutzeinstellungen sind oft mühsam oder gar nicht zu finden oder es kaum zu verstehen, wie sie umgesetzt werden. Wir wollen daher für verschiedene Anwendungsbereiche unseren „Privacy Button“ entwickeln. Für die Anonymisierung von IPv6-Adressen haben wir das schon. Bei Smartphones könnte das etwa eine App sein, die dem Nutzer Kenntnis und – noch wichtiger – Kontrolle über die Datenflüsse gibt.

Einheitlicher Datenschutz für die EU

Die EU-Datenschutz-Grundverordnung soll die 1995 in Kraft getretene Datenschutzrichtlinie ersetzen und das Datenschutzrecht in den EU-Mitgliedsstaaten vereinheitlichen. Die Verordnung wird dann in der gesamten EU unmittelbar geltend und lässt sich durch nationales Recht nicht ändern.

Die Reaktionen auf den im Januar 2012 vorgestellten Entwurf sind unterschiedlich. Der BITKOM begrüßt grundsätzlich die EU-weite Abstimmung der Datenschutzbehörden sowie die geplante Selbstregulierung der Wirtschaft. Der Hightechverband bemängelt aber Vorgaben, deren Umsetzung in den Unternehmen teilweise gar nicht oder nur mit hohem Aufwand machbar wären. Die Bundesregierung fordert Spielräume für eine nationale Ausgestaltung und Öffnungsklauseln. Das Bundesinnenministerium zählt etliche Regelungen auf, die in der EU-Verordnung bisher nicht erwähnt sind, darunter jene zur Videoüberwachung oder zur Datenübermittlung an Auskunfteien.

Dr. Claus Ulmer kommentiert den Entwurf der EU-Datenschutz-Grundverordnung.

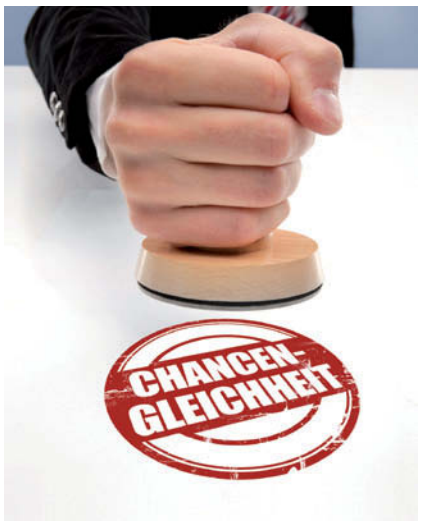
Dr. Claus Ulmer ist seit Juli 2002 Konzernbeauftragter für den Datenschutz des Deutsche Telekom Konzerns. Nach seinem Studium der Rechtswissenschaften in Tübingen und München und der Promotion an der Uni Tübingen war Ulmer von 1993 bis 1999 Rechtsanwalt in einer Stuttgarter Wirtschaftskanzlei mit Schwerpunkten im Arbeitsrecht. Von 1999 bis 2002 war er Syndikusanwalt bei debis Systemhaus und ab Januar 2001 auch Datenschutzbeauftragter. Zwischen August 2001 und Juni 2002 leitete er den Datenschutz von T-Systems International.

Verschärfte Meldepflicht

Telekom erfüllt neue Vorgaben des Telekommunikationsgesetzes bereits seit mehreren Jahren.

Seit März 2012 müssen Telekommunikationsprovider Datenschutzverletzungen auch dann melden, wenn Mitarbeiter Daten unberechtigt löschen oder verändern. Die Aufsichtsbehörden sind über alle Vorfälle dieser Art zu unterrichten. Die Verbraucher müssen von den Fällen erfahren, die zu schwerwiegenden Beeinträchtigungen führen. Mit der zusätzlichen Informationspflicht schafft das Telekommunikationsgesetz (TKG) mehr Transparenz in der TK-Branche. Zuvor mussten Anbieter nur dann informieren, wenn Daten unberechtigt an Dritte gelangten, etwa durch Verlust oder Diebstahl. Mit der Neuregelung geht das TKG nun über die Vorgaben des Bundesdatenschutzgesetzes hinaus. Die Telekom hat die neue Meldepflicht aus dem Stand weg umsetzen können, da sie bereits seit mehreren Jahren freiwillig über Datenvorfälle berichtet.

Transparenz für die TK-Branche.



TKG-Novelle beendet Wettbewerbsnachteile.

Chancengleichheit

Gesetzesnovelle erlaubt weltweite Verarbeitung von Telekommunikationsdaten.

Mit der 2012 in Kraft getretenen Novelle des Telekommunikationsgesetzes (TKG) hat die Bundesregierung eine Vorschrift gestrichen, die Telekommunikationsunternehmen erhebliche Wettbewerbsnachteile brachte: In den zurückliegenden Jahren war die Übermittlung personenbezogener Daten in das EU-Ausland nur in wenigen Ausnahmefällen zulässig. In diesem Punkt ging das TKG weit über das Regelungsniveau des Bundesdatenschutzgesetzes (BDSG) hinaus. Im März 2012 ist die branchenspezifische TKG-Vorschrift weggefallen. Seither gelten die Vorgaben des BDSG nun auch für Telekommunikationsanbieter. Auf diese Weise eröffnen sich ganz neue Betriebsmodelle. Wie andere Unternehmen auch kann die Deutsche Telekom nun zum Beispiel weltweit Partnerunternehmen in die Fernwartung ihrer Systeme einbinden. Indem Servicetechniker auf mehreren Kontinenten zusammenarbeiten, lassen sich 24-Stunden-Dienstleistungen nach dem „Follow-the-Sun-Prinzip“ anbieten. Das bisherige Datenschutzniveau bleibt unangetastet: Die Telekom verpflichtet alle außereuropäischen Partner auf gleich hohe Schutzstandards wie innerhalb von Europa. Ein Absinken des Datenschutzniveaus für die Kunden ist dadurch ausgeschlossen.

Mehr Rechtssicherheit

Bundesnetzagentur veröffentlicht Leitfaden zur Verkehrsdatenspeicherung.

Wie lange dürfen und wie lange sollten Telekommunikationsunternehmen die Verkehrsdaten ihrer Kunden speichern? Belastbare Antworten gibt ein im September 2012 erschienener Leitfaden. Anhand konkreter Empfehlungen zeigen der Bundesdatenschutzbeauftragte und die Bundesnetzagentur darin auf, mit welchen Speicherfristen Anbieter und Verbraucher Rechtssicherheit gewinnen. Neben den klassischen Telekommunikationsdaten behandelt der Leitfaden auch die Verkehrsdaten, die im E-Mail- und Internetverkehr erhoben werden. Anbieter nutzen diese Daten in erster Linie für die Abrechnung mit ihren Kunden und anderen Netzbetreibern. Zudem dürfen die Verkehrsdaten aber auch in das Störungsmanagement eingehen.

Abgestuft nach Datenkategorien und Verwendungszwecken gibt der Leitfaden Empfehlungen, wann es sich anbietet, Verkehrsdaten früher zu löschen, als es das Telekommunikationsgesetz vorschreibt. Die Telekom hält die meisten der empfohlenen Fristen bereits heute ein oder unterschreitet diese (vgl. Infografik). Lediglich an zwei Stellen liegt die Telekom über den Richtwerten der Aufsichtsbehörden, jedoch immer noch innerhalb der gesetzlich vorgegebenen Fristen. In beiden Fällen handelt es sich um Daten, welche die Telekom in anonymisierter Form für externe Serviceprovider vorhält, wenn diese ihren Kunden eine Einwendungsfrist von 180 Tagen gewähren. Im Rahmen der Neuverhandlung der Serviceverträge wird eine Anpassung der Speicherfristen angestrebt.

Vorratsdatenspeicherung – Ende offen

Während die EU-Richtlinie evaluiert wird, ist eine Neuregelung in Deutschland noch nicht absehbar.

Auch im Jahr 2012 hat die Bundesregierung keinen Konsens zur Neuregelung der Vorratsdatenspeicherung gefunden. Aktivitäten waren dagegen auf europäischer Ebene zu verzeichnen: Nach Überprüfung der EU-Richtlinie zur Vorratsdatenspeicherung scheint es Tendenzen zu geben, die Mindestspeicherfrist auf drei Monate abzusenken. Die aktuelle Richtlinie fordert Fristen zwischen sechs und 24 Monaten.

Stillstand in Berlin

In Deutschland herrscht weiterhin politische Uneinigkeit, wie eine gesetzliche Neuregelung ausgestaltet werden soll. 2010 hatte das Bundesverfassungsgericht das damalige Bundesgesetz für verfassungswidrig erklärt. Gegenwärtig werden innerhalb der Bundesregierung zwei unterschiedliche Lösungsansätze diskutiert: Während das Innenministerium eine sechsmonatige Vorratsdatenspeicherung anstrebt, spricht sich das Justizressort für das so genannte Quick-Freeze-Verfahren in Kombination mit einer „kleinen Vorratsdatenspeicherung“ aus. Im Quick-Freeze-Verfahren verhindern Telekommunikationsunternehmen im Einzelfall die vorgesehene Löschung von Verkehrsdaten, wenn eine berechtigte Stelle angezeigt hat, diese Daten innerhalb einer bestimmten Frist abrufen zu wollen. Zudem sollen IP-Adressdaten für sieben Tage anlasslos gespeichert werden.

Deutsche Telekom erfüllt Vorgaben zur Verkehrsdatenspeicherung.

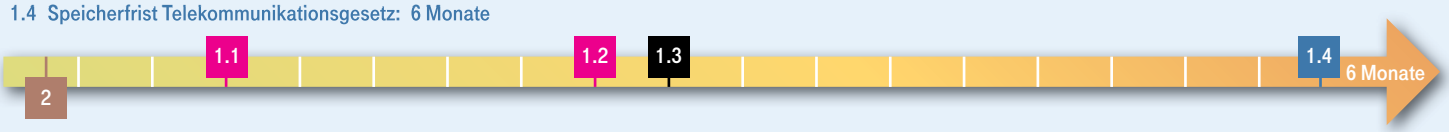
Bereits heute speichert die Deutsche Telekom IP-Adressdaten für sieben Tage, um Malware wirksam bekämpfen zu können. Dies geschieht in Übereinstimmung mit dem Leitfaden zur Verkehrsdatenspeicherung der Bundesnetzagentur. Sollte sich die Bundesregierung erneut für eine sechsmonatige Speicherung entscheiden, ist die Telekom jederzeit in der Lage, zu der bis 2010 gültigen Praxis zurückzukehren.

Klage wegen Nichtumsetzung

Inzwischen hat die Europäische Kommission Deutschland wegen Nichtumsetzung der Richtlinie vor dem Europäischen Gerichtshof verklagt. Im Raum steht eine Strafzahlung von 315.000 Euro pro Tag der Nichtumsetzung, die jedoch erst ab Wirksamkeit eines Urteils fällig wird. Wann das Urteil ergehen wird, war Ende 2012 nicht absehbar.

Datenschutzgerechte Speicherung von Verkehrsdaten.

1. **Abrechnungsdaten außerhalb einer Flatrate**
1.1 **Speicherfrist Telekom:** **bis zu 30 Tage** (falls Kunde auf Einzelverbindungsnachweis verzichtet)
1.2 **Speicherfrist Telekom:** **80 Tage** (falls Kunde Einzelverbindungsnachweis wünscht)
1.3 **Speicherfrist Leitfaden:** **3 Monate**
1.4 Speicherfrist Telekommunikationsgesetz: 6 Monate



2. **IP-Adressen und Standortdaten Mobilfunk** (Ausnahme: standortabhängige Mobilfunktarife)
2.1 Speicherfrist Telekommunikationsgesetz: keine Angabe
2.2 Speicherfrist Leitfaden: 7 Tage
2.3 Speicherfrist Telekom: 7 Tage

Die Deutsche Telekom löscht Verkehrsdaten mitunter schneller, als es das Telekommunikationsgesetz vorschreibt.

10 Tage

Quelle: Deutsche Telekom

Mein Haus im Cyberspace

Neues Internetportal klärt Verbraucher über die Arbeit von Geodatendiensten auf.

Seit September 2012 haben Internetnutzer eine zentrale Anlaufstelle für den Datenschutz bei Geodatendiensten. Hierzu zählen zum Beispiel Angebote wie Google Street View. Auf der Website **www.geodatendienstekodex.de** erfahren Verbraucher, wie die Dienste funktionieren, ob ihr Haus erfasst ist und welche Rechte sie haben. Das neue Informationsangebot geht auf die Arbeit des Vereins Selbstregulierung Informationswirtschaft (SRIW) zurück. Der 2011 gegründete SRIW ist ein Bündnis aus acht führenden Diensteanbietern. Unter ihnen die Deutsche Telekom, die den Verein zu etwa einem Drittel finanziell unterstützt.

Ganz oben auf der Agenda des SRIW steht der Datenschutzkodex für Geodatendienste. Hierin verpflichten sich Anbieter von Geodatendiensten gegenüber den Verbrauchern zu Transparenz, Information und der Möglichkeit zum Widerspruch. Im Kern regelt die Selbstverpflichtung, dass Anbieter bei Widersprüchen das eingesetzte Bildmaterial digital unkenntlich machen. Die Telekom engagiert sich für den Datenkodex, da sie eigene Webangebote mit externen Geodatendiensten vernetzt: Während der Telefonbuchdienst Das Örtliche auf Karten und Bilder von Microsoft Bing Maps verlinkt, nutzt das Portal ImmobilienScout24 den Panoramadienst Google Street View.

Datenschutzkodex für Geodatendienste verpflichtet zu Transparenz und Information.

Dringend erforderlich

Beschäftigtendatenschutz braucht eindeutige gesetzliche Grundlage.

Die Telekom sieht es als dringend an, den Beschäftigtendatenschutz zu reformieren. Die Unternehmen haben sich in puncto Beschäftigtendatenschutz zu lange in einem unklaren Rechtsraum bewegt. Nach der Bespitzelungsaffäre hat sich die Telekom einer strengen Eigenbindung unterworfen. Im Januar 2013 wurde nun nach langem Stillstand des Gesetzgebungsverfahrens ein neuer Gesetzesvorschlag vorgelegt, der noch im Laufe des Jahres 2013 verabschiedet werden könnte.

Der Gesetzesvorschlag greift einige der Forderungen der Telekom auf. So enthält der Entwurf nun erstmalig eine Regelung zur Datenübermittlung in Konzernen und berücksichtigt auch das unternehmerische Bedürfnis, Auftragsdatenverarbeitungsverhältnisse mit Unternehmen in Drittstaaten mit einem anerkannt hohen Datenschutzniveau einzugehen. Dies schont Ressourcen und gibt Rechtssicherheit. Der Gesetzesentwurf verbietet die heimliche Videoüberwachung. Eine offene Videoüberwachung bleibt unter bestimmten Voraussetzungen möglich. Bei der Telekom ist bereits seit Jahren durch eine Konzernbetriebsvereinbarung der Einsatz von Techniken zur verdeckten Videoüberwachung verboten. Ebenso ist der Einsatz von Videoüberwachung zu Qualitätssicherungszwecken bei der Telekom untersagt. Insgesamt wird Videoüberwachungstechnik bei der Telekom nur zur Sicherung von Gebäuden und Liegenschaften genutzt.

Zu modernen und innovativen Kommunikationsformen wie Bring your own Device oder zur Verwendung von privaten Endgeräten für dienstliche Zwecke, finden sich bisher leider keine Regelungen im Gesetzesentwurf. Es bleibt abzuwarten, ob der Gesetzgeber dazu adressierte Anregungen der Telekom noch aufgreifen wird.

Informationelle Selbstbestimmung in der Praxis

Deutsche Telekom führt Datenschutzstandard zum anonymen Surfen unter IPv6 ein.

Zeitgleich zum Rollout des neuen Internetprotokolls IPv6 hat die Telekom eine Datenschutzlösung auf den Markt gebracht, mit der sich IP-Adressen zuverlässig verschleiern lassen. Dabei kann der Nutzer selbst entscheiden, wie weit er die Identität seiner Endgeräte anonymisieren will. Die neue Lösung ist seit September 2012 verfügbar und gilt in der Telekommunikationsbranche als erste ihrer Art.

Das neue Internetprotokoll IPv6 bietet 340 Sextillionen IP-Adressen – genügend, um jedes denkbare Endgerät mit einer eigenen Kennung zu versorgen. Somit wären die technischen Voraussetzungen dafür geschaffen, detaillierte Bewegungs- und Nutzerprofile zu erstellen. Gegen diese Folgen greift der Datenschutzstandard der Telekom. Er umfasst drei Mechanismen, die unterschiedlich stark auf die Nachverfolgbarkeit von IP-Adressen einwirken. Beispielsweise sollen Internetnutzer jederzeit per Mausklick ein neues Präfix für die Geräteadresse ihres Routers anfordern können.

Netzseitig ist die neue Datenschutzlösung bereits voll verfügbar. Nach jeder Verbindungstrennung werden dem Kunden zum Zeitpunkt der Wiedereinwahl ein geänderter IPv6-Präfix und eine neue IPv4-Adresse zugewiesen. Mit den neuen Routern der Speedportserie W 724V haben Telekom-Kunden die Möglichkeit, das anonyme Surfen individuell einzustellen. Die Telekom wird den neuen Datenschutzstandard kontinuierlich weiterentwickeln.

Do-Not-Track-Standard auf 2013 vertagt

Lösung zur technischen Umsetzung der EU-Cookie-Richtlinie noch nicht verfügbar.

Das Ziel, die Arbeit zu Do Not Track bis Mitte 2012 abzuschließen, hat sich als zu ehrgeizig erwiesen. Die Diskussionen rund um einen weltweiten Webtrackingstandard waren zu komplex. Zwar hat sich die zuständige Arbeitsgruppe des World Wide Web Consortium (W3C) auf das technische Design des Standards weitgehend geeinigt: Per Mausklick werden Webnutzer festlegen können, ob sie im Internet verfolgt werden dürfen oder nicht. Doch zeigte sich die eigentliche Herausforderung weiterhin auf regulatorischer Seite. Seit ihrer Gründung im Frühjahr 2011 ringt die Do-Not-Track-Arbeitsgruppe um ein gemeinsames Vorgehen, das den Normen aller Rechtsräume ausreichend Geltung verschafft.

Im Kern geht es darum, die Vorgaben des US-amerikanischen und des europäischen Verbraucherschutzes miteinander in Einklang zu bringen. Ende 2012 hat die Do-Not-Track-Initiative eine neue Taskforce gebildet, um für die Europäische Union zu konkretisieren, wo die obere Grenze des Erlaubten liegen soll. Als einziges deutsches Unternehmen bringt sich die Telekom direkt in die Arbeit der W3C-Arbeitsgruppe ein. Ähnlich wie die EU-Kommission sehen die Telekom-Datenschützer Do Not Track als geeignetes Mittel, um die 2009 erlassene EU-Cookie-Richtlinie wirksam umzusetzen.

EU-Cookie-Richtlinie schnell umsetzen.

Rückendeckung für Smart Metering

Während Deutschland den Datenschutz stärkt, engagiert sich die Europäische Union für mehr Datensicherheit.

Smart Metering gilt als Meilenstein auf dem Weg zum intelligentem Energiemanagement. Wenn fernauslesbare Stromzähler rund um die Uhr aktuelle Verbrauchsdaten liefern, profitieren Stromanbieter und Verbraucher gleichermaßen. Versorger erhalten wertvolle Informationen, um ihre Kapazitäten zu steuern und den Netzbetrieb zuverlässig aufrechtzuerhalten. Kunden haben ihre Energiekosten im Blick und fragen Strom vor allem dann nach, wenn er am günstigsten ist.

Datenschutz beim Verbraucher

Beim Smart Metering entstehen personenbezogene Verbrauchsdaten. Somit gilt das Bundesdatenschutzgesetz. Um den Datenschutz zusätzlich zu stärken, hat die Bundesregierung das Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragt, ein Schutzprofil und eine technische Richtlinie zu erstellen. Während das Schutzprofil seit November 2011 vorliegt, kommt die Richtlinie voraussichtlich Anfang 2013.

Das BSI richtet seinen Blick auf die an den Zähler angeschlossene Steuereinheit. Als zentrale Kommunikationsdrehscheibe zwischen Stromzähler und Smart-Metering.Anbieter soll die Steuereinheit zum sicheren Datenhalter werden. Das Profil nennt Anforderungen für eine Gerätearchitektur, die ein hohes Maß an

Smart Metering braucht ein Schutzprofil.

Datenschutz sicherstellt. Beispielsweise muss die Steuereinheit die Verbrauchsdaten verschlüsseln und signieren können, um unberechtigte Zugriffe zu verhindern. Die Anforderungen reichen bis zur Bauweise des Übertragungsgeräts, um auch gegen physische Attacken oder Manipulation von außen gewappnet zu sein.

Datensicherheit im Netzbetrieb

Während sich Deutschland auf den Datenschutz in der Steuereinheit konzentriert, hat die Europäische Union eine Initiative gestartet, welche die Datensicherheit im Betrieb der Stromnetze stärken soll. 2012 hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) eine Arbeitsgruppe gebildet, in der sie gemeinsam mit Wirtschaftsvertretern, unter ihnen die Deutsche Telekom, Empfehlungen für eine ausreichende Datensicherheit erstellt.

Die Empfehlungen zeigen auf, welchen Einfluss Datensicherheit auf die Stabilität der Stromproduktion hat und welche Mindeststandards zukünftige Smart-Grid-Anbieter einhalten sollten. So gilt es zum Beispiel wirksam auszuschließen, dass Angreifer falsche Verbrauchsdaten in die Netze melden, um Betreiber zu einer Fehleinschätzung der aktuellen Netzlast zu bringen. Ende 2012 lag ein erster Entwurf der Datensicherheitsempfehlungen vor. 2013 wird die ENISA ihre Grundlagenarbeit abgeschlossen haben.

Smart Metering
Datensparsamkeit und Datenschutz bilden wichtige Grundsätze für das Smart Metering.

Vertrauensvorsprung in der Bevölkerung

Die Telekom genießt große Vertrauenswürdigkeit im Umgang mit persönlichen Daten.

„Welche Unternehmen halten Sie für vertrauenswürdig, wenn es um den Umgang mit persönlichen Daten geht?“ Bei dieser Frage einer repräsentativen Allensbach-Umfrage landete die Telekom unter den IT- und Telekommunikationsunternehmen mit großem Abstand auf Platz eins. 45 Prozent der Befragten halten die Telekom für vertrauenswürdig. Das zweitplatzierte Unternehmen erreicht nur 27 Prozent. Die Telekom nimmt in allen Altersgruppen den Spitzenplatz ein, genießt aber mit 57 Prozent vor allem bei den über 60-Jährigen einen besonders großen Vertrauensbonus. Das Institut für Demoskopie Allensbach hatte die repräsentative Befragung im Rahmen des Sicherheitsreports im Juni 2012 durchgeführt.

Externe Beratung gewünscht

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 zum Umgang mit Kunden- und Mitarbeiterdaten ebenso wie mit der IT-Sicherheit und der Angemessenheit ergriffener Maßnahmen. Weitere Themen sind 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 auch um die Bewertung von datenschutzrelevanten Prozessen im Konzern bitten. Weiterhin greift der Beirat eigenständig Datenschutz- und Datensicherheitsmaßnahmen auf und erarbeitet entsprechende Vorschläge oder Empfehlungen für den Vorstand der Telekom.

Im Jahr 2012 kam der Datenschutzbeirat zu fünf Sitzungen zusammen. Wichtige Themen umfassten die Bewertung von Datenschutz- und Sicherheitsaspekten neuer Cloud-Anwendungen ebenso wie die Entwicklung in den Wachstumsfeldern Energie und vernetztes Fahrzeug. Der Beirat befasste sich zudem mit dem Entwurf der EU-Datenschutz-Grundverordnung und den zu erwartenden Auswirkungen auf die Deutsche Telekom. Ferner beriet der Beirat über die Auswertung von Entertain-Nutzungsdaten und informierte sich über die Ergebnisse des Basisdatenschutzaudits und das erreichte Datenschutzniveau im Konzern.

Die aktuellen Mitglieder des Datenschutzbeirats:

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

Peter Franck, Mitglied des Vorstands, Chaos Computer Club (CCC)

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

Professor Peter Gola, Vorsitzender des Vorstands der Gesellschaft für Datenschutz und Datensicherheit (GDD)

Bernd H. Harder, Rechtsanwalt, Mitglied des Hauptvorstands des BITKOM e. V., Lehrbeauftragter an der Hochschule der Medien Stuttgart und an der Technischen Universität München (TMU)

Dr. Konstantin von Notz, Bündnis 90/Die Grünen, MdB, Mitglied des Innenausschusses und stellvertretendes Mitglied des Rechtsausschusses und des Unterausschusses Neue Medien, Obmann der Enquetekommission „Internet und digitale Gesellschaft“

Gisela Piltz, MdB, stellvertretende Fraktionsvorsitzende der FDP-Bundestagsfraktion

Gerold Reichenbach, SPD, MdB, Mitglied im Innenausschuss (Berichterstatter für Datenschutz sowie Bevölkerungsschutz und Katastrophenhilfe) und Mitglied im Unterausschuss Bürgerschaftliches Engagement, stellvertretender Vorsitzender der Enquetekommission „Internet und digitale Gesellschaft“

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

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

Halina Wawzyniak, Die Linke, MdB, stellvertretende Parteivorsitzende, Obfrau der Enquetekommission „Internet und digitale Gesellschaft“

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

Vertrauen erarbeitet

Wie in kaum einer anderen Branche muss der Datenschutz in den Unternehmen der Informations-, Telekommunikations- und Medienindustrie eine bedeutende Rolle einnehmen. Dies gilt vor allem dann, wenn die Verarbeitung von Kundendaten ein wesentlicher Bestandteil ihrer Geschäftsmodelle ist. So verfügt die Deutsche Telekom über Daten, mit wem Kunden wie lange telefonieren, welche Filme sie über den Onlinevideoshop Videoload ansehen oder wie sie den Musik-Streamingdienst Spotify nutzen. Auch durch das Cloud Computing entstehen neue Bereiche, in denen die Telekom als Cloud-Anbieter Daten ihrer Kunden erhält und verarbeitet. Dies gilt auch für die Daten, die T-Systems als Auftragsdatenverarbeiter für Unternehmen in ihren Rechenzentren speichert. Hinzu kommen auch die persönlichen Informationen über rund 230.000 Mitarbeiterinnen und Mitarbeiter des Konzerns.

Allein die Aufgabe der Sicherung und des Schutzes der Daten aus Vertragsverhältnissen von über 150 Millionen Anschlüssen ist gewaltig. Die Dimension und Sensibilität dieser verfügbaren Daten verlangen danach, den Schutz der Persönlichkeitsrechte wichtiger zu nehmen als alles andere. Die Telekom muss die personenbezogenen Daten mit allen Möglichkeiten der Technik, dem Know-how ihrer Mitarbeiter und mit dem Rat von externen Spezialisten gegen Zugriffe von außen und vor Missbrauch schützen. Dies stellt in einer zunehmend vernetzten Wirtschaft eine essenzielle Voraussetzung für den Geschäftserfolg dar.

Sich dem Urteil einer kritischen Fachöffentlichkeit zu stellen, bedeutet einen wichtigen Schritt und zeigt, dass Datenschutz bei der Telekom mehr ist als nur ein Lippenbekenntnis. Besonders dem Datenschutzbeirat kommt hier eine wichtige Rolle als externer Beobachter und Ratgeber zu. Dazu gehört auch, dass die Telekom als einer der ersten internationalen Konzerne den Bereich „Datenschutz und Compliance“ auf Vorstandsebene gehoben hat. Alle Maßnahmen dienen der Vertrauensbildung: gegenüber den Kunden, den Mitarbeiterinnen und Mitarbeitern sowie den privaten und öffentlichen Teilhabern am Konzern.

Die Zusammensetzung des Datenschutzbeirats repräsentiert die politische Meinungsvielfalt in Deutschland, aber auch fachliches Know-how der verschiedenen Aspekte des Datenschutzes und der Datensicherheit. Er unterzieht Geschäftsmodellen regelmäßig einem neutralen und kritischen Blick – teilweise sogar bis auf die Ebene von einzelnen Produkten und Dienstleistungen. Es kommen also alle aktuellen datenschutzrelevanten Entwicklungen im Unternehmen auf den Tisch. Die Telekom profitiert so von den Erfahrungen der Mitglieder des Datenschutzbeirats.

Längst spielt das Nacharbeiten von Datenschutzskandalen keine Rolle mehr in den Sitzungen des Datenschutzbeirats. Das Augenmerk richtet sich heute vielmehr auf die vorausschauende Gestaltung des Schutzes der Persönlichkeitsrechte. Mehr und mehr beschäftigen den Datenschutzbeirat konzerninterne Prozesse. Besondere Aufmerksamkeit liegt auch auf den neuen Geschäftsfeldern wie etwas Gesundheit, Energie oder vernetztes Automobil. Hier werden zukünftig personenbezogene Daten in einem noch nicht gekannten Umfang anfallen, die es zu schützen gilt. Bei diesen Anstrengungen unterstützt der Datenschutzbeirat die Telekom.

Alle Maßnahmen, welche die Telekom in den vergangenen vier Jahren rund um den Datenschutz aufgesetzt und umgesetzt hat, haben den Konzern bemerkenswert positiv verändert. Heute gilt die Telekom als Vorreiter in Sachen Datenschutz und Datensicherheit – was sich auch in konkreten Zahlen niederschlägt. 45 Prozent der Bevölkerung halten die Telekom laut einer repräsentativen Umfrage der Demoskopen von Allensbach für vertrauenswürdig, wenn es um den Umgang mit persönlichen Daten geht. Eine erstaunlich hoher Wert, wenn man bedenkt, dass wir es in der Informations-, Telekommunikations- und Medienbranche mit derart vielen persönlichen Daten zu tun haben. Der Blick auf den Wettbewerb untermauert das deutlich: In der Allensbach-Umfrage folgt der nächste Wettbewerber mit 20 Prozentpunkten Abstand.

Die Deutsche Telekom hat dieses Vertrauen nach einem Tief hart erarbeitet und will es in Zukunft nicht nur wahren, sondern weiter ausbauen. Deswegen bleiben wir als Datenschutzbeirat nah dran an der Entwicklung und fragen lieber zweimal, welche Konsequenzen ein Verhalten oder ein Angebot für den Schutz der Persönlichkeitsrechte hat. Weder das hohe Maß an Sensibilität noch die Schamgrenze für Missbrauch dürfen sinken. Auch nicht beim Schutz der Mitarbeiterdaten.

Ein Datenschutzbeirat ist aber auch für andere Unternehmen geeignet. Vor allem dann, wenn die Verarbeitung von Kundendaten ein wesentlicher Bestandteil der Geschäftsmodelle ist. Für diese Unternehmen sollte ein Datenschutzbeirat gewissermaßen „Best Practice“ sein. Er stellt keine Hürde dar, sondern öffnet die Augen, welche ansonsten den Kunden selbst zu einem späteren Zeitpunkt mit möglicherweise negativen Folgen aufgehen werden. Grundsätzlich kann ich anderen Unternehmen daher nur empfehlen: Denken Sie über einen Datenschutzbeirat nach.

Zur Person

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

Moment mal!

Wer Datenschutz und -sicherheit ganzheitlich angehen will, muss auch die eigene Belegschaft informieren und schulen. 2012 hat die Telekom wieder mehrere Informationskampagnen gestartet.

Meist tun Beschäftigte es unbewusst und nur in seltenen Fällen mit krimineller Energie. Sie öffnen externen Angreifern die digitale Tür oder halten sich nicht an Sicherheitsvorschriften. Daher sollten Unternehmen Mitarbeiter aktiv in den Prozess einer wirksamen Sicherheitskultur einbeziehen. Nur dann lassen sich Informationssicherheit und Datenschutz gewährleisten. Das fängt mit der Sensibilisierung für mögliche Datensicherheits- und Datenschutzrisiken an. Damit die Materie nicht zu trocken ist, hat die Telekom im Jahr 2012 neben den üblichen Onlineportalen und Schulungen auch eine „Werbekampagne" sowie spielerische und ganz praktische Mittel zur Aufklärung eingesetzt.

Informationsschutz im Handumdrehen

Viele Mitarbeiter der Telekom haben täglich mit geschäftlichen oder personenbezogenen Daten und Informationen zu tun. Welche Daten dabei wie vertraulich zu behandeln sind oder welche Daten der Datenschutzgesetzgebung unterliegen, ist für die Beschäftigten häufig nicht so einfach einzuordnen. Die Telekom teilt personenbezogene Daten in fünf Datenschutzklassen ein, geschäftliche Informationen kategorisiert sie in vier Vertraulichkeitsklassen – von „Offen" bis „Streng vertraulich".

Durchblick bringt jetzt eine klar strukturierte Informationsdrehscheibe, ähnlich einer Parkscheibe. Auf deren Basis können Mitarbeiter Informationen und Daten schnell korrekt klassifizieren, ohne sich mit exakten Begriffsdefinitionen auskennen zu müssen. Sie erfassen sofort, welcher Schutzbedarf vorliegt und welche Schutzmaßnahmen sie dementsprechend anwenden müssen. Neben einer Papierversion gibt es eine elektronische Variante, die jeder Mitarbeiter an seinem PC-Arbeitsplatz aufrufen kann. Im nächsten Schritt soll 2013 eine Smartphone-App realisiert werden.

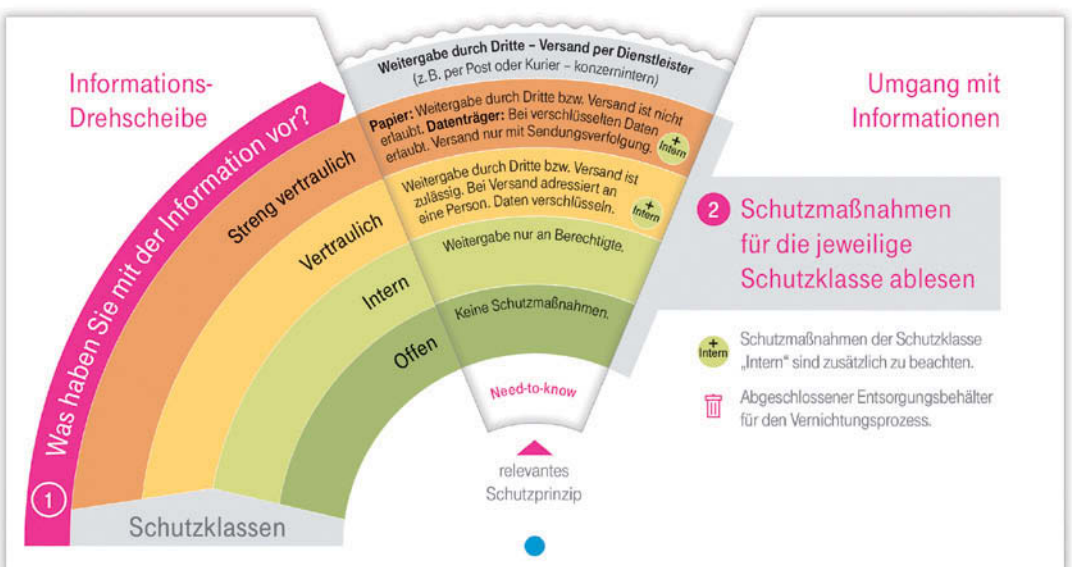
Dazu hat die Telekom eine Reihe von Informationsblättern entwickelt, die einzelne Sicherheitsregeln kurz und verständlich erklären. So gibt es etwa Übersichten über den sicheren Umgang mit Smartphones oder externe Besprechungen. Die Themen und Inhalte sind dabei auf die unterschiedlichen Zielgruppen zugeschnitten: zum Beispiel auf Mitarbeiter eines Teams, Führungskräfte oder Leiter einer Organisationseinheit. Ganz ohne klare Vorschriften geht es aber trotzdem nicht: Alle Beschäftigten der Telekom werden alle zwei Jahre auf die Beachtung des Daten- und Informationsschutzes verpflichtet.

Kampagne gegen Social Engineering

Eine besonders geschickte Methode, um an vertrauliche Daten und Informationen über ein Unternehmen zu kommen, ist Social Engineering. Dabei täuscht der Angreifer einem Mitarbeiter eine falsche Identität vor. Ein Beispiel für Social Engineering sind fingierte Telefonanrufe eines angeblichen Technikers, der vertrauliche Zugangsdaten benötigt. Zu einer elektronischen Variante des Social Engineerings zählt Phishing. Ein typisches Beispiel hierfür ist das Ausspähen von PIN und TAN im Onlinebanking.

Für die Telekom bedeutet Social Engineering ein großes Gefahrenpotenzial, da alle Mitarbeiter davon betroffen sein können. Daher ist die Sensibilisierung der Beschäftigten einer der wichtigsten Schritte zur Wahrung von Informationssicherheit und Datenschutz. Zur Abwehr müssen Mitarbeiter die Angriffsmechanismen theoretisch verstehen und das Abwehrverhalten praktisch üben. Denn Social Engineering setzt auf grundlegende angeborene Mechanismen der menschlichen Informationsverarbeitung und auf emotional gesteuertes, unreflektiertes Handeln. Wer will dem freundlichen Techniker schon den Zugang in sein Büro verweigern, wenn er doch nur einen Fehler beseitigen will? In solchen Situationen müssen Mitarbeiter lernen, sich Zeit zu nehmen, nachzudenken und richtig zu reagieren.

Die Telekom startete 2012 die unternehmensinterne Kampagne „Moment mal". Ziel war es, den Mitarbeitern das richtige Bauchgefühl für bedrohliche Situationen zu vermitteln. Die Botschaften: Ich lass mich nicht unter Druck setzen, nicht täuschen und nicht einwickeln. Die Kampagne, die 2013 fortgesetzt wird, setzt auf einen Medienmix: unter anderem mit einem Audioclip, einem interaktiven Film, einem Typentest, einem Team- und Brettspiel sowie einem Gewinnspiel.



Schutz der Grundrechte

Interview mit **Professor Hansjörg Geiger**, Mitglied des Datenschutzbeirats der Deutschen Telekom.

Herr Professor Geiger, was kommt 2013 auf die Datenschützer zu?
Prof. Hansjörg Geiger: Das zentrale Thema wird die europäische Datenschutzverordnung sein. Der vorliegende Vorschlag der EU-Kommission weist grundsätzlich in die richtige Richtung, fordert jedoch gerade die deutsche Seite auf, sich intensiv in die weitere Diskussion einzuschalten.

Warum gerade Deutschland?
Prof. Hansjörg Geiger: Es geht um den Erhalt unseres hohen Schutzniveaus. Datenschutz zählt hierzulande zu den Grundrechten. Auch aus internationaler Sicht gelten die einschlägigen Entscheidungen des Bundesverfassungsgerichts als echte Errungenschaften. Hiermit meine ich das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Letzteres klingt für Nichtjuristen wahrscheinlich recht sperrig, meint im Kern aber, dass niemand ohne richterliche Anordnung in ein Computer- oder Telekommunikationssystem eindringen darf.

Stehen diese Grundrechte nun wieder zur Disposition?
Prof. Hansjörg Geiger: Wenn Deutschland nicht achtgibt, läuft die Entwicklung zumindest teilweise darauf hinaus. Aufgrund ihrer Rechtsform wird die europäische Datenschutzverordnung unmittelbar geltendes Recht in allen Mitgliedsländern. Dies würde die Spielräume für das deutsche Modell mit seinen vielen bereichsspezifischen Regelungen stark einengen. Deutsche Standards, die über die europäische Grundordnung hinausgehen, hätten keine rechtliche Basis mehr.

„Es geht um nichts weniger als den Erhalt des hohen Datenschutzniveaus in Deutschland."

Werden die deutschen Interessen bereits ausreichend vertreten?
Prof. Hansjörg Geiger: Ob das deutsche Engagement ausreicht, kann nur das weitere Gesetzgebungsverfahren zeigen. Tatsache ist aber, dass Bundesregierung, Opposition und Wirtschaft bereits sehr aktiv sind. So haben etwa die Bundestagsfraktionen von CDU/CSU und FDP sowie die Fraktion der SPD detaillierte Anträge vorgelegt, in denen sie sehr konkret aufzeigen, bei welchen Fragen noch Klärungsbedarf besteht.

Beispielsweise fordern die Antragssteller, dass sich die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nicht nur auf Großunternehmen beschränken darf, sondern auch für Mittelständler gelten soll. Eine andere Forderung betrifft den Umgang mit sensiblen Daten. Hierunter fallen besonders schützenswerte Daten wie zum Beispiel Religionszugehörigkeit oder Mitgliedschaft in einer Gewerkschaft. Da wir davon ausgehen müssen, dass sich unsere gesellschaftlichen Schutzvorstellungen zukünftig weiter verändern werden, sollte der Katalog sensibler Daten nicht abschließend formuliert sein.

Ist bereits erkennbar, ob sich die EU auf diese Forderungen zubewegt?
Prof. Hansjörg Geiger: Der aktuelle Entwurf zeigt einige Verbesserungen, doch wird das deutsche Schutzniveau nicht erreicht. Vor uns liegt daher noch eine Menge Arbeit. Vor allem in der ersten Jahreshälfte. Schließlich verfolgen Kommission und das Europäische Parlament das ehrgeizige Ziel, die Beratungen bis Mitte 2013 abzuschließen.

Sollte sich die Telekommunikationswirtschaft besonders intensiv an der Diskussion beteiligen?
Prof. Hansjörg Geiger: Sie tut es längst. Und das aus gutem Grund. Datenschutz made in Germany gilt auf vielen Märkten als Wettbewerbsvorteil. Würde die neue EU-Verordnung das hiesige Schutzniveau nicht ausreichend abbilden, bliebe nur noch der Ausweg über eine Öffnungsklausel, welche Deutschland die Möglichkeit gäbe, strengere Standards hinzuzufügen. Solche Alleingänge können allerdings nicht im Sinne unserer Volkswirtschaft sein. Zumal eines der vorrangigen Ziele der neuen EU-Verordnung ja gerade darin besteht, die regulatorischen Schieflagen innerhalb Europas auszugleichen. Vor diesem Hintergrund erwarte ich für das Jahr 2013 eine spannende Diskussion.

Professor Hansjörg Geiger beschäftigt sich mit dem Thema Datenschutz seit Anfang der 70er-Jahre. Sein beruflicher und akademischer Werdegang umfasst zahlreiche Stationen in Wirtschaft, Forschung, Justiz und Politik. Professor Geiger war unter anderem als freier Wissenschaftler bei Siemens, als Staatsanwalt und Richter am Amtsgericht München, als Referatsleiter beim Bayerischen Landesbeauftragten für den Datenschutz, als Staatssekretär im Bundesministerium der Justiz, als Präsident des Bundesamtes für Verfassungsschutz und als Präsident des Bundesnachrichtendienstes tätig.

Risiken verlagern

Überzogene Panikmache oder höchste Eisenbahn? Diese Frage stellen sich Wolfgang Ischinger, Leiter der Münchner Sicherheitskonferenz, und der Vorstandsvorsitzende der Deutschen Telekom, René Obermann, für das Thema Cyberkrieg nicht. Für beide steht fest: Es ist Zeit, zu handeln.

Wolfgang Ischinger, Leiter der Münchner Sicherheitskonferenz.

Wolfgang Ischinger hat im Mai 2008 den Vorsitz der Münchner Sicherheitskonferenz übernommen. Der Jurist und Völkerrechtler war zuvor von 1975 bis 2008 mit zahlreichen Aufgaben als Spitzendiplomat im Auswärtigen Amt der Bundesrepublik Deutschland betraut. Unter anderem war Ischinger an den deutschen Botschaften in Washington, D.C., Paris und London tätig sowie als Ministerialdirektor, Leiter der Politischen Abteilung sowie Staatssekretär des Auswärtigen Amtes. Er leitete die deutschen Delegationen bei den Bosnien-Friedensverhandlungen und war zudem Repräsentant der Europäischen Union in den Troikaverhandlungen über den Status des Kosovo.

Vor zwei Jahren setzte der ehemalige deutsche Botschafter in Großbritannien und den USA zum ersten Mal das Thema Cybersicherheit auf die Agenda der Münchner Sicherheitskonferenz. Das Interesse der Führungskräfte aus Wirtschaft, Politik und Wissenschaft war so groß, dass Wolfgang Ischinger im September 2012 gemeinsam mit René Obermann erstmals zu einem separaten Cyber-Security-Gipfel nach Bonn einlud. 50 Führungskräfte sollten teilnehmen. Am Ende diskutierten rund 80 Topmanager über Cyberkrieg und IT-Sicherheit.

Herr Ischinger, warum braucht das Thema Cybersicherheit eine eigene Konferenz?
Wolfgang Ischinger: Weil Wirtschaft und Staat zunehmend aus dem Internet angegriffen werden. Damit entwickelt sich ein völlig neuer Bedrohungstypus, der eigenen Gesetzen folgt und ganz andere Sicherheits- und Abwehrmaßnahmen erfordert. Dies scheint vielen aber noch nicht bewusst zu sein. Zwar wissen IT-Experten einiges über die Risiken aus dem Netz, aber ob Unternehmenschefs die entsprechenden Gefahren wirklich wahrnehmen und richtig bewerten, daran bestehen durchaus Zweifel. Wir müssen dies also zu einem strategischen Thema für Chefetagen entwickeln. Und dazu trägt ein hochrangig besetzter eigener Cybersicherheitsgipfel deutlich bei.

Aber die Gefahren enden nicht an Unternehmens- oder Ländergrenzen.
Wolfgang Ischinger: Wir stehen immer mehr genuinen transnationalen globalen Herausforderungen gegenüber, denen Staaten und selbst Staatengruppen kaum mehr etwas entgegensetzen können. Dazu zählen etwa Naturkatastrophen. Kein Phänomen ist transnationaler als der Cyberspace. Aber genau in diesem Feld sind wir auf internationaler Ebene von tragfähigen Regelungen und Abkommen weit entfernt. Es gibt null internationale Handlungsfähigkeit! Daher sind hier auf nationaler und internationaler Ebene Fortschritte dringend erwünscht und nötig. Zumal sich Cybersicherheit zu einer Standortfrage entwickelt. Ohne Zweifel werden die gut vorbereiteten Staaten weltweit einen besseren Ruf genießen als diejenigen Staaten, die nichts gegen den Cyberkrieg tun.

Herr Obermann, wie ernst schätzen Sie die Lage denn ein?
René Obermann: Organisierte Kriminalität und Wirtschaftsspionage mithilfe des Netzes sind

sich ins Netz

René Obermann, Vorstandsvorsitzender der Deutschen Telekom.

kein Stoff mehr für Science-Fiction-Filme. Praktisch alle Bereiche des öffentlichen und privaten Lebens hängen heute von funktionierenden Telekommunikations- und IT-Infrastrukturen ab. Das heißt, nicht nur ein Unternehmen, sondern ein ganzer Standort kann von Cyberangriffen betroffen sein. Gesteuerte Angriffe aus dem Netz können gravierende Folgen haben, etwa Stromnetze und Finanzmärkte lahmlegen. Ein Beispiel erlebte die USA Ende 2011, als Betreiber von Erdgaspipelines monatelang mit Phishingattacken angegriffen wurden. Ein Klick auf einen der bösartigen Links hätte ausgereicht, dass sich Malware von selbst in den Systemen installiert. Dann wären die Täter unter anderem in der Lage gewesen, Systeme zur Kontrolle von Gaskompressoren zu manipulieren.

Wie sollte eine angemessene Reaktion auf die digitale Bedrohungslage aussehen?

Wolfgang Ischinger: Die Zeit ist vorbei, in der sich jeder allein gegen Viren, Würmer und Trojaner zur Wehr setzen konnte. Wir erleben eine zunehmende Professionalisierung der Cyberangriffe. Hobbyangreifer lassen sich noch mit technischen Mitteln abwehren. Aber hier ist inzwischen ein neuer Industriezweig entstanden. Hauptberufliche Cyberkriminelle entwickeln im Auftrag von Unternehmen und Staaten Cyberwaffen, mit denen sie Ziele attackieren. Dies zeigen Trojaner wie Stuxnet, den offenbar eine staatliche Stelle in Auftrag gegeben hat. Es geht also nicht mehr nur darum, ein bisschen Schaden anzurichten oder jemanden zu ärgern. Die Gefahr hat deutlich zugenommen, dass sich Staaten unter anderem mit ihren Geheimdiensten in einen Cyberkrieg begeben.

Der aber immer nur lokal stattfinden würde, da nur einzelne Computer angegriffen werden können?

René Obermann: Nein, denn längst ist alles, was eine IP-Adresse hat, miteinander vernetzt. Damit steigt das Risiko, dass kritische Infrastrukturen einer Region oder gar eines Staates ausgeschaltet werden. Es gab bereits Angriffsversuche auf Atomkraftwerke. Nicht auszudenken wäre es zum Beispiel, wenn Cyber-Kriminelle Steuerungssysteme eines Kraftwerks manipulieren würden. Auch die Bundesregierung registriert immer häufiger Attacken auf ihr Regierungsnetz. Wer es nicht auf reines Ausschalten von Rechnern abgesehen hat, könnte Katastrophen auslösen – schon

René Obermann ist seit 2006 Vorstandsvorsitzender der Deutschen Telekom AG. Zuvor war Obermann sowohl Vorstandsvorsitzender der T-Mobile International AG & Co. KG als auch Konzernvorstand für den Bereich Mobilfunk. Begonnen hat seine berufliche Karriere mit einer kaufmännischen Ausbildung bei der BMW AG in München. Danach gründete er 1986 das eigene Unternehmen ABC Telekom, an dem sich 1991 der Mischkonzern Hutchison Whampoa aus Hongkong beteiligte. Die daraus entstandene Hutchison Mobilfunk GmbH führte Obermann als geschäftsführender Gesellschafter und dann als Vorsitzender der Geschäftsführung.

heute. Würden etwa gefälschte Hard- und Softwarekomponenten in einen Flugzeugtyp eingebaut, wäre es möglich, Maschinen einer ganzen Baureihe aus der Ferne zu lenken.

Aber direkt von Cyberwar zu sprechen, scheint etwas übertrieben.
Wolfgang Ischinger: Das sehen wir anders. Kritisch wird es dann, wenn eine Cyberattacke so viel zerstören würde, dass Regierungen sich gezwungen sehen müssten, militärisch zu reagieren. In den USA oder der NATO befasst man sich in Strategiepapieren längst mit dieser Frage.

Dann spricht vieles dafür, die Vernetzung zu stoppen?
Wolfgang Ischinger: Die Vernetzung lässt sich nicht mehr aufhalten. Dabei nehmen wir die Risiken bewusst in Kauf, denn für Unternehmen und Regierungen sind die Vorteile des Netzes völlig unbestritten. Sie garantieren Zugang zu Märkten sowie Innovationen und damit zu Wirtschaftswachstum. Eine globale Wirtschaft lässt sich nur noch bewältigen, wenn wir vernetzt arbeiten, handeln und leben. Oder wollen Sie ernsthaft vorschlagen, dass wir Smartphones oder Tablet-PCs wieder abschaffen und das Rad der Geschichte zurückdrehen?

Unternehmen wie die Telekom tragen zur zunehmenden Vernetzung der Gesellschaft bei. Sind wir auf dem richtigen Weg?
René Obermann: Trotz aller unbestreitbaren Sicherheitsrisiken muss es weitergehen mit der Vernetzung. Wir müssen aber noch besser lernen, mit den neuen Risiken richtig umzugehen. Sie Schritt für Schritt auf ein Minimum zu verringern – wohl wissend, dass wir niemals zu hundert Prozent sicher sein können.

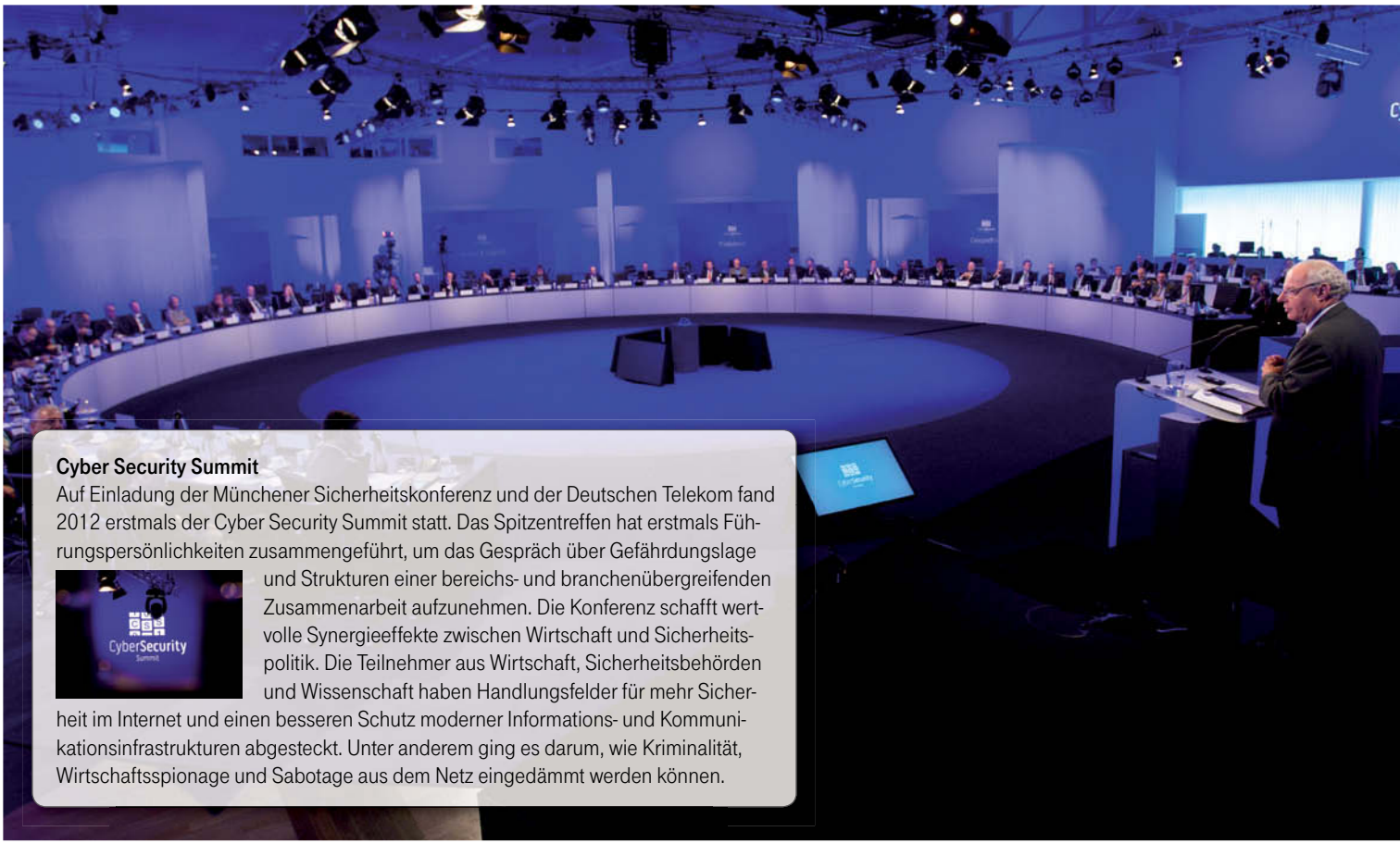
Sie haben Geschäftsfelder aufgebaut, welche die intelligente Vernetzung vorantreiben. Welche Rolle spielen hier Sicherheit und Datenschutz?
René Obermann: Sie meinen damit die Bereiche Energie, Gesundheit und Auto. In diesen Branchen steht Sicherheit aus unterschiedlichen Gründen ganz oben auf der Agenda. Die Energiebranche steckt mitten in einer Umbruchphase, unter anderem ausgelöst durch die Energiewende. Die Stromnetze brauchen mehr Intelligenz, damit sich die Stromeinspeisung aus Tausenden Fotovoltaikanlagen und Windrädern managen lässt. Damit entsteht neben dem Transportnetz für Strom ein Datennetz, in dem Informationen zwischen den Erzeugern und Verbrauchern ausgetauscht werden. Diese Netze und Daten müssen wir sichern. Schließlich handelt es sich um eine kritische Infrastruktur.

Und wie sieht es im Gesundheitswesen aus?
René Obermann: Hier ist der Datenschutz von besonders großer Bedeutung. Er wird gern als Argument gegen Vernetzung angeführt. Die Gesundheitsbranche tut sich daher noch schwer, die Vorteile der Vernetzung für sich zu nutzen. Ob Patientendaten aber in Hängeregistern oder in oft spärlich gesicherten Praxisinformationssystemen besser aufgehoben sind, möchte ich bezweifeln. Da wir das Telekommunikations-, Medien- und Datenschutzgesetz täglich umsetzen, haben wir vielfältige Erfahrungen mit dem Datenschutz gesammelt, und wissen daher auch, wie sich das im Gesundheitswesen lösen lässt.

Wie lässt sich denn mit dem Thema Cybersicherheit angemessen umgehen?
Wolfgang Ischinger: Der Kampf gegen Cybergefahren lässt sich nur gemeinsam gewinnen. Daher halte ich es aus sicherheitspolitischer Sicht für sehr wichtig, eine Informationssammelstelle einzurichten. Viele Unternehmen verschweigen Hackerangriffe immer noch. Sie befürchten einen Imageschaden, wenn alle Welt erfährt, dass sie Ziel von Cyberangriffen waren. Wenn sie aber ihre Erkenntnisse weitergeben, dann helfen sie anderen, sich besser zu schützen. Umgekehrt hilft es ihnen auch.

Munich Security Conference msc
Münchner Sicherheitskonferenz

Münchner Sicherheitskonferenz
Die Münchner Sicherheitskonferenz ist das wichtigste unabhängige Forum zum Gedankenaustausch von Entscheidungsträgern der internationalen Sicherheitspolitik. Jedes Jahr bietet sie hochrangigen Teilnehmern aus aller Welt ein Forum zur intensiven Diskussion der aktuellen und zukünftigen sicherheitspolitischen Herausforderungen. Die Münchner Sicherheitskonferenz erörtert und analysiert aktuelle sicherheitspolitische Herausforderungen und greift Themen der Zukunft auf. Dazu gehört auch die Erweiterung um Themen wie Sicherheit in einer digitalen vernetzten Welt.



Cyber Security Summit
Auf Einladung der Münchener Sicherheitskonferenz und der Deutschen Telekom fand 2012 erstmals der Cyber Security Summit statt. Das Spitzentreffen hat erstmals Führungspersönlichkeiten zusammengeführt, um das Gespräch über Gefährdungslage und Strukturen einer bereichs- und branchenübergreifenden Zusammenarbeit aufzunehmen. Die Konferenz schafft wertvolle Synergieeffekte zwischen Wirtschaft und Sicherheitspolitik. Die Teilnehmer aus Wirtschaft, Sicherheitsbehörden und Wissenschaft haben Handlungsfelder für mehr Sicherheit im Internet und einen besseren Schutz moderner Informations- und Kommunikationsinfrastrukturen abgesteckt. Unter anderem ging es darum, wie Kriminalität, Wirtschaftsspionage und Sabotage aus dem Netz eingedämmt werden können.

Und soll sich der Staat aus der Problemlösung raushalten?
Wolfgang Ischinger: Um auf nationaler Ebene weiterzukommen, ist Vertrauen essenziell notwendig. Zwischen Staat und Wirtschaft gibt es dabei allerdings ein interessantes Spannungsfeld. Der Wunsch der Wirtschaft ist, dass sich der Staat möglichst nicht in die Wirtschaft einmischen soll. Bei Fragen der öffentlichen Sicherheit allerdings soll der Staat die Verantwortung übernehmen. Nirgends überlappen sich diese beiden Positionen so sehr, wie beim Thema Cybersicherheit. Dabei kann ich schon verstehen, dass sich Unternehmen mit der Offenlegung von Cyberangriffen schwertun. Das führt jedoch dazu, dass wir zu wenig erfahren und wissen. Ohne Information wird aber Innovation bei der Bekämpfung von Cyberangriffen noch schwieriger sein, als sie es ohnehin ist. Daher müssen wir uns dringend auf gemeinsame Vorgehensweisen einigen.

Wie hält es die Telekom mit der offenen Information?
René Obermann: Wir berichten über Angriffe auf die Systeme. Zwischen dem 3. und 6. September 2012 gab es massive Hackerangriffe auf unsere Systeme. Wir hatten die Situation unter Kontrolle, konnten auch das Rechenzentrum identifizieren, von dem der Cyber-Angriff ausging. Solche Informationen geben wir zum Beispiel an das BSI weiter, denn damit lässt sich in anderen Unternehmen Schlimmes verhindern. Wir brauchen also ein Bündnis für Cyber-Sicherheit, an dem sich alle Branchen beteiligen. Mehr als 70 Prozent der kritischen Infrastrukturen liegen in privater Hand. Deswegen müssen wir als Privatsektor zusammenarbeiten, offen und ehrlich miteinander umgehen und voneinander lernen.

Wie soll dieses Bündnis aussehen?
Wolfgang Ischinger: Wir haben zum Abschluss des Cyber Security Summit ein Eckpunktepapier verabschiedet. Hier haben die Teilnehmer festgelegt, dass bisherige Aktivitäten besser verzahnt werden müssen, und die Akteure aus Wirtschaft, Politik und Gesellschaft sektorenübergreifend besser vernetzt werden. Vordringliche Aufgabe eines solchen Bündnisses – idealerweise unter Begleitung durch die Bundesregierung und als Gemeinschaftsaktion der Spitzenverbände – ist der Aufbau einer Plattform, auf der sich alle Industriezweige und Unternehmen aller Größen einbringen können. Ein solches Forum wird den offenen und schnellen Transfer von Erkenntnissen auch über Angriffsszenarien zwischen den Akteuren ermöglichen.

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

Schnelle Eingreiftruppe

Das Deutsche Telekom CERT koordiniert das Management von Sicherheitsvorfällen für alle Informations- und Netzwerktechnologien des Konzerns.

Pro Tag erhält das Cyber Emergency Response Team (CERT) zur Überprüfung zehn Meldungen zu neuen Schwachstellen.

„Das Spannende an unserer Arbeit ist, dass wir morgens kaum sagen können, was uns tagsüber in Atem halten wird. Die wirklich kritischen Sicherheitsvorfälle sind immer die ersten ihrer Art. Um sie zu lösen, richten wir unsere Abwehr immer wieder neu aus“, bringt Bernd Eßer die Kernkompetenz seines Teams auf den Punkt. Seit zwei Jahren leitet der erfahrene Sicherheitsexperte das Cyber Emergency Response Team (CERT) der Deutschen Telekom. Mit seinen Kollegen steht er an vorderster Front, wenn Hacker Schwachstellen entdecken oder Cyber-Kriminelle Angriffe organisieren.

So auch am 3. November 2011, als ihm die US-amerikanische Bundespolizei mitteilte, dass Zehntausende von Telekom-Kunden die Schadsoftware DNS-Changer auf ihren Rechnern hätten. „Der Anruf kam an einem Montagabend“, erinnert sich Eßer. „Wir mussten davon ausgehen, dass die betroffenen DSL-Kunden am darauffolgenden Morgen offline sein würden. In einer solchen Situation muss es eine Instanz im Unternehmen geben, die in kürzestmöglicher Zeit alle relevanten Kräfte an einen Tisch bringt, um wirksame Lösungen zu finden, die den Kunden helfen.“

Permanente Aufklärung

Das Cyber Emergency Response Team ist diese Instanz. Als rund um die Uhr erreichbares Team unterschiedlichster Sicherheitsexperten sorgt es dafür, dass die Informations- und Netzwerktechnologien der Deutschen Telekom Gruppe auch

im Ernstfall zuverlässig weiterarbeiten. Neben einem Höchstmaß an technischem Sachverstand bringen die CERT-Mitarbeiter fundierte Kenntnisse in den Geschäftsfeldern und Arbeitsabläufen des Konzerns mit. Nur so können sie belastbar einschätzen, wie wahrscheinlich es ist, dass eine neu aufgedeckte Technologieschwachstelle die Telekom oder ihre Kunden gefährdet.

Pro Tag erhält das CERT durchschnittlich zehn Meldungen zu neuen Schwachstellen, die auf ihre Relevanz für den Konzern genau geprüft werden. Die ergiebigsten externen Quellen sind staatliche Stellen und CERTs anderer Unternehmen. Die Sicherheitsexperten der Telekom unterhalten gut eingespielte Netzwerke mit Internetserviceprovidern und anderen Telekommunikationsunternehmen in allen Teilen der Welt. Insbesondere in Europa ist es bereits etablierte Praxis, einander schnellstmöglich zu warnen, sobald man erkennt, dass die Systeme des anderen in den Fokus von Angreifern geraten.

Quelle Internet

Zusätzliches Wissen erhalten die CERT-Mitarbeiter von Strafverfolgungs- und Regierungsbehörden. Besonders wertvoll sind die Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI), da sie Erkenntnisse zu Gefahren vermitteln, die sich zunächst in anderen Wirtschaftszweigen entwickeln, bevor sie in der Telekommunikationsbranche sichtbar werden. Wichtige Hinweise kommen aber auch aus internen Quellen. Neben dem Vorstand ist es vor allem die Pressestelle, die Meldungen von Journalisten und nicht selten auch von Endverbrauchern weiterleitet. Zudem hat das Deutsche Telekom CERT eigene Eingangskanäle geschaffen, über die jedermann Sicherheitsvorfälle per E-Mail (cert@telekom.de) melden kann.

Zur täglichen Arbeit von Bernd Eßer und seinen Mitarbeitern gehört es, Quellen wie zum Beispiel Internetforen oder Twitter auszuwerten, in denen unterschiedliche Hackergemeinschaften ihr Wissen über Schwachstellen und deren potenzielle Ausnutzung teilen. Doch damit nicht genug. Um Schwachstellen möglichst als Erste aufzudecken, unterzieht das CERT alle im Internet erreichbaren Portale und Systeme der Telekom Group regelmäßigen Überprüfungen.

Soforthilfe: unter cert@telekom.de jederzeit Sicherheitsvorfälle per E-Mail melden.

Incident Management

Zeigt sich eine Schwachstelle mit unmittelbaren Risiken für den Geschäftsbetrieb, startet die eigentliche Vorfallsbearbeitung, das sogenannte Incident Management. Um potenzielle Gefahren schnellstmöglich abzuwenden, bildet das CERT eine Taskforce aus handlungsfähigen Kollegen, die den Einsatz der betroffenen Systeme verantworten. Oft müssen auch Zulieferer und Partner mit an den Tisch. So auch im April 2012, als eine kritische Sicherheitslücke im WLAN-Betrieb mehrerer DSL-Router bekannt wurde. Die Taskforce reichte vom Vertrieb über Produktentwicklung, Einkauf und Logistik bis zum Kundendienst, der die Geräte installiert und wartet.

„Wenn viele unterschiedliche Beteiligte am Tisch sitzen und jeder verständlicherweise erst einmal nur seine eigene Verantwortlichkeit im Blick hat, ist es unsere Aufgabe, die erforderlichen Schritte präzise zu definieren und ihre Ausführung durchzusetzen“, erläutert Deutsche Telekom CERT-Leiter Bernd Eßer. „Nicht selten müssen wir die Beteiligten dann davon überzeugen, dass sie ihre etablierten Prozesswege erheblich verkürzen müssen, damit wir den Vorfall rechtzeitig in den Griff bekommen.“

Den Routervorfall aus dem Frühjahr sieht Eßer als Paradebeispiel. Um die Sicherheitslücke zu schließen, musste die Firmware der betroffenen Produkte aktualisiert werden. Eine Aufgabe, die üblicherweise mit mehrwöchigen Entwicklungs-, Abnahme- und Auslieferungszyklen einhergeht. „Gemeinsam haben wir den Job dann in drei Tagen erledigt. Ich erinnere mich noch sehr gut daran, dass uns bei Bekanntwerden der Schwachstelle kaum jemand eine solche Reaktionszeit zugetraut hatte.“ Der Vorfall zeige sehr gut, so Eßer, wie wichtig es ist, sich in der Gefahrenabwehr flexibel aufzustellen. „Hierbei hat das Cyber Emergency Response Team die Aufgabe, eindeutige Vorgaben zu setzen und alle Partner ihren Stärken entsprechend einzubinden. Um potenzielle Schäden abzuwenden, müssen wir uns dann manchmal regelrecht neu erfinden.“

Agenda

Die Sicherheitsexperten des CERT

- koordinieren das Management kritischer Sicherheitsvorfälle
- ermitteln und bewerten Bedrohungen für die Kerntechnologien des Konzerns
- bewerten und verteilen Sicherheitswarnungen und Handlungsempfehlungen
- auditieren Sicherheitsarchitekturen und -prozesse sowie Systemlandschaften, die einem erhöhten Gefahrenpotenzial aus dem Internet ausgesetzt sind
- scannen Schwachstellen in Portalen und Systemen, die über das Internet erreichbar sind.

Bernd Eßer
ist Leiter Deutsche Telekom CERT

„In einer Risikosituation muss es eine Instanz im Unternehmen geben, die in kürzestmöglicher Zeit alle relevanten Kräfte an einen Tisch bringt, um wirksame Lösungen zu finden.“

DNS-Changer

Weltweit waren vier Millionen Computer mit einem Schadcode infiziert. Die Deutsche Telekom, das BSI und das Bundeskriminalamt entwickelten einen Schnelltest, mit dem jeder Nutzer seinen PC online überprüfen konnte.

Der Vorfall schlug weltweit hohe Wellen. Er war das Ergebnis einer Art von Cyber-Kriminalität, die bis zu ihrer Aufdeckung durch das FBI von niemandem als potenzielle Bedrohung gesehen worden war: Über einen Zeitraum von mehr als sieben Jahren hatte eine Gruppe estnischer Hacker etwa vier Millionen Computer mit dem Schadcode DNS-Changer infiziert. Der DNS-Changer erlaubte es den Cyber-Kriminellen, das Domain Name System (DNS) der Rechner zu manipulieren. Ihr Geschäftsmodell bestand darin, die gekaperten Rechner auf präparierte Internetseiten zu lenken, wenn die Nutzer ausgewählte Portale aufriefen, die allesamt hohe Werbeerlöse erzielen. Die Esten bauten die Portale nach und tauschten die Werbebanner gegen solche aus, die sie selbst vermarkteten. Das einträgliche Geschäft erlaubte es den Hackern, zwei Großrechenzentren in Detroit und New York zu betreiben. Dort standen ihnen insgesamt 1600 Server zur Verfügung, mit denen sie die infizierten Rechner manipulieren konnten.

Die Grenzen des Machbaren

Nachdem das FBI die Hacker im November 2011 verhaftete hatte, stellte die amerikanische Bundespolizei fest, dass eine Abschaltung der beiden Rechenzentren dazu geführt hätte, dass die mit dem DNS-Changer verseuchten Computer keine Webadressen mehr hätten auflösen können. Das Deutsche Telekom CERT erfuhr von dem Sachverhalt am 3. November 2011. Telefonisch teilte das FBI den Sicherheitsexperten der Telekom mit, dass man das Detroiter Rechenzentrum noch in der Nacht abschalten wolle. Um den gesamten Datenverkehr auf sichere Server in New York umzuleiten, baten die Anrufer die Deutsche Telekom um Mithilfe. Hierzu hätte der Provider in die DNS-Konfiguration der betroffenen Rechner eingreifen müssen. Da ein solches Vorgehen mit dem deutschen Recht unvereinbar war, entschied das CERT gemeinsam mit dem Konzerndatenschutz, der Bitte nicht nachzukommen. In dieser Situation musste das CERT davon ausgehen, dass eine fünfstellige Kundenzahl Gefahr lief, am kommenden Morgen keinen Internetzugang mehr zu haben. Noch in der Nacht wurden Informationen und Hilfetexte für sämtliche Callcenter sowie Briefings für die Abteilungsleiter im Kundenservice erstellt. Das Krisenmanagement musste jedoch nicht aktiviert werden, da das FBI bis zum Morgen einen anderen Provider gefunden hatte, der den Verkehr umleitete.

Der Onlineschnelltest half 19.000 Kunden der Telekom, den DNS-Changer zu entfernen.

Schnelltest macht Schule

Dessen ungeachtet galt es nun eine weitere Aufgabe zu lösen. Das FBI forderte die Provider weltweit auf, infizierte Kundenrechner innerhalb von drei Monaten von der Schadsoftware zu befreien. Um so viele Internetnutzer wie möglich zu erreichen, entwickelte das Deutsche Telekom CERT zusammen mit dem BSI und dem Bundeskriminalamt einen leicht zu bedienenden, zuverlässigen Schnelltest. Auf der Seite www.dns-ok.de konnten Nutzer per Mausklick überprüfen, ob ihre Rechner mit dem Schadcode befallen waren. Zudem stellte die Seite die Mittel bereit, um sich zu desinfizieren. Dank intensiver Medienarbeit – das CERT hatte die Presseabteilung der Telekom mit eingeschaltet – wurde der Schnelltest mehr als 22 Millionen Mal aufgerufen. Allein am ersten Tag zählte die Telekom 10 Millionen Zugriffe. Zudem machte der Schnelltest weltweit Schule. 15 Länder nahmen ihn als Best Practice, um analoge Tests zu schalten.

Parallel dazu konnte die Telekom 19.000 eigene Kunden identifizieren, die sich den Schadcode eingefangen hatten. Per E-Mail erhielten sie eine Anleitung dazu, wie sich der DNS-Changer entfernen ließ. Der Schnelltest und die direkte Kundenansprache erzielten die gewünschte Wirkung: Als das FBI die New Yorker Server Anfang Juli endgültig abgeschaltet hatte, kam es zu keinem Anstieg der Kundenanfragen zu fehlerhaften Internetzugängen.

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

Vorprogrammierte Verwundbarkeit

Herr Franck, wie schätzen Sie als Experte und Mitglied des Datenschutzbeirats der Telekom die Qualität kritischer Schwachstellen ein? Hat sich gegenüber den Vorjahren etwas verändert?
Peter Franck: Meine auffallendste Beobachtung ist die Omnipräsenz nutzbarer Schwachstellen in praktisch jeder Art von technischen Systemen, seien es nun IT- oder Kommunikationssysteme, Mobilgeräte oder Mikrocontroller, Fahrzeuge oder Industrieanlagen.

Was bedeutet das für die Anwender dieser Systeme?
Peter Franck: Man wird sich an eine Vielzahl von Schwachstellen gewöhnen müssen. Es ist davon auszugehen, dass jedes System kompromittiert ist, sofern eine Kompromittierung für irgendeinen mittelmäßig qualifizierten Angreifer lohnenswert erscheint. Dadurch wird nach meiner Prognose das heute überwiegend verbreitete, völlig realitätsferne Vertrauen in elektronisch realisierte Funktionen noch nachhaltig erschüttert werden.

Wofür interessieren sich Angreifer besonders stark?
Peter Franck: Das hängt erheblich von der Motivation der Angreifer ab. Hacker zum Beispiel wollen nur spielen. Sie informieren oftmals die Betreiber über die gewonnenen Erkenntnisse. Steckt eine kommerzielle oder kriminelle Motivation hinter dem Angriff, geht es um den maximal erzielbaren Ertrag. Politisch motivierte Angreifer nutzen Angriffe eher als Mittel des Protests und institutionellen Angreifern geht es regelmäßig um einen Informationsvorsprung oder eine gezielte Störung. Daher ist für jede fragliche Einheit das Risiko anhand der möglichen Angreifergruppen und deren mutmaßlicher Interessen individuell einzuschätzen.

Müssen die betroffenen Unternehmen ihre Abwehr anpassen?
Peter Franck: Unternehmen tun gut daran, sich mit der Materie auseinanderzusetzen, denn betroffen sind heute praktisch alle. Dies als reine Abwehraufgabe zu verstehen, reicht meines Erachtens nicht aus. Die Verwundbarkeit technischer Systeme ist durch die vorherrschenden Industriestandards quasi vorprogrammiert. Daher sollte die Abwägung schon bei der Planung und Entwicklung von Anlagen erfolgen. Die nachträgliche Vernetzung vormals autonomer Anlagen bedarf besonderer Sorgfalt. In besonders kritischen Einheiten würde ich den ausschließlichen Einsatz beweisbarer Systeme empfehlen.

Für welche Unternehmen ist es sinnvoll, ein CERT aufzubauen?
Peter Franck: Ein CERT ist immer dann sinnvoll, wenn das Geschäftsmodell hochgradig von der Verfügbarkeit informationstechnischer Systeme abhängig, und der Vernetzungsgrad dieser Systeme hoch ist. Es eignet sich prinzipiell dazu, eine Betriebsbehinderung durch induzierte Störung technischer Systeme zu verkürzen oder gar zu verhindern.

Der Chaos Computer Club (CCC)
ist ein deutscher Verein, in dem sich Hacker zusammengeschlossen haben. Laut CCC erfordert die Informationsgesellschaft „ein neues Menschenrecht auf weltweite, ungehinderte Kommunikation“, weshalb der Club sich „grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt“.

Die Mitgliedschaft steht jedem offen, der sich mit diesen Zielen identifizieren kann. Der CCC ist ein eingetragener Verein nach deutschem Recht mit Sitz in Hamburg. Er wurde gegründet, um Hackern eine Plattform zu geben und über Aktivitäten berichten zu können. Die Mitarbeit im CCC ist nicht an eine Mitgliedschaft gebunden.

Beratungsstärke

Das Deutsche Telekom CERT klärt Mitarbeiter und Kunden über aktuelle Cybergefahren auf.

Das Cyber Emergency Response Team (CERT) der Deutschen Telekom schützt den Konzern und seine Kunden vor Gefahren aus dem Internet. Eine der zentralen Aufgaben ist die Gefahrenberatung (engl. Advisory Management). Rund um die Uhr analysieren die CERT-Experten die aktuelle Bedrohungslage und leiten daraus Sicherheitswarnungen und Handlungsempfehlungen ab. Die Gesamtzahl der im Jahr 2012 veröffentlichten Sicherheitshinweise belief sich auf 1.120. Sie lag damit auf vergleichbar hohem Niveau wie in den beiden vorangegangenen Jahren. Viele dieser Fälle adressieren Schwachstellen, die zu Denial-of-Service-Angriffen oder Drive-by-Infektionen führen können. Beim Blick auf die Betriebssysteme zeigen sich keine signifikanten Unterschiede zwischen den Marktführern Unix und Windows: Während 48 Prozent der Schwachstellen Unix-Plattformen betrafen, lag der Vergleichswert für Windows-Systeme bei 43 Prozent.

Risikomanagement im Vertrieb

Der Round Table „Sicherheit im Vertrieb“ prüft den Datenschutz und die Datensicherheit der Telekom-Vertriebspartner.

Eine Vielzahl von externen Vertriebspartnern unterstützt die Telekom bei der Vermarktung ihrer Produkte an die Kunden. Über die entsprechenden Kanäle werden auch bestehende Kunden auf neue Produkte hingewiesen oder laufende Verträge verlängert. Diese externen Partner unterliegen denselben hohen Datenschutz- und Datensicherheitsanforderungen wie die Telekom selbst. Leider gibt es einzelne Partner oder auch Mitarbeiter dieser Partner, die sich nicht an die strengen Vorgaben halten. Um solche Fälle zu prüfen, gegebenenfalls rechtliche Schritte einzuleiten oder präventive Maßnahmen zu installieren, gibt es seit 2010 einen Round Table „Sicherheit im Vertrieb“.

Dieses interne Beratungs- und Informationsgremium kommt alle 14 Tage zusammen. Die Mitglieder diskutieren und bewerten dann aus ihrer jeweiligen Perspektive vertriebsrelevante Betrugsfälle wie Provisionsbetrug oder den Einsatz nicht autorisierter Vertriebspartner. Derartigen Fällen liegen im Allgemeinen eine unzulässige Datenverarbeitung und -nutzung zugrunde, welche über die vertraglich festgelegten Zwecke hinausgehen. In den Round-Table-Sitzungen wird dann darüber entschieden, welche Möglichkeiten es gibt, gegen solche Vertragspartner rechtlich vorzugehen.

Die Vertreter des Round Table kommen aus der Konzernsicherheit, dem Konzerndatenschutz, dem Compliancebereich, der Rechtsabteilung sowie den Vertriebseinheiten. Das Gremium entwickelt auch Sanktionskriterien und sorgt in Missbrauchsfällen dafür, dass die Telekom von den Betrugsfällen nachhaltig lernt und Lücken schließt. Insofern verfügt der Round Table über Empfehlungskompetenz im Hinblick auf Sanktionen und Gegenmaßnahmen.

Präventive Aufklärung

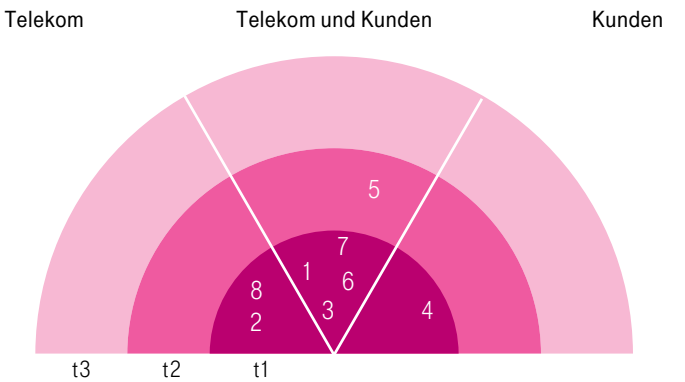
Bedrohungsradar zeigt die Entwicklung geschäftskritischer Cybergefahren.

Im Cloud Computing zählt Verfügbarkeit zu den zentralen Gütekriterien. Um möglichen Datenverlusten und dem Ausfall von Diensten vorzubeugen, investieren Cloud-Anbieter erhebliche Mittel in die Notfallwiederherstellung ihrer Systeme (engl. Disaster Recovery). So auch die Telekom, die jedem Cloud-Rechenzentrum ein zweites Rechenzentrum zur Seite stellt, das im Falle eines Falles den Betrieb übernimmt. Dass Disaster-Recovery-Systeme ihrerseits ausfallen könnten, galt bis 2011 als rein theoretisches Problem. Doch nach mehreren Vorfällen bei internationalen Wettbewerbern hat das Thema eine neue Qualität gewonnen.

Die veränderte Gefahrenlage spiegelt sich auch im sogenannten Bedrohungsradar wider, mit dem das Deutsche Telekom CERT die Entwicklung von Cybergefahren darstellt (vgl. Infografik). Der Radar liefert belastbare Informationen, um die Geschäftsrisiken einzuschätzen, welche von Cybergefahren ausgehen. Die vorbeugende Aufklärungsarbeit erlaubt es der Telekom, erforderliche Sicherheitsmaßnahmen vorausschauend zu planen und punktgenau auszuführen.

Die grafische Darstellung des Radars zeigt die zeitliche Nähe einer Bedrohung und ihre möglichen Angriffspunkte. Das Deutsche Telekom CERT erläutert die Sicht des Radars in einem sogenannten Risikoportfolio. Dieses bereitet wesentliche Ergebnisse der Risikoanalyse auf, die dem Radar zugrunde liegt. Detailliert geht es auf mögliche Schäden ein. Zudem beziffert das Risikoportfolio die Wahrscheinlichkeit, dass Angreifer eine vorhandene Schwachstelle ausnutzen werden.

Gefahrenradar



Bedrohungen

1 Advanced Persistent Threats (APT)
2 Spear Phishing gegen Telekom-Mitarbeiter
3 Mobiler Schadcode
4 Angriffe auf mobiles Banking
5 Denial-of-Service-Angriffe auf DNS-Infrastruktur
6 Angriffe auf DSL-Router
7 Ausfälle von Cloud-Diensten.
8 Shitstorms (dt. Empörungswellen)

Entwicklungsstadien

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

Quelle: Deutsche Telekom

Herbstoffensive

Denial-of-Service-Attacken gewinnen an Durchschlagskraft.

Das Domain Name System (DNS) zählt zu den attraktivsten Angriffszielen im Cyberspace. Nicht ohne Grund: Indem das DNS Websitennamen wie zum Beispiel www.telekom.de in IP-Adressen auflöst, bildet es das technische Rückgrat der Kommunikation im Internet. Vor diesem Hintergrund gehört der Umgang mit DNS-Angriffen zum Tagesgeschäft der Internetprovider.

Im Herbst 2012 stieg der Angriffsdruck noch einmal zusätzlich an. Neben klassischen Denial-of-Service(DoS)-Attacken, die Server über eine Vielzahl zeitgleicher Anfragen in die Knie zu zwingen versuchen, traten verstärkt auch sogenannte Reflected Denial-of-Service-Angriffe in Erscheinung. Statt den üblichen Weg zu gehen und ein Botnet aus Tausenden von Rechnern in Stellung zu bringen, nutzt diese Angriffsform reguläre DNS-Server im Internet, um über den Umweg solcher Server die eigentlichen Ziele anzugreifen.

Anfang September waren einige DNS-Server der Deutschen Telekom einem massiven Angriff dieser Art ausgesetzt. Das konzerneigene Cyber Emergency Response Team (CERT) verhinderte den Ausfall der Infrastruktur und wehrte den Angreifer erfolgreich ab. Das Team nutzte eine spezielle Sicherheitsplattform, um den Angriff zu analysieren und unschädlich zu machen. Als Ursprung des Angriffs wurden Computer im Rechenzentrum eines deutschen Hosters lokalisiert. Der Angriffsverlauf zeigt, dass Provider verstärkt kooperieren müssen, um Cyberattacken gemeinsam abzuwehren.

Vertrauenssache

Telekom hält potenzielle Angreifer von T-Online-Nutzerkonten fern.

Eine steigende Zahl von Hackern missbraucht die Vertrauensstellung von Internetnutzern, um in deren Namen die Angebote von Webportalen zu nutzen. Dieser vergleichsweise moderne Angriffstyp heißt Cross-Site Request Forgery (CSRF). 2012 erhielt die Telekom einen externen Hinweis auf CSRF-Schwachstellen im E-Mail-Center von T-Online. Potenzielle Angreifer hätten damit unter anderem die Möglichkeit gehabt, E-Mails zu löschen. Hierzu hätten sich T-Online-Nutzer im Portal anmelden und noch während der laufenden Sitzung eine mit Schadcode präparierte Webseite aufrufen müssen, die dann den Löschvorgang gesteuert hätte. Die Deutsche Telekom hat die Schwachstelle unmittelbar nach ihrem Bekanntwerden geschlossen. Auf den betroffenen Portalseiten wurde ein transaktionsbezogenes Sicherheitsmerkmal – ein sogenanntes CSRF Token – eingebaut, das derartige Angriffe verhindert.

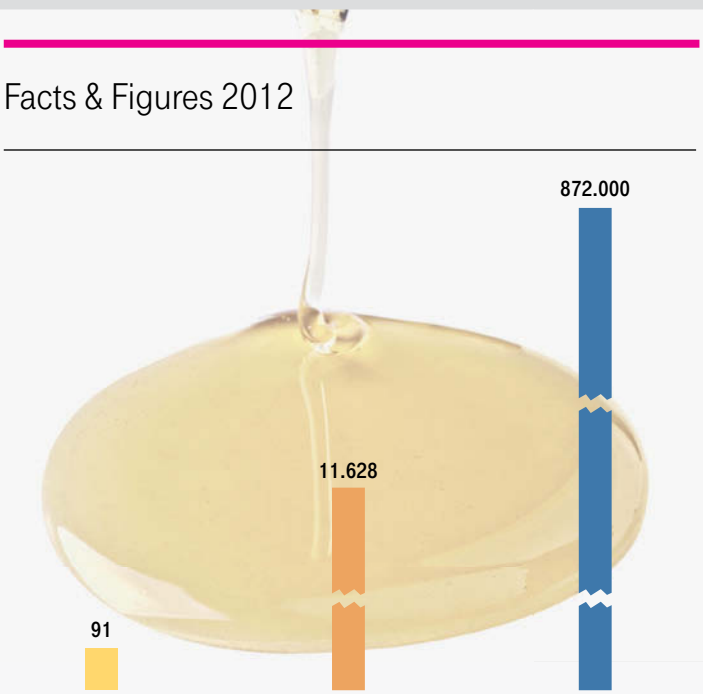
Süße Verführer

Honeypots gewähren Zugang zum Wissen der Gegenseite.

Angreifer erschließen sich immer neue Ressourcen, mit denen sie ihr Vorgehen perfektionieren. Entsprechend schnell verändern sich die Bedrohungen für die Internetwirtschaft. Um die Potenziale der Gegenseite zeitnah aufzuklären, verfügt die Deutsche Telekom über ein mehrstufiges Frühwarnsystem. Zu den zentralen Elementen darin zählen die sogenannten Honeypots (dt. Honigtöpfe). Hierbei handelt es sich um Systeme, die Schwachstellen vortäuschen, um Angriffe auf sich zu ziehen und analysierbar zu machen. Weltweit betreibt die Deutsche Telekom 91 virtuelle Lockangebote dieser Art. 2012 wurden sie täglich bis zu 400.000 Mal angegriffen.

Sämtliche Honeypots arbeiten isoliert von der eigentlichen Infrastruktur der Deutschen Telekom. Kompromittierungen können die konzerneigene Infrastruktur daher nicht gefährden. Eine Reihe von Honeypot-Systemen ist selbstlernend, sodass sich auch unbekannte Angriffe aufzeichnen und untersuchen lassen. Mit ihrer Aufklärungsarbeit gewinnt die Deutsche Telekom belastbare Informationen darüber, wie sich die Gefahrenlage verändert und wie der Konzern seine Abwehrmechanismen fortentwickeln muss.

Facts & Figures 2012



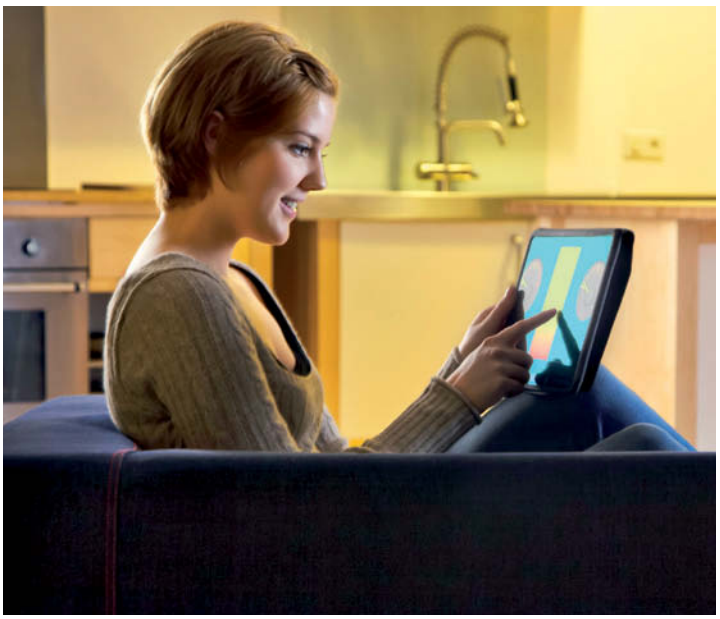
Quelle: Deutsche Telekom

Safety first

Mit Datenschutz und Datensicherheit kann man nicht früh genug beginnen. Daher bewertet die Telekom bereits in einer frühen Phase jeder System- oder Produktentwicklung deren Risikopotenzial bezüglich Datenschutz und Datensicherheit und stellt eine angemessene Beratung und Prüfung sicher. Denn Lösungen wie das „Intelligente Haus" benötigen bestmöglichen Schutz. Von Thomas Tschersich, Leiter IT-Sicherheit, Deutsche Telekom.

Bei der Deutschen Telekom wird es keine Bananenprodukte geben, deren Datenschutz und -sicherheit erst beim Kunden reifen. Stattdessen gilt der Grundsatz Datenschutz und Datensicherheit by Design. Dafür sorgt seit 2010 das Privacy-and-Security-Assessment-Verfahren (PSA), das inzwischen mehr als 4.000 Entwicklungsprojekte für IT-Systeme und -produkte durchlaufen haben. Das PSA-Verfahren stellt sicher, dass künftige Lösungen bereits vor Projektbeginn nach ihrer Kritikalität gewichtet werden, um später im Livebetrieb ein angemessenes Datenschutz- und Datensicherheitsniveau zu gewährleisten.

Eigens für das PSA-Verfahren hat die Deutsche Telekom einen einfachen Fragebogen entwickelt, der eine Bewertungssystematik bereitstellt, mit der für alle Neuentwicklungen die Kritikalität ermittelt wird. Anhand dieser Methodik wird jedes Projekt in eine der Datenschutz- und Datensicherheitskategorien A, B oder C eingestuft. Dabei steht Kategorie A für komplexe Entwicklungsvorhaben mit höchster Datenschutz- und Datensicherheitsrelevanz. Solche Projekte werden direkt durch Experten begleitet, beraten, geprüft und freigegeben, die im Vorstandsbereich Datenschutz, Recht und Compliance (DRC) der Deutschen Telekom arbeiten.



Immobilienbesitzer können im vernetzten Haus zukünftig mit mobilen Endgeräten oder dem PC Aktoren und Sensoren steuern. Das zentrale Steuerelement muss sicherstellen, dass sensible Daten nicht in die falschen Hände geraten.

Das intelligente Heim bequem und sicher steuern

Aktuell fällt ungefähr ein Drittel aller Entwicklungsprojekte unter Kategorie A, allein im Jahr 2012 waren es mehr als 600 an der Zahl. Zu diesen A-Projekten gehört unter anderem das „Intelligente Haus" (Connected Home), für das die Telekom die Infrastrukturplattform entwickelt. Deren Herzstück bildet die Qivicon-Box, die Nutzer zu Hause in ihr Netzwerk integrieren und mit deren Hilfe sie über Smartphone, iPad oder PC zahlreiche Aktoren und Sensoren steuern können. Auf die Qivicon-Box laden Anwender die Apps verschiedener Hersteller wie E.ON, Miele oder Samsung, mit denen die Telekom im Projekt Connected Home zusammenarbeitet.

Damit lassen sich beispielsweise Raumtemperaturen via Kopplung an den Thermostaten überwachen oder das Öffnen und Schließen von Rollläden über das Internet sicher fernsteuern. Einige Systeme registrieren sogar Versuche, die Jalousien von außen zu öffnen, und leiten die Meldung an zuvor definierte Empfänger weiter. Das intelligente Haus ermöglicht zudem mit „Smart Metering" die Kontrolle des Stromverbrauchs. Und sobald intelligente Stromnetze (Smart Grids) zur Verfügung stehen, können Verbraucher künftig auch ihre Stromkosten senken, indem sie beispielsweise ihre entsprechend ausgestattete Wasch- oder Geschirrspülmaschine via App so einstellen, dass sie zu einem Zeitpunkt in Gang gesetzt wird, zu dem wenig Energie nachgefragt wird und die Kilowattstunde besonders preiswert ist.

Während die Partner die Sicherheit ihrer Apps selbst verantworten, muss die Telekom dafür sorgen, dass die unterschiedlichen Hersteller-Apps auf der Qivicon-Box des Kunden sauber voneinander abgegrenzt sind. Nur dann ist

Zur Person

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

sichergestellt, dass sensible Daten nicht in die falschen Hände geraten. Neben Personen-, Verbrauchs- und Kostendaten schützt die Telekom-Lösung sicherheitsrelevante Angaben wie etwa die Zeitpunkte einer Rollladenschaltung oder einer Alarmanlagenaktivierung.

Sicherheitsvorkehrungen früh verankern

Entsprechend viel Arbeit gab es, um die passenden Anforderungen an Datenschutz und Datensicherheit zu identifizieren und umzusetzen. Je ein Berater aus den Telekom-Bereichen Group IT Security (GIS) und Group Privacy (GPR) begleitet das Connected-Home-Projekt seit der ersten Ideenskizze über die Entwicklung von Showcases für CeBIT 2012 und IFA 2012 bis hin zum derzeitigen Pilotstatus. Die Berater unterstützten die Entwickler beim Lösungsdesign und sensibilisierten für die besonderen Risiken dieses Projekts. Die Begleitung läuft weiter bis zur Freigabe für den Livebetrieb. In dieser Zeit wird das Produkt weiter auf Herz und Nieren geprüft.

Besonderes Augenmerk mussten die Produktentwickler auf die Option der Nutzer legen, mit der Qivicon-Box Informationen aus unterschiedlichen Apps zu steuern. Technisch ausgedrückt: Es galt, die strikte Mandantentrennung beziehungsweise Multimandantenfähigkeit bereits im Design zu verankern. Ferner hatten die Entwickler alle relevanten Vorschriften des Telekommunikationsgesetzes und des Telemediengesetzes zu beachten und erhielten die Vorgabe, alle über Qivicon laufenden Kommunikationsströme ausnahmslos zu verschlüsseln. Last, but not least muss die Datenhoheit der Nutzer gewahrt bleiben. So stehen Kunden mehrere Alternativen zur Verfügung, um ihre Daten und Apps zu speichern und zu verwalten, sei es per lokalem Back-up, etwa auf einem USB-Stick, oder in der Telekom-Cloud.

Wie bei jedem Entwicklungsprojekt arbeiteten die Sicherheitsexperten auf Grundlage des standardisierten Datenschutz- und sicherheitskonzepts. Darüber hinaus klärten GIS und GPR individuell mit den Entwicklern spezifische Fragestellungen, da für ein komplexes und in dieser Form bisher nicht durchge-führtes Projekt wie Connected Home noch keine standardisierten Anforderungssets oder „Blaupausen“ vorliegen konnten. Gleichwohl flossen die Erfahrungen aus thematisch verwandten Projekten wie Smart Metering in die Planung der Datenschutz- und

Kein Produkt ohne grünes Licht

Die Dokumentation des Datenschutz- und Datensicherheitsstatus erfolgt mithilfe des standardisierten Datenschutz- und sicherheitskonzepts (SDSK). Dieses wird ein „Produktleben“ lang gepflegt. Hier finden sich nicht nur sämtliche Informationen von der Produktbeschreibung bis zu späteren Weiterentwicklungen, sondern hier gibt es auch den Freigabestatus der einzelnen Entwicklungsschritte. Solange dabei nicht alle wesentlichen Lampen auf Grün stehen, kommt kein Produkt auf den Markt. Denn bei Projekten der A-Kategorie haben die Sicherheitsexperten buchstäblich bis zur letzten Minute ein Vetorecht, falls wichtige Datenschutz- und Datensicherheitsfunktionen fehlen.

Datensicherheitskategorie A, B oder C?

Kategorie	Relevanz / Detailtiefe der Betreuung / Freigabe	Verteilung in Prozent
A	■ Hohe Relevanz, da komplexe und / oder kritische Projekte. ■ Das Projekt wird durch Datenschutz- und / oder sicherheitsexperten aus den Bereichen GIS und GPR direkt begleitet, beraten, geprüft und freigegeben.	25 %
B	■ Relevanz, aber weniger komplexe Projekte mit weniger sensiblen Daten. ■ Die Umsetzung von Standardanforderungen erfolgt durch die Projekte selbst, ggf. mit Unterstützung durch lokale Sicherheitsorganisationen. ■ Die Freigabe erfolgt durch Selbsterklärung des Projektleiters, ggf. geprüft durch lokale Sicherheitsorganisationen; die Bereiche GIS und GPR ü-berprüfen stichprobenartig.	37 %
C	■ Keine Änderungen oder generell keine Relevanz. ■ Die Projekte nehmen keine Änderungen vor, die Datenschutz- und / oder sicherheitsrelevanz haben. ■ Es bedarf keiner Freigabe; die Bereiche GIS und GPR überprüfen die Projektkategorisierungen stichprobenartig.	38 %

Integrierte Sicherheit

Das PSA-Verfahren ist in die Entwicklungsprozesse der Telekom integriert. An den Entscheidungspunkten (Gates) zwischen den einzelnen Prozessschritten wird festgelegt, ob ein Übergang in den nächsten Prozessschritt erfolgt. Voraussetzung für den Übergang bildet eine ausdrückliche Gate-Entscheidung durch das jeweils verantwortliche Management. Das PSA-Verfahren ist an diese Entscheidungspunkte zum Projektstart und zur Wirkbetriebsaufnahme gekoppelt. Sobald eine Projektidee generiert und skizziert ist, wird sie hinsichtlich ihrer Datenschutz- und Datensicherheitsrelevanz kategorisiert. Mit dem Ende der Phase „Realisierung", das heißt vor der Aufnahme des Wirkbetriebs, muss das PSA-Verfahren erfolgreich abgeschlossen sein. Dazu müssen alle notwendigen Freigaben vorliegen. Wurden Auflagen zum Wirkbetrieb erteilt, wird die Umsetzung der daraus resultierenden Maßnahmen bis zum Projektabschluss nachverfolgt. Bei Projekten ohne GIS- und GPR-Betreuung erfolgen Qualitätskontrolle und Wirksamkeitsprüfung des Verfahrens über Stichproben.

Datensicherheitsmaßnahmen ein. Inzwischen haben Qivicon-Box und Intelligentes Haus die erste Pilotierungsphase erfolgreich hinter sich gebracht, sodass Anfang 2013 wie vorgesehen das zweite Pilotprojekt starten kann.

Neue Projekte mit weiterentwickeltem PSA-Verfahren

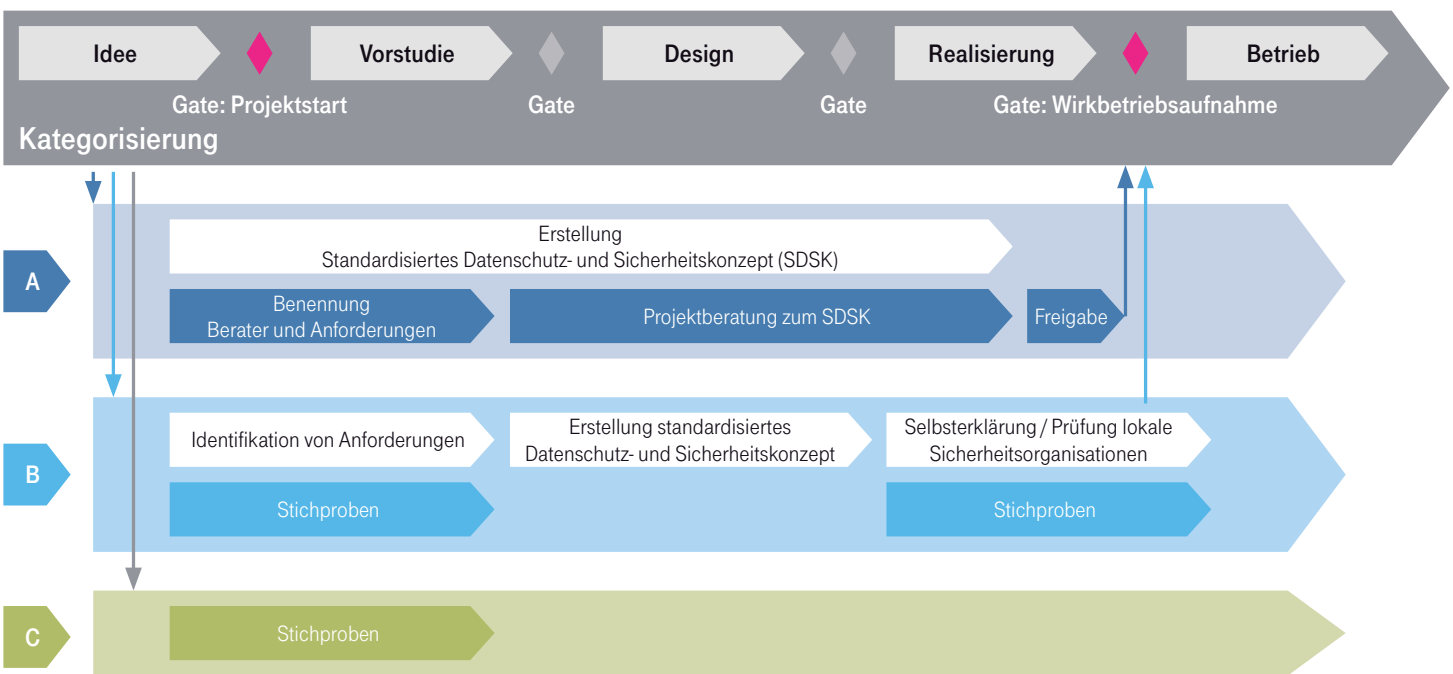
Darüber hinaus haben die PSA-Experten 2013 eine Reihe weiterer Aufgaben. Zahlreiche neue Projekte der A-Kategorie werden starten, während eine Reihe bereits laufender Projekte ihren Abschluss findet oder umfangreich weiterentwickelt wird. Dazu zählen unter anderem der Business Marketplace für kleine und mittelständische Unternehmen, der weitere Ausbau des LTE-Mobilfunknetzes der 4. Generation (Long Term Evolution) und die Übertragung von Fernsehprogrammen auf Tabletrechner im Rahmen von „Entertain to go".

In der Zwischenzeit hat die Telekom das PSA-Verfahren weiterentwickelt und verbessert. So wurden einzelne Tools und Dokumente überarbeitet, Schulungskonzepte weiterentwickelt und Hilfsmittel wie etwa einfache Checklisten für Projektleiter und Systemverantwortliche ergänzt. Außerdem galt es, neue Anforderungen zum Datenschutz und zur Datensicherheit zu integrieren. So entwickelten die Experten ein Workflowtool, das die Benutzer medienbruchfrei durch den gesamten PSA-Prozess führt – und natürlich wurde auch die Entwicklung dieses Tools nach dem PSA-Verfahren kategorisiert und geprüft.

Datenschutz und -sicherheit als Designkriterien

Zwar ist seit der Einführung von PSA der Aufwand zu Beginn eines Entwicklungsprojekts scheinbar höher als zuvor. Doch die frühe Einbindung von Datenschutz und Datensicherheit ermöglicht nun ein durchgängig strukturiertes Arbeiten, sodass teure Nachbesserungen der Vergangenheit angehören. Die Telekom geht den einzig richtigen Weg: Datenschutz und -sicherheit sind entscheidende Design-kriterien. Da die Datenschutz- und Sicherheitsberater bereits von der ersten Projektskizze an eingebunden werden, erhält ihre Arbeit mehr Struktur und Transparenz. End- und Geschäftskunden profitieren gleichermaßen von einem adäquaten Datenschutz- und Datensicherheitsniveau, welches durch das PSA-Vorgehensmodell gewährleistet wird.

Der PSA-Prozess im Überblick



Strafverfolgung von Cyberattacken

Lassen sich Cyberangriffe strafrechtlich verfolgen? Wenn ja, wie? Bei der Telekom gibt es dafür Spezialisten im Bereich Wirtschaftsstrafrecht.

Liegt nach strafrechtlicher Prüfung ein Anfangsverdacht vor, erstattet die Telekom Strafanzeige: meist gegen unbekannt.

Denial-of-Service-Attacken, Hacking, Phishing oder Massenspam: Immer wenn die Telekom mit einem Cyberangriff konfrontiert ist, schaltet das Cyber Emergency Response Team (CERT) nach Einleitung präventiver Sofortmaßnahmen auch den Bereich Wirtschaftsstrafrecht – Group Criminal Law (GCL) – ein. Sofern nach strafrechtlicher Prüfung des Sachverhalts ein Anfangsverdacht auf eine strafbare Handlung vorliegt, nehmen die Juristen schnellstmöglich Kontakt zu den Ermittlungsbehörden auf und erstatten Strafanzeige – meist gegen unbekannt, denn der mögliche Straftäter lässt sich im virtuellen Raum des Internets selten direkt identifizieren.

Schnelles Handeln spielt eine entscheidende Rolle, denn die Straftäter hinterlassen – wenn überhaupt – nur digitale Spuren ihrer Angriffe. In der Regel sind dies IP-Adressen von Servern sowie Datum und Uhrzeit der Attacke. Problem dabei: Solange keine strafrechtliche Verfolgung durch die entsprechende Staatsanwaltschaft angelaufen ist, unterliegen diese „Beweismittel“ denselben gesetzlich festgelegten Speicherfristen wie die aufgezeichneten Daten mit nicht kriminellem Hintergrund: maximal sieben Tage. Ist diese Frist vor Erstattung der Strafanzeige verstrichen, sind alle Daten mit Hinweis auf den Ursprung des Angriffes gelöscht.

Wenn die Telekom rechtzeitig Strafanzeige erstattet hat, gehen die Ermittlungsbehörden in der Regel umgehend auf die Regionalstellen für staatliche Sonderauflagen (ReSA) zu, die als staatlich beauftragte Instanz auf Grundlage eines richterlichen Beschlusses oder auf Anordnung der Staatsanwaltschaft die IP-Adressen auswerten darf. Erst wenn sich die IP-Adressen einem oder mehreren Inhabern zuordnen lassen, kann die Ermittlungsbehörde zum Beispiel Durchsuchungen vornehmen oder die Inhaber sowie Zeugen befragen. Bei Vorliegen eines hinreichenden Tatverdachts erhebt die Staatsanwaltschaft in der Regel Anklage.

Besonders schwierig für die Ermittler wird es, wenn Angreifer ein Botnet für ihre Straftat nutzen. Hierbei bauen die Täter illegal betriebene Computernetzwerke auf, für die sie ohne Wissen der Nutzer oftmals private PCs, aber auch Großrechner von Unternehmen nutzen. Dafür schleusen sie Viren und Trojaner auf deren Rechner ein und schließen sie zu einem virtuellen Netz zusammen. Auf diese Weise versenden sie beispielsweise Spam- und Phishing-Mails von diesen fremden Rechnern, die dann ihre IP-Adresse als „Beweismittel“ hinterlassen. Fälle von Botnet-Angriffen leiten die Ermittler oftmals an die Ermittlungskommission „Black Hat“ des Landeskriminalamtes Düsseldorf weiter. Die Black-Hat-Ermittler versuchen dann, die an dem Botnet beteiligten Einzelrechner zu identifizieren und unschädlich zu machen. Weiterhin versuchen sie die beteiligten Rechner durch Maßnahmen wie Firewalls und Virenscanner vor weiteren Botnets zu schützen.

Das Strafgesetzbuch (StGB) enthält einige Strafvorschriften, die speziell für die strafrechtliche Bewertung von Cyberangriffen einschlägig sind. So besagt etwa § 303a StGB, dass Personen, die Daten rechtswidrig löschen, unterdrücken, unbrauchbar machen oder verändern, mit einer Freiheitsstrafe bis zu zwei Jahren oder mit einer Geldstrafe bestraft werden können. Sogar der Versuch ist strafbar. Hierunter können etwa Massenspams fallen. § 303b StGB befasst sich mit Computersabotage und ist einschlägige Vorschrift für die strafrechtliche Bewertung von DDoS-Attacken. Die §§ 202a und 202b StGB, die das Ausspähen bzw. Abfangen von Daten unter Strafe stellen, sind Grundlage für die strafrechtliche Verfolgung von Hacking. Auf Fälle des Phisings können, je nach Fallkonstellation, mehrere der genannten Strafvorschriften anwendbar sein.

Die Wolke ganzheitlich sichern

Noch immer warnen Skeptiker vor den Datenschutz- und Datensicherheitsrisiken des Cloud Computing. Dabei sind die Gefahren kaum höher als im klassischen IT-Outsourcing. Und dieses Mehr an Risiken lässt sich in den Griff bekommen.

Zur Person

Reinhard Clemens ist seit Dezember 2007 Mitglied des Vorstands der Deutschen Telekom AG und Chief Executive Officer (CEO) von T-Systems. Zuvor war Clemens seit 2001 bei EDS in Deutschland unter anderem als Vorsitzender der Geschäftsführung für den Vertrieb, Business Operations und Strategie in Zentraleuropa verantwortlich.

Die Vorteile des Cloud Computing sind aus betriebswirtschaftlicher Sicht unbestritten, der Trend zur Nutzung von industrialisierter und weitgehend standardisierter IT aus Soft- und Hardwarefabriken ist ungebrochen. Immer weniger Unternehmen wollen teure Rechenzen-tren betreiben und beziehen standardisierte IT-Leistungen lieber aus der Cloud – günstiger als jemals zuvor. Teure Anfangsinvestitionen (CAPEX) entfallen. Stattdessen wandeln sie Aufwände für die IT in überwiegend laufende Kosten (OPEX). Außerdem lassen sich IT-Ressourcen erheblich schneller als bisher beschaffen, wodurch Unternehmen flexibler auf sich ändernde Marktanforderungen reagieren können.

So weit die betriebswirtschaftliche Seite des Cloud Computing. Sie wird dazu führen, dass Unternehmen im Zeitraum eines Jahrzehnts den überwiegenden Teil ihres IT-Bedarfs aus der Cloud beziehen werden. Während sich aber Privatkunden im Zeitalter von Social Media, Onlineshopping oder mobilen Diensten offenbar immer weniger Gedanken über den Schutz und die Sicherheit ihrer Daten machen, trauen viele Unternehmenskunden den Cloud-Anbietern noch nicht so ganz. Sie befürchten, dass mit Cloud Computing ihre Daten nicht mehr sicher sind und der Zugriff auf die Daten – also die Verfügbarkeit – leidet. Diese Skepsis ist nachvollziehbar, denn Daten bilden heute das neue Öl in den Getrieben unserer Wirtschaftsmaschinerie. Daten und ihre effizeinte Verwendung entscheiden mit über den Erfolg von Unternehmen. Daten sind ein Wert an sich, und diesen dürfen Unternehmen nicht leichtfertig verspielen.

In Magdeburg erweitert die Telekom das bestehende Rechenzentrum. Es bildet zusammen mit einem Neubau in Biere ein Zwillingsrechenzentrum für Cloud-Services.

Wenig neue Risiken durch Cloud Computing

Allerdings wird in der öffentlichen Debatte über Cloud-Sicherheit oftmals nicht zwischen der sogenannten Public Cloud und hochsicheren Private Clouds, wie sie die Telekom anbietet, unterschieden. Vielleicht ist es übertrieben, von „business as usual“ zu sprechen. Aber für seriöse Anbieter wie die Telekom, die schon seit vielen Jahren Kundendaten im Zuges eines klassischen Outsourcing verarbeitet und die Entwicklung des Cloud Computing als Pionier stetig vorantreibt, sind Themen wie Schutz vor Datenmissbrauch oder Datenverlust ganz und gar nicht neu. Telekom-Experten arbeiten beständig daran, die externen und internene Risiken des Cloud Computing auf ein Minimum zu begrenzen. Die Telekom geht diese Aufgabe ganzheitlich an, prüft alle möglichen Gefahrenquellen und führt Schutzmaßnahmen strukturiert ein.

Dabei gilt es nicht nur, das aktuell technisch Machbare zu nutzen. Cloud-Nutzer und -Anbieter reduzieren die Risiken des Cloud Computing deutlich, indem sie in partnerschaftlich enger Zusammenarbeit neben technischen auch prozessuale Sicherheitsvorkehrungen in verschiedenen Bereichen treffen. Die Telekom hat dafür eine Sicherheitstopologie entworfen, welche zwölf Aufgabenkreise umfasst, die jedes Unternehmen im Interesse der Sicherheit für die eigenen Daten und Applikationen in der Cloud beachten sollte.

Die Telekom hat das schon bestehende sehr hohe Datenschutz- und Datensicherheitsniveau der eigenen Rechenzentren für ihre Cloud-Angebote nochmals erhöht. Zu den erweiterten Risiken im Cloud-Bereich zählen zum Beispiel Datenverlust und Datenspionage oder das Hosting der IT auf einer Infrastruktur, die ein Unternehmen oder auch eine Privatperson mit anderen teilt.

Dem Datenverlust lässt sich mit der Spiegelung von Rechenzentren begegnen. Für die Trennung von Mandanten, die auf denselben physikalischen Servern laufen, sorgen Virtual Local Area Networks (VLAN). Sie verhindern, dass ein Kunde im Rechenzentrum auf Anwendungen oder Daten eines anderen Kunden zugreifen kann. Entsprechend verfügt jeder Rechner über exakt so viele, voneinander getrennte Zugangswege, wie Kunden aktuell auf ihm angelegt sind. Die Zugangswege beziehungsweise Netzwerke sind komplett isoliert.

ISO-Zertifizierung und IT-Grundschutzkatalog

Unternehmen sollten also den Cloud-Provider sorgfältig auswählen und unbedingt hohe Servicelevel durchsetzen. Wer als Anbieter keine Transparenz bezüglich Risikovorsorge erkennen lässt, ist wenig vertrauenswürdig. Und ohne Vertrauen zum Cloud-Provider sollten sich Unternehmen gut überlegen, ob sie in die Cloud gehen.

Wer auf einen Cloud-Anbieter setzt, sollte vorher prüfen, inwieweit dieser zertifiziert ist. Hier besteht derzeit allerdings eine Krux: Zwar gibt es etwa mit der ISO-Norm 27001 bestehende und anerkannte Zertifizierungen – wozu auch der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) formulierte IT-Grundschutzkatalog gehört, der stärker auf die Absicherung der technischen Infrastruktur abzielt. Doch ist die ISO-Norm 27001 noch nicht explizit auf die Cloud-Computing-Risiken zugeschnitten. So fehlen Bausteine wie beispielsweise die Netze, die virtualisierten Router und Switches, das Cloud-Management, aber auch der eigene Umgang mit den Risiken. Trotzdem bietet eine Zertifizierung nach ISO 27001 erste Anhaltspunkte bei der Auswahl des Cloud-Anbieters. Dies bestätigt auch das BSI. Die Norm besteht aus mehr als 130 Punkten, welche unter anderem die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems spezifizieren. Das klingt nach viel Arbeit -– und ist es auch, selbst für Speizialisten wie die Telekom.

Da die ISO 27001 IT-Sicherheit aus der Sicht von Prozessen und Abläufen innerhalb des Unternehmens betrachtet, unterstreicht sie, dass IT-Sicherheit auch alle Mitarbeiter angeht und nicht rein technisch betrachtet werden darf. Ein zentrales Element der ISO 27001 ist die Implementierung eines IT-Security-Managementsystems (ISMS). Sie fordert zum Beispiel von einem Cloud-Service-Provider, dass er eine Informationssicherheitsrichtlinie erstellt und umsetzt und diese in regelmäßigen Abständen durch unabhängige Expertenaudits überprüfen lässt.

Die Deutsche Telekom setzt alles daran, Cloud Computing sicher zu machen. Selbst internationale Konzerne vertrauen ihre Daten inzwischen den Cloud-Rechenzentren der Telekom an. Auch immer mehr Klein- und mittelständische Unternehmen verlieren ihre Scheu gegenüber der Cloud. Sie vertrauen dem ganzheitlichen Sicherheitsansatz der Telekom und erkennen, dass ihre Daten bei einem Cloud-Spezialisten besser aufgehoben sind.

---

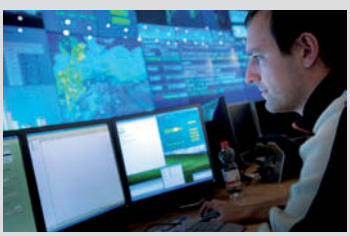
von **Reinhard Clemens**, Vorstand Deutsche Telekom und CEO T-Systems

Sicheres Cloud Computing muss folgende Aspekte beachten:

1. Verwaltung von Identitäten mit Rollen und Rechten, Endpunktsicherheit und Zugriffskontrolle
2. Anwenderinfrastruktur und sichere Kommunikation in die Wolke
3. IT-Systeme im Rechenzentrum
4. Sichere Kommunikation innerhalb der Wolke und Serviceorchestrierung
5. Schutz der IT-Systeme aufseiten des Serviceproviders
6. Sicherheit des Rechenzentrums
7. Sicherheitsorganisation und sichere Administration
8. Servicemanagement und Verfügbarkeit
9. Vertragsgestaltung, Prozessintegration und Migration
10. Sicherheits- und Schwachstellenmanagement
11. Nachweisführung und Vorfallmanagement
12. Anforderungsmanagement und Compliance

Sichere Cloud-Rechenzentren

Besonderes Augenmerk legt die Telekom in ihren Cloud-Rechenzentren auf das Thema Sicherheit. Daher hat sie eine umfassende, systematische Sicherheitsarchitektur entworfen: die „Enterprise Security Architecture for Reliable ICT Services“ (ESARIS). ESARIS beschreibt in einer durchgehend hierarchischen und modularen Dokumentation, mit welchen Standards die Telekom die Sicherheit von Cloud-Services gewährleistet. Diese Standards enthalten alle technischen, organisatorischen und prozessbezogenen Maßnahmen, die eine sichere industrialisierte ICT-Produktion ermöglichen. ESARIS berücksichtigt alle Risiken der Sicherheitstopologie für das Cloud Computing und stellt die erreichte Sicherheit damit auch transparent gegenüber dem Kunden dar. Die methodische Herangehensweise überlässt nichts dem Zufall. Sie garantiert, dass bei der Integration des Kunden in die Cloud keine Elemente vergessen oder außer Acht gelassen werden. Damit dies auch Wirklichkeit und die erreichte Sicherheit stets überprüft und verbessert wird, betreibt die Telekom ein übergreifendes Information-Security-Managementsystem (ISMS).



Mitarbeiter überwachen in den Rechenzentren nicht nur den Betrieb der Server, sondern auch die Sicherheit der Daten.

www.t-systems.de/news-media/white-papers-zu-loesungen/773396
Das White Paper „Cloud Security“ zeigt, wie eine ganzheitliche Sicherheitstopologie Cloud Computing sicher macht.

Sicherheit auf einen Blick

Telekom bündelt Wissen zu Sicherheitsprodukten und zur Gefahrenabwehr in zwei neuen Webportalen.

Tag für Tag tauchen rund 100.000 neue Varianten von Schadsoftware auf. Tendenz weiter steigend. Gleichzeitig zeichnen Honeypots der Deutschen Telekom eine konstant hohe Anzahl von Angriffen auf Webportale auf. Die gute Nachricht: Ausreichend gewartete IT-Systeme wehren 90 Prozent der Angriffe erfolgreich ab. Mit etwa 100 eigenen Sicherheitsexperten sichert die Telekom die Produkte für ihre Kunden.

Damit auch auf Kundenseite keine Angriffsflächen entstehen, baut die Telekom ihre Kommunikationsarbeit weiter aus. Auf zwei neuen Webportalen erhalten Privat-, Geschäfts- und Großkunden Informationen zu relevanten Gefahren und wirksamen Gegenmitteln. Während das Produktportal **www.telekom.de/sicherheit** einen Gesamtüberblick über das Sicherheitsportfolio gibt, vermittelt das Wissensportal **www.telekom.com/sicherheit** erprobte Vorgehensweisen, sogenannte Best Practices, zur Erhöhung der eigenen Sicherheit. Weiterhin bietet die Deutsche Telekom auf diesem Portal die gesammelten Sicherheitsanforderungen für die Produktentwicklung in einem Paket zum kostenfreien Download an.

Cloud-Dienst überzeugt durch Bedienerfreundlichkeit, Datenschutz und Sicherheit.

Die Fachzeitung Computer Bild sieht die TelekomCloud im Vergleichstest mit Apples iCloud als klaren Sieger. In der Ausgabe 2/2012 schickte die Redaktion beide Speicherwolken durch einen umfangreichen Testparcours. Angebotsumfang und Funktionen standen dabei ebenso auf dem Prüfplan wie Bedienerfreundlichkeit, Recht, Datenschutz und Sicherheit. Mit einem Gesamtergebnis von 2,47 schnitt die TelekomCloud deutlich besser ab als die iCloud, welche einen Wert von 5,00 erreichte.

Besonders positiv bewerteten die Tester, dass sich die TelekomCloud mit jedem internetfähigen PC sowie mit allen Apple iOS-, Android- und Windows Mobile-Handys nutzen lässt. Da der Datenaustausch mit der TelekomCloud komplett verschlüsselt erfolgt, gab es in der Testkategorie „Recht, Datenschutz und Sicherheit“ die Bestnote 1,62. Die größten Unterschiede zwischen den getesteten Produkten förderte eine juristische Prüfung der allgemeinen Geschäftsbedingungen zutage: Die TelekomCloud hat hier die Bewertung „gut“ erhalten.

Grenzenlose Kommunikation

Neue Technologie führt Sprachdienste, Office-IT und Konferenzlösungen sicher zusammen.

Identische Sprachdienste für Bürotelefon, Tabletcomputer und Office-PC, freier Zugang zu Videokonferenzen mit Smartphone, Videotelefon oder Telepresence. Diese Szenarien zeigen, wie die Telekom Mitarbeitern und Partnern ITK-Lösungen bereitstellt, deren aktuelle Aufgaben bestmöglich unterstützen. Hierzu hat die Geschäftskundentochter T-Systems eine Technologieplattform geschaffen, auf der die Sprachdienste, Office-IT-Systeme und Konferenzlösungen des Konzerns sicher zusammenarbeiten. Was zuvor aus Gründen der Sicherheit und des Datenschutzes getrennt voneinander ablaufen musste, bringt die neue Plattform in nutzerfreundlichen Lösungen zusammen. Beispielsweise hatte die Telekom die Sprach- von der Officeinfrastruktur separiert, um eine ausreichende Abhörsicherheit zu schaffen. Für den Sprachverkehr bedeutete dies, dass sich nur Telefone, jedoch keine PCs in das Voice-over-IP-Netz einwählen durften. Demgegenüber lassen sich die einzelnen Systeme auf der neuen Integrationsplattform verbinden, ohne den Datenschutz und die Datensicherheit zu gefährden.

Europa probt den Ernstfall

Cyber Europe 2012: 400 Experten aus 25 Ländern wehren groß angelegten Botnetangriff gemeinsam ab.

Hacker errichten ein internationales Botnet und greifen Europas Finanzsektor mit massiven Distributed Denial of Service(DDoS)-Attacken an. Mit diesem Angriffsszenario konfrontierte die Europäische Agentur für Netz- und Informationssicherheit (ENISA) die 400 Teilnehmer der Abwehrübung Cyber Europe im Oktober 2012. Neben staatlichen Stellen aus 25 Mitgliedsländern der Europäischen Union und der Euro-päischen Freihandelsassoziation nahmen erstmals auch Privatunternehmen daran teil. Unter ihnen die Deutsche Telekom in der Rolle eines Internetserviceprovider (ISP), der mithilfe des Cyber Emergency Response Teams (CERT) Angriffe gegen Großkunden abwehrte.

Die Kernaufgabe der Sicherheitsexperten bestand darin, Abwehrmaßnahmen gemeinsam zu entwickeln und durchzuführen. Schlüssel zum Erfolg war der Aufbau einer engmaschigen Kommunikation, um Informationen zu Angriffsmustern, Schwachstellen und Lösungswegen länderübergreifend auszutauschen. In einer konzertierten Aktion aller nationalen CERTs ließen sich die Server des attackierenden Botnetzes gezielt abschalten. Insgesamt lösten die Teilnehmer des Cyber Europe 2012 mehr als 1000 Sicherheitsvorfälle. Öffentliche und private Stellen bewiesen ihre Fähigkeit, die Funktion des Internets auch im massiven Angriffsfall aufrechtzuerhalten. Die nächste Übung ist für 2014 geplant.

Im Rahmen der Cyber Europe 2012 haben Experten die Abwehr von Cyberangriffen erfolgreich geprobt.

Sicherheit von Anfang an

Die Telekom hat Datenschutz und Sicherheit zu den Designkriterien ihrer Entwicklungen gemacht – kein Produkt kommt auf den Markt, wenn es nicht die entsprechenden Anforderungen erfüllt. Was dieser Grundsatz für die Praxis bedeutet, kann die weltweite Entwicklercommunity seit September 2012 im Internet überprüfen. Auf ihrem neuen Wissensportal **www.telekom.com/sicherheit** hat die Telekom mehr als 1300 technischen Sicherheitsanforderungen veröffentlicht, welche für die Produkte und Prozesse des Konzerns gelten. Sie reichen von einer allgemeinen, technologieneutralen Ebene (wie ist ein Datenbanksystem zu sichern) bis zu produktbezogenen Anforderungen – so zum Beispiel für MySQL-Datenbanken, in denen Benutzerdaten gespeichert werden.

Um Entwicklern und technischen Projektleitern möglichst konkrete Handlungsempfehlungen zu geben, liefert das Dokument zahlreiche Umsetzungsbeispiele. „Wir setzen auf Transparenz: Zum einen sollen Entwickler unsere Anforderungen schon im Vorfeld kennen. Zum anderen stellen wir uns damit einer Diskussion über die Kriterien und können diese durch internes und externes Feedback weiter verbessern“, erläutert Thomas Tschersich, Leiter IT-Sicherheit der Telekom. Um den Stand der Kriterienentwicklung fortzuschreiben, wird die Telekom die veröffentlichten Sicherheitsanforderungen zweimal jährlich aktualisieren.

Wie viel Regulierung ist nötig? Wie viel Meldepflicht möglich?

Im November 2012 hat das Bundesinnenministerium erste Eckpunkte für ein geplantes IT-Sicherheitsgesetz bekannt gegeben. Die Deutsche Telekom begrüßt die Initiative.

Die Eckpunkte sehen unter anderem vor, dass Betreiber kritischer Infrastrukturen wie Telekommunikationsunternehmen oder Energie- und Wasserversorger sowie Internetprovider ihre Sicherheitsmaßnahmen verbessern. Die Bundesregierung will damit einen einheitlichen Mindeststandard im Bereich der Sicherheit kritischer Infrastrukturen erreichen. Geplant ist zudem eine erweiterte Meldepflicht bei IT-Sicherheitsvorfällen. Eine noch wichtigere Rolle als bisher soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) einnehmen. Unter anderem soll das BSI Befugnisse erhalten, sicherheitsrelevante Hard- und Software zu testen und die Ergebnisse veröffentlichen zu dürfen.

Wichtig ist der Dialog, den die Bundesregierung mit den unterschiedlichen Branchen sowie den Betreibern kritischer Infrastrukturen angestoßen hat. Dieser stellt sicher, dass sich das Sicherheitsniveau in einzelnen Branchen durch Impulse von außen weiterentwickelt. Nur so lässt sich ein einheitlich hohes Sicherheitsniveau bei unterschiedlichen Betreibern erreichen.

Selbstregulierung ist der beste Weg angesichts der Dynamik der Entwicklung

Es gibt jedoch auch Argumente, die gegen einzelne gesetzgeberische Maßnahmen sprechen. Die Dynamik, mit der sich IT-Angriffe auf die Systeme von Unternehmen und Verwaltungen verfeinern und verändern, ist äußerst hoch. Ein langwieriges Gesetzgebungsverfahren eignet sich nur bedingt dafür, mit diesem rasanten Tempo mithalten zu können. Daher wäre es auch denkbar, dass sich im Rahmen einer Selbstregulierung die jeweiligen Unternehmen einer Branche auf gemeinsame hohe Sicherheitsstandards einigen.

Die Bundesregierung will mit einem IT-Sicherheitsgesetz einen einheitlichen Schutzschirm für kritische Infrastrukturen aufspannen.

Ein weiterer Aspekt ist zudem, dass insbesondere die Betreiber kritischer Infrastrukturen Wege finden müssen, die Sicherheits- und Schutzlevels ihrer Produkte und Dienstleistungen im kompletten Lebenszyklus zu gewährleisten. Aus diesem Grund hat die Telekom bereits vor drei Jahren ein „Privacy and Security Assessment"-Verfahren entwickelt. Dieses Verfahren ist für jedes Produkt und jede Dienstleistung der Telekom obligatorisch und trägt dem Gedanken des „Security by Design" Rechnung. Solche Verfahren wären in allen Unternehmen einsetzbar. Hier müsste ein Gesetz nur den Rahmen für weitere Selbstregulierung setzen.

Ganz entscheidend ist es, dass IT-Sicherheitsvorfälle klar und transparent gegenüber Kunden und Anwendern veröffentlicht werden. Diesen Meldeprozess und den Austausch über Branchengrenzen hinweg praktiziert die Telekom bereits heute. So informiert sie Endverbraucher und Anwender über vorhandene Kundenkontaktkanäle und Portale über konkrete Gefährdungen und bietet geeignete Sicherheitslösungen an.

Wie viel Meldepflicht ist sinnvoll? Und welche Verantwortung hat der Kunde?

Es bleibt bisher unklar, welchen Mehrwert die in den Eckpunkten des BMI skizzierte Meldeverpflichtung gegenüber schon vorhandenen Meldepflichten haben soll. Zumal im Telekommunikationsgesetz, dem Post- und Telekommunikationssicherstellungsgesetz, dem Telemediengesetz und dem Bundesdatenschutzgesetz entsprechende Meldepflichten längst verankert sind.

Insbesondere in der Praxis wäre eine Erweiterung der Meldepflicht kaum zu bewerkstelligen. Schon heute werden die Rechnersysteme der Telekom jeden Tag mehr als 100.000 Mal angegriffen. Es ist daher zu hinterfragen, ob es sinnvoll wäre, alle Vorfälle zu melden. Diesbezüglich sieht die Telekom noch Klärungsbedarf.

Zudem lässt sich aufgrund der Komplexität nicht sicherstellen, dass Kunden vollständig informiert sind. Daher braucht es klare Spielregeln, welche Verantwortung Provider, aber auch die Kunden selbst übernehmen.

Zur Person

Wolfgang Kopf, LL.M. ist seit November 2006 Leiter Politik und Regulierung der Deutschen Telekom AG in Bonn. 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 in Mainz, Speyer und London.

Gemeinsame Marschrichtung

Die Telekom vernetzt alle Handlungsfelder des Sicherheitsmanagements in einem einzigen Regelungsrahmen. So erreicht der Konzern weltweit einheitliche Sicherheitsstandards und ein adäquat hohes Sicherheitsniveau.

Spielen klassische Themen wie Gebäudeschutz oder personelle Sicherheit angesichts wachsender Cyber-Gefahren noch eine Rolle? Zweifellos hat die Digitalisierung der Wirtschaft auch deren Bedrohungen in die Datenwelt gebracht. Dennoch sind digitale und physische Sicherheit keineswegs entkoppelt. Vielmehr bedingen sie einander.

Sicherheit im Cloud Computing ist ein Paradebeispiel. Wer die Cloud-Daten in den Rechenzentren nur vor digitalem Zugriff schützt, den Zutrittsschutz jedoch vernachlässigt, hat im Ernstfall nichts gewonnen. Ein Virus wie Stuxnet, der dem Vernehmen nach die Atomanlagen von Natanz infiziert hat, ist ein Beleg dafür, dass selbst Hochsicherheitssysteme offen für Angriffe sind, wenn relevante Handlungsfelder übersehen werden. Schädlinge, die über die USB-Schnittstelle in Rechner eingeschleust werden, kommen nicht über das Datennetz. Sie passieren die Kontrollen in der Regel auf USB-Sticks, die von Menschen hineingetragen werden.

Je stärker die Digitalisierung vorangeht, desto geschäftskritischer wird es für Unternehmen, alle Aufgabengebiete ihres Sicherheitsmanagements im Verbund zu steuern. Die Fachwelt nennt dies die Konvergenz von klassischer Konzernsicherheit und technischer Sicherheit. Um entsprechend handlungsfähig zu sein, hat die Telekom 2010 ihre Konzernrichtlinien für Sicherheit aufeinander abgestimmt und in einen gemeinsamen Regelungsrahmen gesetzt. Dieses sogenannte Security Policy Framework deckt sämtliche Handlungsfelder des Sicherheitsmanagements ab. 2012 hat der Konzern verstärkt die konzernweite Komponente in den Fokus genommen.

Sicherheit als Business Enabler

Einer der wesentlichen Erfolgsfaktoren der Einführung liegt im Augenmaß, mit dem die Konzernzentrale die Richtlinien in die einzelnen Unternehmenseinheiten hineinträgt. Um ein nachhaltiges Sicherheitsmanagement zu etablieren, gilt es, die Tochterunternehmen dort abzuholen, wo sie in ihrer aktuellen Entwicklung stehen. Je nach Größe, situativem Umfeld, Geschäftsmodell und Erfahrungsstand muss eine behutsame Modifizierung möglich sein, um das angemessene Sicherheitsniveau und die wirtschaftliche Leistungsfähigkeit in Balance zu halten.

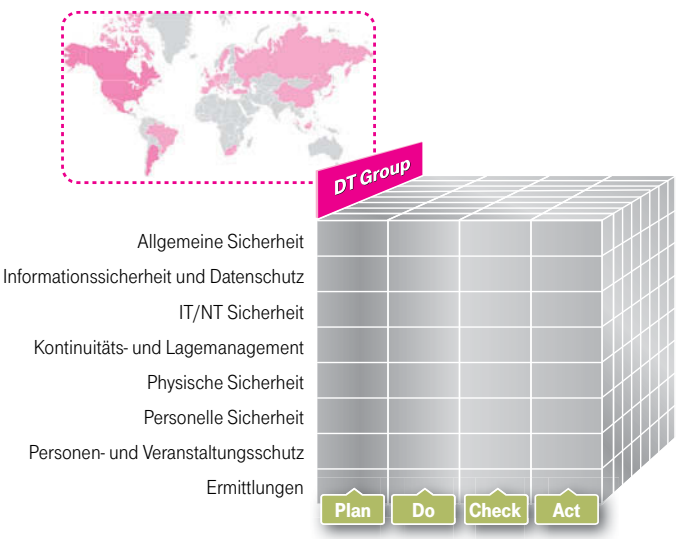
Beispielsweise brauchen neu hinzugekommene Unternehmen eine faire Chance, organisch in das Sicherheitsframework hineinzuwachsen. Dabei ist es allerdings von elementarer Bedeutung, eine transparente Vorgehensweise mit verbindlichen Umsetzungsschritten zu vereinbaren. Hierin sind Mindeststandards formuliert, die schrittweise ausgebaut werden, bis die Unternehmen die Konzernrichtlinien vollständig erfüllen.

Somit erreichen wir eine business-verträgliche Adaption sämtlicher Standards und vermeiden ein Sicherheitsmanagement, das nur auf dem Papier stattfindet. Versteht sich das Sicherheitsmanagement als Business Enabler, dann können sich Geschäftsfelder entwickeln, ohne die Sicherheit zu vernachlässigen.

Zudem steht die Konzernsicherheit in fortwährendem Austausch mit den Sicherheitsverantwortlichen der einzelnen Unternehmenseinheiten. Ziel ist ein wechselseitiger Lernprozess auf Augenhöhe. Wir nutzen die Expertise aller, um sowohl die Richtlinien als auch die Einzelmaßnahmen kontinuierlich weiterzuentwickeln. Im Einklang mit dem ISO- Standard 27001 steuern wir die Lebenszyklen unserer Regeln und Aktivitäten nach dem sogenannten Plan-Do-Check-Act-Verfahren.

Lebenszyklen managen

Für den Policyprozess bedeutet dies: Welche Vorgaben brauchen wir (Plan)? Wie implementieren wir diese (Do)? Setzen Gesellschaften, Abteilungen und Mitarbeiter die Regeln ausreichend um und beachten diese (Check)? Was lernen wir daraus für die fortwährende Optimierung unserer Regeln (Act)? Mit den Erkenntnissen der Act-Phase setzt der kontinuierliche Verbesserungsprozess wieder in der Plan-Phase an und startet aufs Neue. In diesem Sinne sind wir beispielsweise gerade dabei, das konzernweite Sicherheitsreporting weiter zu harmonisieren und einen noch verlässlicheren Blick auf das Gesamtbild zu erlangen.



Von **Axel Petri**, Konzernsicherheitskoordinator der Deutschen Telekom

Zur Person

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

Zeitenwechsel

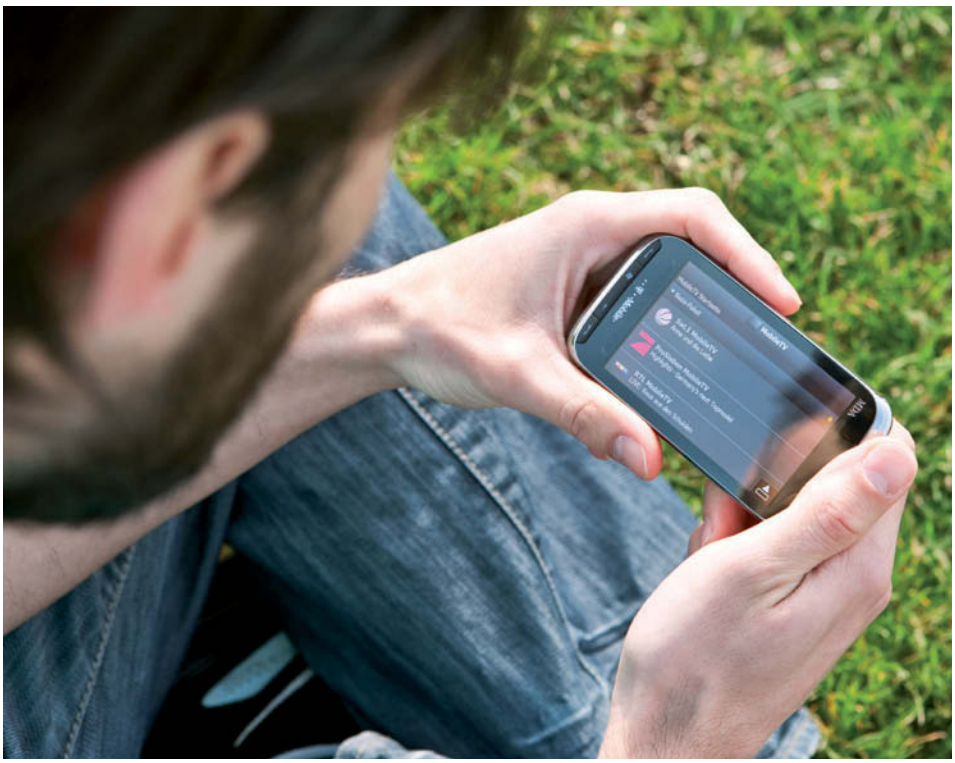
Das mobile Internet rückt ins Fadenkreuz der Angreifer. Superschnelle Mobilfunkstandards wie UMTS und LTE sowie mächtige Betriebssysteme wie Apple iOS und Google Android eröffnen nicht nur Anwendern, sondern auch Cyberkriminellen neue Möglichkeiten, ihre Ziele leichter zu erreichen. Um die heraufziehenden Gefahren zu beherrschen, müssen die Unternehmen von den Angreifern lernen und neue Trends zeitnah verfolgen.

In den Frühwarnsystemen der Deutschen Telekom zeichnet sich die neue Qualität der Angriffe bereits seit Anfang 2012 ab. Zwei Jahre zuvor hatten die Sicherheitsexperten des Konzerns sogenannte Honeypots (dt. Honigtöpfe) aufgestellt, die verwundbare Smartphones simulieren, um potenzielle Angreifer anzulocken. Die digitalen Bärenfallen erlauben es, das Vorgehen der virtuellen Einbrecher in Echtzeit zu verfolgen. 2012 wurden die mobilen Honeypots durchschnittlich 30.000 Mal pro Monat angegriffen. 30 dieser Angriffe hatten es besonders in sich: Statt wie bisher üblich rein automatisiert nach vermuteten Schwachstellen zu suchen, griffen die Hacker nun äußerst zielgenau an. Beispielsweise erhielten die Honeypots maßgeschneiderte Anfragen, mit denen die Angreifer die Adressbücher der Smartphones auslesen wollten. Zudem beobachteten die Telekom-Experten Versuche, Schadcode hochzuladen, um die in den Honeypots ausgelegten Smartphones in Botnetze einzubinden.

In Botnetzen schalten Cyberkriminelle viele Tausende, nicht selten sogar Millionen von Internetrechnern zusammen, um die Reichweite und Durchschlagskraft ihrer Angriffe zu steigern. Dass internetfähige Handys dazu ebenfalls missbraucht werden könnten, galt bis zum Frühjahr 2012 noch als theoretische Bedrohung. Vor dem Hintergrund der neuen Erkenntnisse gehen die Sicherheitsexperten der Deutschen Telekom für das Jahr 2013 davon aus, dass eine Reihe von Botnetzaktivisten die Experimentierphase beenden und ihre bisherigen Angriffe ausweiten wird. Ende 2012 wurde in den USA das erste größere, mehr als 10.000 Nutzer umfassende Botnetz für das Android-Betriebssystem gefunden.

Eigenverantwortung

Die Mehrzahl der Nutzer steht dem raschen Wandel weitgehend unvorbereitet gegenüber. Schaut man sich an, auf welchen Wegen sich Smartphones sichern lassen, so tut sich ein tief greifendes Strukturproblem auf. Ein Problem, das es vor allem für Businessanwender in sich hat. Denn sobald Unternehmen ihre Mitarbeiter mit mobilen Endgeräten ausstatten, müssen sie eine Lösung dafür finden, dass sich die Rollen im Sicherheitsmanagement um 180 Grad drehen. Während PC-Anwender davon ausgehen können, dass die erforderlichen Sicherheitspatches und Updates ohne ihr Zutun im Hintergrund installiert werden, stellt sich die Situation bei den Smartphones grundlegend anders dar. Ändert sich die Gefahrenlage, so besteht der einzig wirksame Schutz in der Regel darin, die Firmware der Endgeräte zu aktualisieren. Mit Ausnahme von BlackBerry bietet jedoch keines der marktführenden Betriebssysteme eine ausreichende Managementlösung, um die aktuell erforderlichen Sicherheitsmechanismen per Fernwartung aufzuspielen.



Experten beobachten Versuche, Schadcode in Smartphones zu laden und sie in Botnetze einzubinden.

Somit sind die Unternehmen auf die Aktivität ihrer Mitarbeiter angewiesen. Für viele Endanwender sind Aktualisierungen dieser Art jedoch alles andere als ein trivialer Prozess. Und auch diejenigen, die ihn beherrschen, haben die Tendenz, ihn aufzuschieben, da er zusätzliche Arbeit bedeutet. In der Praxis vergehen oftmals Wochen, wenn nicht Monate, bis sich Nutzer dazu entschließen, ein erforderliches Update aufzuspielen. In der Zwischenzeit nimmt die Verwundbarkeit der mobilen Endgeräte jedoch permanent zu.

MIt der flächendeckenden Ausbreitung von mobilen Hochgeschwindigkeitsnetzen entstehen neue Angriffsszenarien für professionelle Hacker.

Sicherer, weil einfacher

Steuernd einwirken können Unternehmen dabei nur indirekt. Nutzungsvereinbarungen helfen ihnen, die Mitarbeiter auf ihre neue Rolle im Sicherheitsmanagement vorzubereiten. Schulungen sind wertvoll, um den Endanwendern das erforderliche Wissen zu vermitteln. Im eigentlichen Tagesgeschäft haben die Betriebe dann jedoch nur ein einziges scharfes Schwert, um das Aktualisierungsregime dann auch tatsächlich durchzusetzen. Über präzise ausgerichteten Zugangskontrollen stellen sie sicher, dass sich nur solche Endgeräte ins Unternehmensnetz einwählen, deren Firmwareversion die gewünschten Sicherheitsmechanismen vorhält. Alle anderen Endgeräte bleiben so lange außen vor, bis ihre Nutzer die Updates durchgeführt haben.

Die zentrale Zugangssteuerung ist eine der Kernaufgaben einer durchgängigen Managementlösung, welche die Deutsche Telekom in den vergangenen beiden Jahren entwickelt hat. Diese sogenannte Mobilityplattform bietet alle erforderlichen Dienste für das Management von mobilen Endgeräten (vgl. Kasten 1). Gleichzeitig stellt sie den Anwendern eine stetig steigende Zahl von mobilen Applikationen bereit. Ende 2012 waren alle Apple iOS- und Android-Geräte anbindbar, welche die Deutsche Telekom für die interne Nutzung zugelassen hat.

Je nach Informationswunsch stehen mobilen Mitarbeitern zwei unterschiedliche Zugangswege offen. Wollen Anwender ihre E-Mails, Kontaktinformationen und Kalenderdaten synchronisieren, nutzt die Mobilityplattform den Microsoft Exchange Server. Für den Fall, dass Mitarbeiter auf das Intranet oder die betriebswirtschaftlichen Anwendungen des Konzerns zugreifen wollen, gibt es einen gesonderten, zusätzlich abgesicherten Zugang. Hierfür hat die Deutsche Telekom eine Authentifizierungsmethode entwickelt, die ein Höchstmaß an Sicherheit erzeugt, ohne die Nutzerfreundlichkeit einzuschränken. In der Praxis müssen die Anwender nur noch ein einziges Merkmal – Passwort oder Nutzernamen – eingeben. Im Hintergrund erzeugen Applikation und Plattform ein zusätzliches Sicherheitsmerkmal. Passen sämtliche Merkmale zusammen, erhält der Nutzer den gewünschten Zugriff. Die neue Methode ersetzt die sonst übliche und von vielen Anwendern als umständlich empfundene Einwahl in ein virtuelles privates Netzwerk (VPN).

Wissenstransfer

Die Datenschützer der Group Privacy und die Datensicherheitsexperten der Group Information Security haben die Entwicklung der Mobilityplattform begleitet. Über das Privacy and Security Assessment-Verfahren haben sie sichergestellt, dass Datenschutz und Datensicherheit im Design der Plattform fest verankert sind. Produktentwickler nennen diesen Grundsatz „Security by Design“. Welche konkreten Anforderungen in die Entwicklungsarbeit eingingen, zeigen die Experten im Wissensportal **www.telekom.com/sicherheit**. Softwareingenieure und Projektmanager finden dort einen umfangreichen Katalog mit technischen Sicherheitsanforderungen, welche die Produkte des Konzerns erfüllen müssen. Die Telekom teilt dieses Wissen in der Überzeugung, dass “Security by Design“ die wirksamste Form der Gefahrenabwehr ist. Geht der Entwicklungsgrundsatz in Lösungen wie die neue Mobilitätsplattform ein, so schaffen sich Unternehmen die Mittel, um den Mehrwert des mobilen Internets zu erschließen, ohne die Risiken der neuen Technologie aus den Augen zu verlieren.

Zentrale Sicherheitsanforderungen

- Eine Plattform zum Managen der Geräte.
- Alle Geräte müssen vollständig verschlüsselt sein.
- Es muss einen gesicherten Zugang zum internen Firmennetzwerk geben.
- Es muss ein gesicherter Zugang zum Mailbackend vorhanden sein.
- Es muss ein Prüffilter auf die zugriffsberechtigte Hardware installiert sein.
- Es muss ein Prüffilter auf die erforderliche Betriebsversion eingesetzt sein.
- Es muss eine Möglichkeit zum sicheren Fernlöschen vorhanden sein.
- Ist die Nutzung von Apps erlaubt, muss es eine Nutzungsvereinbarung zwischen Unternehmen und Mitarbeiter geben.
- Die Sicherheitspolicy darf nicht durch den Nutzer veränderbar sein.

Kundendienst an der Cyberfront

Das Abuse-Team ist Ansprechpartner für jeden, der den Missbrauch von Internetdiensten der Deutschen Telekom melden will. 2012 gingen die Sicherheitsexperten mehr als einer Million Hinweise nach.

Der Missbrauch (engl. Abuse) von Kundenaccounts hat viele Gesichter. Der Versand von unerwünschten E-Mails gehört ebenso dazu wie Hackerangriffe auf Kundenrechner oder das Kompromittieren von Homepages. Aktive Aufklärungsarbeit zählt daher zur Kernkompetenz des Abuse-Teams der Telekom. So wurden 2012 insgesamt 337.257 Kunden darüber informiert, dass ihre Rechner mit Schadcode infiziert waren.

In den meisten Fällen verfügt das Abuse-Team über belastbare Erkenntnisse, welche Malware im Spiel ist. Daher sind die Sicherheitsexperten der Telekom in der Lage, den betroffenen Kunden präzise Informationen dazu zu liefern, wie sie ihre Rechnersysteme desinfizieren können. Im Verlauf des Jahres 2012 trafen zum Beispiel immer mehr Hinweise auf Infektionen mit den Trojanern „ZeuS/ZeuS peer to peer“ und „bankpatch/multibanker“ ein. Während bis zum Sommer 5.069.147 Meldungen eingingen, stieg die Zahl im zweiten Halbjahr auf insgesamt 8.250.571. Dabei handelt es sich um Trojaner, die über Botnetze auf Endkundenrechner gelangen und Zugangsdaten zum Onlinebanking abgreifen. Dank der zeitnahen Information durch das Abuse-Team sank das Risiko der Kunden, dass die Malware ihr Ziel erreichen konnte.

Der Trojaner ZeuS hat 2012 auf Rechnern Zugangsdaten zum Online-Banking abgegriffen.

Wissensvorsprung

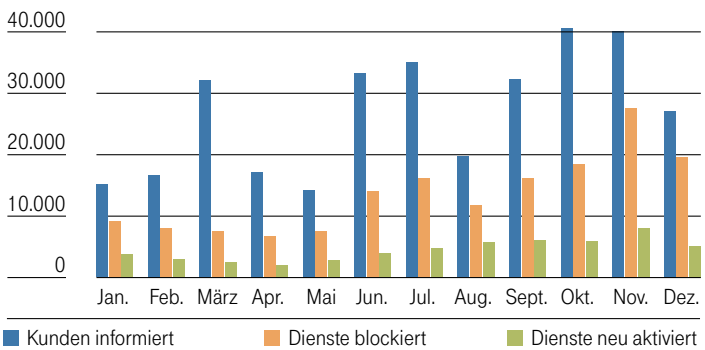
„Dieses sehr spezifische Wissen verdanken wir einer engen Zusammenarbeit mit externen Sicherheitsorganisationen, die den Missbrauch von Internetdiensten aufklären und den Providern die IP-Adressen der betroffenen Computer mitteilen“, erläutert Markus Weyrich, Mitarbeiter des Telekom Abuse-Teams. „Unsere wichtigste Quelle ist die Shadow Server Foundation, eine Organisation freiwilliger Netzaktivisten, die sich dem Kampf der Botnetze verschrieben hat. Zusätzlich zu den IP-Adressen erhalten wir Informationen zu den Schadcodes, die auf den Kundenrechnern aktiv sind.“

Das Abuse-Team hat ein Zeitfenster von sieben Tagen, um die gelieferten IP-Adressen aufzulösen und die betroffenen Kunden zu ermitteln. Nach Ablauf der siebentägigen Frist werden die Verkehrsdaten gelöscht (vgl. Infografik zur Verkehrsdatenspeicherung auf S. 15). 2012 erhielt die Telekom 1 bis 1,2 Millionen Hinweise pro Monat. Zentrales Eingangstor ist das Postfach abuse@t-online.de. Sämtliche Hinweise werden zunächst auf ihre Richtigkeit und Relevanz geprüft. Knapp zehn Prozent der Meldungen werden daraufhin weiterbearbeitet. Bei den übrigen handelt es sich zumeist um Doppler, die aus unterschiedlichen Quellen eintreffen. Neben der bereits genannten Shadow Server Foundation zählen Sicherheitsorganisationen wie Abusix Abuse Reporting, Gossler, Junk-E-Mail-Filter, Scomp, SpamVZ, Trend Micro und Uceprotect zu den Hinweisgebern. Hinzu kommen Meldungen anderer Internetserviceprovider, Hinweise von Ermittlungsbehörden sowie Anfragen von Kunden.

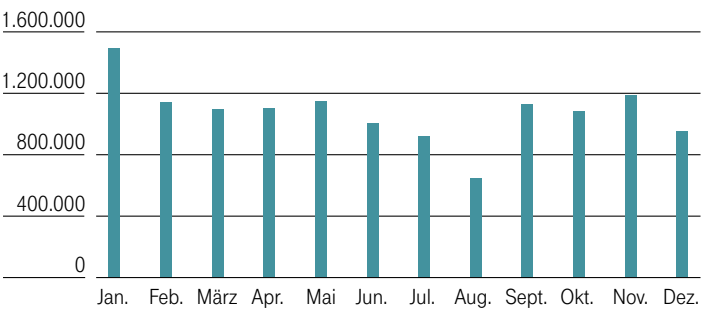
Neue Wege

Einer der Aktivitätsschwerpunkte lag auch 2012 auf der Bekämpfung von Botnetzen. Hierunter versteht man Netzwerke aus Internetrechnern, die ohne das Wissen ihrer Nutzer über eine Schadsoftware zusammengeschlossen werden.

Kundenkontakte 2012



Eingegangene Hinweise 2012



Ist ein Computer Teil eines Botnetzes, kann er unbemerkt auf ferngesteuerte Befehle reagieren, um zum Beispiel Spammails zu versenden oder andere Rechner zu infizieren. Obwohl die Aktivität der in der Regel weltweit agierenden Botnetze im Jahr 2012 weiterhin sehr hoch war, registrierte die Deutsche Telekom einen Rückgang der Fallzahlen. Gegenüber 2011 sank die Zahl der eingegangenen Hinweise von 9.146.790 auf 8.250.571, was einem 9,79-prozentigen Rückgang entspricht. Gleichzeitig verringerte sich die Zahl der Serviceeinschränkungen (Port-25-Sperren) von von 205.737 auf 132.906.

Das Abuse-Team identifiziert die betroffenen Kunden und empfiehlt ihnen per E-Mail und Briefpost, den Schadcode zeitnah mit einer aktuellen Virenschutzsoftware zu entfernen. Führt der Kunde die empfohlene Bereinigung nicht durch und attackiert der Kundenrechner auch weiterhin andere Systeme, so kann das Abuse-Team weitere Schritte einleiten. Ultima Ratio ist die Sperrung einzelner Dienste, beispielsweise des E-Mail-Versands.

Im Spätsommer 2012 sah sich das Abuse-Team erstmals gezwungen, von diesem Regelvorgehen abzuweichen. Um auf eine neuartige Bedrohung angemessen reagieren zu können, mussten Dienste gesperrt werden, ohne die betroffenen Kunden im Vorfeld der Aktion darüber zu informieren. Was war geschehen? Im asiatischen Raum war ein neues Netzwerk aktiv geworden, das neue Wege ging. Normalerweise konzentriert sich der Botnetzmissbrauch auf relativ wenige Rechner. Solange sie online sind, reizen die Angreifer die Ressourcen dieser Rechner maximal aus, um zum Beispiel so viele Spammails wie möglich zu versenden. Die übrigen Rechner des Netzwerks werden in der Zwischenzeit in Ruhe gelassen.

Der Neuankömmling aus Asien kehrte das gewohnte Vorgehen jedoch vollständig um. Er verteilte relativ wenige Anfragen pro Rechner, nutzte dafür aber alle angemeldeten Computer gleichzeitig. „Da nun viele Kunden zeitgleich betroffen waren, mussten wir den Regelprozess ändern“, erläutert Markus Weyrich. „Jeden Kunden wie üblich zunächst zu informieren, hätte zu viele Kunden zu lange einem zu hohen Risiko ausgesetzt. Daher trafen wir die Entscheidung, Sperrung und Kundeninformation parallel durchzuführen.“

Mittlerrolle

Der Fall zeigt: Vor dem Hintergrund der sich fortwährend ändernden Missbrauchsmuster muss das Abuse-Team seine Arbeit ständig neu ausrichten. Mitunter sind die Sicherheitsexperten dann sogar als Mediatoren gefragt. So auch im Frühsommer 2012, als der Suchmaschinenanbieter Google einen kompletten IP-Adressbereich der Deutschen Telekom auf eine schwarze Liste gesetzt hatte. Grund war ein Unternehmenskunde der Telekom, der IP-Adressen aus diesem Bereich bezieht und den Versuch unternommen hatte, Suchergebnisse in einer Weise zu beeinflussen, die Google als Manipulation bewertet.

Daraufhin hatte Google für den gesamten IP-Adressbereich sogenannte Captures gesetzt. Hierbei handelt es sich um spezielle Sicherheitsabfragen aus Buchstaben und Zahlen, mit denen Diensteanbieter sicherstellen, dass Anfragen von Menschen und nicht etwa von Softwareprogrammen stammen. Fortan mussten sämtliche Telekom-Kunden des betroffenen Adressbereichs – Nutzer aus dem Großraum Berlin – bei allen Google-Suchen die geforderte Sicherheitsabfrage ausfüllen. „Für Internetnutzer ein äußerst lästiger Vorgang“, erklärt Markus Weyrich. „Wir haben uns deshalb mit unserem Geschäftskunden über die Vorwürfe von Google unterhalten. Da das Unternehmen belegen konnte, dass seine Aktionen durch deutsches Recht gedeckt waren, kam die von Google gewünschte Dienstsperre jedoch nicht in Betracht. Stattdessen haben wir begonnen, zwischen den beiden Parteien zu vermitteln. Eine gewisse Annäherung ist bereits erkennbar. Doch da hier sehr unterschiedliche Auffassungen von Datenmissbrauch aufeinanderprallen, wird sich die Mediationsarbeit im Jahr 2013 noch weiter fortsetzen.“

Aufgabengebiete des Abuse-Teams der Deutschen Telekom (Auswahl)

- Empfang unerwünschter E-Mails mit Werbeinhalten (Spam)
- Empfang von E-Mails mit Viren und Würmern
- Empfang von Phising-E-Mails
- Hackerangriffe auf Kundencomputer
- Teilnahme von Telekom-Kunden an Botnetzen
- Verdacht auf Missbrauch von Zugangsdaten
- Verdacht auf Mailserverblocking
- Verdacht auf Missbrauch von Gästebüchern (z. B. Beleidigungen)
- Missbrauch in Foren und Chats durch Telekom-Kunden
- Strafrechtlich relevante Inhalte auf Homepages unserer Kunden
- Fragen zu Urheberrechtsverletzungen

Onlinesicherheitscheck
Wer seinen Internetrechner auf Viren, Würmer und andere Bedrohungen überprüfen lassen möchte, ohne eine spezielle Software installieren zu müssen, kann dies tun unter:

http://hilfe.telekom.de/hsp/cms/content/HSP/de/3378/FAQ/faq-223701325

Die Allianz für Cyber-Sicherheit:

Internettechnologien haben in den vergangenen Jahren zu Innovationsschüben in der IT- und Telekommunikationsindustrie geführt. Die rasant voranschreitende Vernetzung von IT-Systemen über das Internet hat zu neuen Chancen und Perspektiven sowohl für Bürger als auch für Organisationen, Unternehmen und Verwaltungen geführt. Annähernd jeder Lebens- und Wirtschaftsbereich ist heute mit Informationstechnologie durchzogen und damit Teil des Cyber-Raums. Somit sind auch die Wertschöpfungsprozesse der realen Welt mittlerweile intensiv über den virtuellen Raum verknüpft und ohne ihn kaum mehr denkbar. Diese Entwicklung erfordert von allen Beteiligten eine stetige Auseinandersetzung einerseits mit dem unbestreitbar großen innovativen Potenzial, das IT-Lösungen bieten können – andererseits aber auch mit den Risiken und Sicherheitsmaßnahmen, die notwendig sind, um IT sicher und zuverlässig zu betreiben und Daten verantwortungsvoll zu nutzen. Das Streben nach einem sicheren Cyber-Raum ist eine Herausforderung, die nur durch gemeinsame Anstrengungen von Wirtschaft, Wissenschaft und Verwaltung möglich wird. Ausdruck dessen ist die Allianz für Cyber-Sicherheit, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) als Plattform für den Informations- und Erfahrungsaustausch auf diesem Gebiet initiiert haben.

Cyber-Angriffe werden von unterschiedlichen Tätergruppen mit unterschiedlichen Zielsetzungen durchgeführt. Das Spektrum reicht von Überlastangriffen (Denial of Service) durch Aktivisten und Erpresser über die Manipulation von Internetbanking-Vorgängen durch Kriminelle bis hin zu Ausspähung und Sabotage durch fremde staatliche Stellen. Viele Angriffsziele können dabei relativ einfach attackiert und die Angriffswege effektiv verschleiert werden. Zudem ist die heutige Informationstechnik aufgrund ihrer Komplexität nicht fehlerfrei und damit immer wieder verwundbar. Unbestritten ist, dass durch diese Bedrohungslage nicht nur einzelne Institutionen gefährdet werden. Auch IT-Systeme von kritischen Infrastrukturen, deren Verfügbarkeit und Verlässlichkeit für unsere Gesellschaft von besonderer Bedeutung sind, sind Teil des Cyber-Raums und dadurch den genannten Risiken ausgesetzt.

Gemeinsam handeln: die Allianz für Cyber-Sicherheit

Es stellt sich die Frage, wie angesichts dieser Gefährdungslage ein effektiver und effizienter Schutz vor Cyber-Angriffen erreicht werden kann und welches Risiko tragfähig ist. BSI-Erkenntnisse zeigen, dass sich weit mehr als 80 Prozent der bekannten Angriffe mit Standardschutzmaßnahmen abwehren lassen, beispielsweise im Rahmen von IT-Grundschutz. Leider haben im Bereich der Umsetzung solcher Maßnahmen noch viele Institutionen Nachholbedarf.

Nachhaltige Sicherheit lässt sich nur durch ein kooperatives Vorgehen aller Akteure in Wirtschaft, Wissenschaft und Staat sowie eine kontinuierliche Anpassung aller Maßnahmen zur Prävention, Erkennung und Reaktion an die Gefährdungslage und die Methoden der Angreifer erreichen. Als Kooperationsplattform haben das BSI und der BITKOM die Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de) initiiert. Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, die Informationssicherheit in Deutschland zu erhöhen und die Widerstandsfähigkeit von IT-Systemen gegenüber Cyber-Angriffen zu stärken. Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und unterstützt den Informations- und Erfahrungsaustausch. Für Unternehmen und Organisationen sind mehrere Formen des Mitwirkens möglich – abhängig von der Art und Weise, wie sich eine Institution engagieren möchte.

Allianz für Cyber-Sicherheit

Partner der Allianz für Cyber-Sicherheit können Institutionen werden, die durch aktive Beiträge die Cyber-Sicherheit in Deutschland gestalten, fördern und verbessern möchten. Partner können beispielsweise Computernotfallteams (CERTs), IT-Hersteller und -Dienstleister, Internet-Infrastrukturbetreiber oder Forschungseinrichtungen sein. Als Teilnehmer der Allianz für Cyber-Sicherheit sind Institutionen sowohl aus dem privatwirtschaftlichen als auch

Michael Hange ist Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

„Die Allianz für Cyber-Sicherheit richtet sich an alle deutschen Institutionen aus dem privaten und öffentlichen Sektor."

mehr Schutz durch Kooperation

aus dem öffentlichen Sektor eingeladen, die von den Informationen und Leistungen der Allianz profitieren und die Cyber-Sicherheit ihrer Institution verbessern möchten.

Die Allianz für Cyber-Sicherheit richtet sich an alle deutschen Institutionen aus dem privaten und öffentlichen Sektor. Aufgabe der Multiplikatoren der Allianz für Cyber-Sicherheit ist es daher, die Reichweite der Allianz zu erhöhen, indem sie etwa aktuelle Informationen an ihre Mitglieder oder an andere Adressatenkreise vermitteln oder durch Gremien-, oder Öffentlichkeitsarbeit für die Anliegen der Cyber-Sicherheit sensibilisieren. Als Multiplikatoren können etwa Wirtschaftsverbände, Industrie- und Handelskammern oder Medien die Allianz unterstützen.

Angebote und Leistungen der Allianz

Ein wesentliches Angebot der Allianz für Cyber-Sicherheit beinhaltet die Förderung des Dialogs zwischen allen Beteiligten, nämlich in der IT-Branche tätige Unternehmen und deren Benutzer von Informationstechnologie. Hierfür werden den Benutzern einerseits Informationen zum Einsatz von IT zur Verfügung gestellt, andererseits werden umfassende Möglichkeiten zum Erfahrungsaustausch geschaffen oder weiter ausgebaut. Zu den Angeboten gehören beispielsweise Warnhinweise zu aktuellen Cyber-Bedrohungen, Best Practices, Standards und Lösungen zur Absicherung der verwendeten Systeme, aber auch Empfehlungen zum generellen sicheren Einsatz von IT-Komponenten. Neben der zentralen Informationsverteilung setzt die Allianz dabei auch auf den direkten Austausch in kleineren Gruppen, beispielsweise in regionalen und branchenbezogenen Arbeitskreisen oder in Form von Stammtischen.

Um Risiken fundiert bewerten zu können und das IT-Sicherheitsniveau in Deutschland zu verbessern, ist eine umfassende Kenntnis der aktuellen Sicherheitslage unabdingbar. Im Rahmen der Allianz stellt das BSI daher aktuelle Lageinformationen zur Verfügung, damit Institutionen ihre Aktivitäten darauf ausrichten können. Um die Vollständigkeit der Lageinformationen weiter zu erhöhen, besteht auch für Partner und Teilnehmer die Möglichkeit, eigene Erkenntnisse einzubringen oder Ereignisse im Zusammenhang mit Cyber-Angriffen an das BSI zu melden.

Die Schaffung von mehr Cyber-Sicherheit bedeutet eine Gemeinschaftsaufgabe für Staat, Wirtschaft und Wissenschaft. Durch die Teilnahme am Erfahrungsaustausch oder einen aktiven Beitrag als Partner oder Multiplikator im Rahmen der Allianz für Cyber-Sicherheit können Institutionen daran mitwirken, die Cyber-Sicherheit in Deutschland weiter zu verbessern und aktiv zu gestalten. Alle deutschen Institutionen sind aufgerufen, sich an diesem Prozess zu beteiligen!

von **Michael Hange**, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Gemeinsam sind sie stark

Die bundesweite Initiative Allianz für Cyber-Sicherheit ist Anfang 2012 gestartet. Die Initiative, an der sich die Deutsche Telekom intensiv und aktiv beteiligt, verfolgt das Ziel, Informationen zur Cyber-Sicherheit in Deutschland bereitzustellen sowie ein umfassenders Bild der aktuellen Gefährdungslage

Die bundesweite Initiative Allianz für Cybersicherheit bringt IT- und Sicherheitsexperten zusammen.

zu ermöglichen. Die Initiative richtet sich an IT- und Sicherheitsverantwortliche in Unternehmen und Organisationen jeglicher Größe. Damit ergänzt die Allianz im Rahmen der Cybersicherheitsstrategie für Deutschland die Maßnahmen des Umsetzungsplans KRITIS (Nationale Strategie zum Schutz Kritischer Infrastrukturen), welche für die kritischen Informationsinfrastrukturen ergriffen werden.

Die Allianz für Cyber-Sicherheit ist eine gemeinsame Initiative des Bundesamt für Sicherheit in der Informationstechnik (BSI) und des BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) und lädt Hersteller, IT- und Telekommunikationsdienstleister, Träger der Internetinfrastrukturen, CERTs, Anwenderbranchen mit intensivem IT-Einsatz sowie Multiplikatoren aus Medien und Wissenschaft ein, in der Allianz mitzuwirken.

„Wir brauchen flächendeckend ein verlässliches und aktuelles Lagebild zur Cybersicherheit für den Standort Deutschland sowie gleichzeitig den Erfahrungsaustausch und die Hilfe im Schadensfall direkt vor Ort“, betonte BITKOM-Präsident Professor Dieter Kempf, anlässlich der Vorstellung der Initiativenidee während der CeBIT 2012 in Hannover.

IMPRESSUM

Herausgeber

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

Fotos

Deutsche Telekom AG,
Fotolia, iStockphoto, Kai Mörk

Stand 1/2013

www.telekom.com/datenschutz

www.telekom.com/sicherheit

Datenschutzratgeber 2012