

Sendesperrfrist: 10. Oktober 2008, 11.00 Uhr / Beginn Rede

René Obermann

– Es gilt das gesprochene Wort –

Rede

anlässlich der Pressekonferenz

„Schutz von Kundendaten bei der Deutschen Telekom AG“

der Deutschen Telekom AG

am 10. Oktober 2008 in Bonn

René Obermann

Vorstandsvorsitzender

Deutsche Telekom AG

Meine Damen und Herren,

auch ich begrüße Sie ganz herzlich zu diesem Pressegespräch. Vielen Dank, dass Sie unserer kurzfristigen Einladung gefolgt sind. Über das Thema „Datenschutz bei der Deutschen Telekom“ ist seit der Bespitzelungsaffäre und dann ganz besonders nach den Veröffentlichungen des Spiegels am Montag viel gesprochen und geschrieben worden. Deswegen möchten wir Ihnen und der Öffentlichkeit heute einige Dinge einordnen – vor allem, welche Maßnahmen wir zusätzlich einleiten, um die Daten unserer Kunden in Zukunft noch wirkungsvoller zu schützen.

Die Deutsche Telekom hat alleine in Deutschland mehr als 1000 Betriebsstandorte, ca. 140000 Beschäftigte, wir haben darüber hinaus 800 eigene T-Shops und über 10.000 Vertriebspartner. Monatlich kommen viele Millionen Kunden in unsere Shops und schließen bei uns neue Verträge ab, beauftragen einen Reparatur- oder Installationservice oder rufen im Callcenter an, um z.B. Tarif, Adresse oder Kontoverbindung zu ändern. Dabei müssen unsere Mitarbeiter naturgemäß viele Daten verarbeiten, um guten Service zu leisten, insbesondere erfordert guter Service auch eine dezentrale Verfügbarkeit dieser Daten.

Die Daten wecken aber auch Begehrlichkeiten zum Missbrauch. Deshalb sehen wir uns immer wieder Versuchen ausgesetzt, in unsere Systeme einzudringen und sich unbefugt Daten zu beschaffen oder sonstigen Schaden anzurichten. Diese Versuche gibt es seit vielen Jahren. Und deshalb haben wir in den vergangenen Jahren zahlreiche Anstrengungen unternommen, um mit einem modernen Datenschutz diese Angriffe abzuwehren. In der überwiegenden Mehrheit der Fälle sind und waren wir erfolgreich – aber eben nicht bei allen. Das zeigt nicht zuletzt die aktuelle Berichterstattung.

Aber wir stehen dem nicht tatenlos gegenüber. Im Gegenteil: Wir haben in den vergangenen Jahren systematisch den Datenschutz bei der Deutschen Telekom verbessert. Aber letztlich ist es ein ständiger Wettlauf zwischen Kriminellen, anders kann man meiner Ansicht nach Datendiebe nicht nennen, und Datenschützern. Ein Phänomen, das übrigens keinesfalls auf die Deutsche Telekom beschränkt ist. Sondern, das haben die vielen Fälle in den vergangenen Monaten gezeigt, es ist längst zu einem Phänomen der Informationsgesellschaft geworden ist.

Trotzdem oder gerade deshalb, müssen wir vor dem Hintergrund der aktuellen Ereignisse feststellen, dass wir zusätzlichen Handlungsbedarf in Sachen

Datenschutz- und sicherheit haben und in Zukunft anders kommunizieren sollten.

Noch mal: Das heißt nicht, dass unser Datenschutz schlecht ist. Das Gegenteil wurde uns ja von unabhängiger Seite auch immer wieder bestätigt. Wir sind aber zu der Überzeugung gelangt, dass wir jetzt neue Maßstäbe im Bereich Datensicherheit setzen müssen. Darum haben wir ein umfangreiches Maßnahmenpaket erarbeitet, das wir Ihnen heute vorstellen.

Dabei geht es um drei große Schwerpunkte mit zahlreichen konkreten Einzelmaßnahmen, die Herr Höttges Ihnen im Anschluss vorstellen wird:

1. Wir wollen den Datenschutz stärken. Wir werden deshalb dem Aufsichtsrat in der nächsten Sitzung vorschlagen, ein neues Vorstands-Ressort für den Bereich Datenschutz, Recht und Compliance zu schaffen. Das Thema „Datenschutz“ und Sicherheit würde damit zukünftig auf oberster Management-Ebene verankert sein. Verbunden damit wären auch deutliche finanzielle und personelle Aufstockungen und ein Veto-Recht bei Geschäftsentscheidungen mit datenschutzrechtlicher Relevanz.
2. Transparenz. Es wurde kritisiert, dass wir nicht immer zeitnah über Vorgänge informiert haben. Dafür gab es eine Reihe von Gründen, zum Beispiel um Trittbrettfahrer nicht anzulocken. Aber wir haben die Kritik verstanden und werden unsere Informationspolitik anders ausrichten. Wir wollen transparenter werden. Um drei wichtige Beispiele zu nennen: Wir werden sehr kurzfristig, schon nächste Woche, eine Internetseite schalten, auf der wir über aktuelle Datenschutzthemen informieren. Wir werden einen jährlichen Datenschutzbericht veröffentlichen und wir werden einen Datenschutzrat berufen, bei dem Experten aus Politik, Forschung und Lehre, auch und gerade die kritischen, mit uns in einen konstruktiven Dialog über das Thema „Datenschutz“ treten wollen. Außerdem werden wir uns von unabhängiger dritter Seite zertifizieren lassen. Zum Punkt „Transparenz“ gehört aber auch

klarzumachen, dass es keine 100 prozentige Sicherheit geben kann und geben wird. Niemand, nicht die Deutsche Telekom aber auch kein anderes Unternehmen, kann ausschließen, dass es alle kriminellen Attacken abwehren kann. Aber wir können alle Anstrengungen unternehmen, um einen hohen Schutz zu gewährleisten und das werden wir.

3. Wir wollen ohne Kompromisse und konzernweit die höchsten Standards beim operativen Datenschutz umsetzen. Dabei geht es zum Beispiel um die Organisation von Zugriffsberechtigungen, eine stringente Einführung neuer Systeme oder die noch intensivere Schulung insbesondere auch von tausenden Führungskräften und aller Mitarbeiter.

Wir wollen damit ein Signal setzen, das wir auch als einen wichtigen Impuls für unsere Branche insgesamt verstehen. Und was das Wichtigste ist: Wir wollen bei unseren Kunden verlorenes Vertrauen zurückgewinnen. Die Umsetzung dieser Maßnahmen, die Ihnen Herr Höttges gleich im Detail vorstellen wird, hat begonnen und zwar mit Priorität. Unsere Kunden werden die ersten Maßnahmen in den nächsten Wochen bemerken. Das kann auch dazu führen, dass Serviceleistungen etwas länger dauern als bisher, weil z.B. TAN's oder ein zusätzliches Passwort eingegeben werden müssen.

Meine Damen und Herren,

es handelt sich dabei nicht um ein Programm, das zu einem Zeitpunkt x abgeschlossen wird, sondern um eine grundsätzliche und dauerhaft neue Herangehensweise. Letztlich ist es immer ein Wettlauf zwischen Datenschutz und potenziellen Angreifern. Zunächst werden wir uns nochmals ganz genau die jüngsten Fälle anschauen und auch analysieren, ob und wo es Fehlverhalten gegeben hat. Dazu haben wir einen entsprechenden Revisionsbericht bereits in Auftrag gegeben. Wenn dieser Bericht Fehlverhalten feststellen sollte, werden wir daraus die Konsequenzen ziehen.

