Datenschutz

Zugriff verweigert

[16.10.2014] Vor einem US-Gericht setzt sich Microsoft dafür ein, Daten vor dem Zugriff Dritter zu schützen. Auf welche Argumente der Konzern dabei setzt, erläutert Marianne Janik, Senior Director Public Sector und Mitglied der Geschäftsleitung bei Microsoft Deutschland.

Frau Dr. Janik, ein Bundesgericht in New York hat entschieden, dass amerikanische IT-Anbieter auch dann Kundendaten an US-Behörden herausgeben müssen, wenn diese in Europa gespeichert sind. Was ist der Hintergrund des Urteils?

In dem angesprochenen Fall geht es um die Aufforderung von US-Behörden an Microsoft, die E-Mail-Daten eines unserer Kunden, gegen den ein Ermittlungsverfahren läuft, aus unserem Consumer-Dienst Outlook.com preiszugeben. Unseren Einspruch gegen diese Aufforderung haben sowohl das zunächst zuständige Magistratsgericht als auch jüngst das Bundesgericht in New York abgelehnt. Das Urteil ist vorerst ausgesetzt und daher noch nicht rechtskräftig.

Wenn das Urteil rechtskräftig wird, was bedeutet das für Ihr Cloud-Geschäft in Europa, insbesondere auch mit der öffentlichen Verwaltung?

Welche direkten Auswirkungen ein rechtskräftiges Urteil auf unser Cloud-Geschäft hätte, wäre nur hypothetisch zu beantworten. Fakt ist aber: Wir müssen unseren Kunden ein Höchstmaß an Sicherheit garantieren können und auf ihre individuellen Bedürfnisse eingehen. Wir bieten daher bereits heute jedem Kunden die Cloud-Lösung an, die aus seiner Sicht die beste ist. Im Public Sector erlebe ich es zum Beispiel, dass kleine Kunden sowie betriebswirtschaftlich ausgerichtete Organisationen der Public Cloud deutlich offener gegenüberstehen als große Behörden. Die wiederum setzen vielfach auf Private Clouds, also auf eine IT-Infrastruktur innerhalb ihrer Organisation. Insgesamt gewinnt aber die Kombination aus privater und öffentlicher Cloud – die frei skalierbare Hybrid Cloud – für unsere Kunden aus der öffentlichen Verwaltung an Relevanz.

„Wir müssen unseren Kunden ein Höchstmaß an Sicherheit garantieren können."
Microsoft wird die Entscheidung des New Yorker Bundesgerichts anfechten. Wie lauten die Argumente?

In unserer Rolle als einer der weltweit führenden IT-Hersteller sehen wir unsere Verantwortung vor allem darin, die Daten und die Privatsphäre unserer Kunden bestmöglich vor Zugriffen Dritter zu schützen – ganz gleich, ob durch Cyber-Kriminelle oder durch unrechtmäßige Zugriffe staatlicher Institutionen. Mit genau solch einem unrechtmäßigen Zugriff durch die US-Behörden sehen wir uns im aktuellen Fall konfrontiert. Wir begründen unseren Einspruch damit, dass die Kundendaten nicht auf amerikanischem Boden, sondern ausschließlich in unserem Rechenzentrum im irischen Dublin gespeichert sind. Denn unsere Rechtsauffassung ist es, dass ein US-Staatsanwalt nicht die Befugnis hat, E-Mail-Konten zu durchsuchen, deren Daten außerhalb der USA gespeichert sind. Er hat schließlich auch nicht das Recht, ein Haus in einem Land außerhalb der USA durchsuchen zu lassen. Was in der physischen Welt Bestand hat, sehen wir auch in der digitalen Welt als gültig an.

Was hat Microsoft bereits getan, um unautorisierte Zugriffe auf Daten zu verhindern, wie spiegelt sich das in den Produkten wider?

Alle unsere Produkte werden nach den Prinzipien Privacy by Design und Privacy by Default entwickelt – also mit datenschutzfreundlichen Voreinstellungen, die standardmäßig aktiviert sind. Ein Beispiel dafür ist die „Do Not Track“-Funktion des Internet Explorers, wodurch den besuchten Websites und auch Dritten, deren Inhalte auf diesen Internet-Seiten gehostet werden, mitgeteilt wird: Ich will nicht, dass meine Browser-Aktivitäten nachverfolgt werden. Erst kürzlich haben wir außerdem durch das Verschlüsselungsprotokoll Transport Layer Security (TLS) die Verschlüsselung von ein- und ausgehenden E-Mails unseres Dienstes Outlook.com verbessert.

Welche weiteren Möglichkeiten hat ein Unternehmen wie Microsoft, die Daten der Kunden zu schützen?

Neben der Implementierung eines bestmöglichen Datenschutzes in unseren Produkten, setzen wir vor allem darauf, unsere Kunden auf Gefahren frühzeitig aufmerksam zu machen und ihnen das nötige Rüstzeug an die Hand zu geben, damit sie bewusst und eigenverantwortlich mit ihren Daten umgehen. Mit den regelmäßigen Security Bulletins und den Security Intelligence Reports geben wir Nutzern zum Beispiel einen Überblick über aktuelle Bedrohungen im Internet und zeigen Maßnahmen, wie sie die eigene IT-Sicherheit ausbauen können. Über unser Engagement in der Initiative Deutschland sicher im Netz (DsiN) informieren wir ebenfalls über sicherheitsrelevante Themen, bieten direkte Schutzmaßnahmen an und schärfen damit das Bewusstsein von Unternehmen und Privatanwendern für die eigene IT-Sicherheit. In eine ähnliche Richtung geht auch unsere Initiative IT-Fitness. Hier kann jeder Anwender sein eigenes Sicherheitsverhalten im Netz überprüfen und einschätzen. Damit sich auch die Politik davon überzeugen kann, dass wir keine Hintertüren in unsere Produkte einbauen, errichten wir zurzeit in Brüssel ein internationales Transparenz-Zentrum, in dem wir Regierungsvertretern die Möglichkeit geben werden, den Quellcode unserer Software einzusehen. Im Gegenzug sehen wir die Politik in der Pflicht, den Schutz von Bürgern und Unternehmen zu fördern und dadurch neue Wachstumschancen freizusetzen. Daher ist es prinzipiell zu begrüßen, dass die Bundesregierung eine Digitale Agenda vorgelegt hat. Es zeigt, dass die Regierungskoalition die Bedeutung der Digitalisierung inklusive deren Chancen und Risiken erkannt hat. Die Agenda bildet bisher jedoch nur einen Rahmen für künftiges Regierungshandeln und gesetzliche Regelungen – hier müssen zügig Taten folgen, um tatsächliche Rechtssicherheit für Nutzer und Wirtschaft zu schaffen.

()

Dieser Beitrag ist in der Oktober-Ausgabe von Kommune21 im Schwerpunkt Datenschutz erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, Recht, Marianne Janik