Handelsblatt

Handelsblatt Nr. 109 vom 11.06.2013 Seite 001

Seite 1 Tagesthema

Ärger über einen Freund

Die Datensammelwut der USA empört deutsche Firmen: Sie misstrauen Internetkonzernen wie Google und Facebook, die dem Geheimdienst zuarbeiten. Die Kanzlerin soll bei US-Präsident Obama intervenieren.

Jens Koenen, Michael Inacker, Daniel Delhaes, Klaus Stratmann
Frankfurt, Berlin

Sie sind das Gold moderner digitaler Gesellschaften: Daten. Als Verkaufsinformationen entscheiden sie über wirtschaftliche Erfolge, als Geheimdienstinformationen über Krieg und Frieden.

Deshalb erscheint es kaum überraschend, dass die US-amerikanische National Security Agency (NSA) zum Schutz der nationalen Sicherheit seit Jahren den E-Mail-Verkehr, Skype-Telefonate oder Videokonferenzen ausländischer Internetnutzer überwacht.

Für Empörung sorgt jetzt aber die Enthüllung, dass der US-Geheimdienst den Datenfluss direkt an den Servern von weltweit agierenden Internetkonzernen wie Microsoft, Yahoo, Google, Apple, Facebook, Youtube, Skype und AOL abgreift. Allein im Frühjahr soll die NSA binnen eines Monats 97 Milliarden Dateneinheiten aus Computer-Netzwerken überall auf der Welt gesammelt haben. Kritiker sprechen bereits von den „Vereinigten Daten von Amerika" – abgesegnet von einem im Geheimen tagenden Gericht, das die NSA zu der gigantischen Sammelaktion ermächtigt.

Peter Schaar, Datenschutzbeauftragter der Bundesregierung, spricht im Handelsblatt-Interview von einer völlig „neuen Dimension". Nicht nur Datenschützer kritisieren das Programm, auch die deutsche Wirtschaft ist alarmiert. „Das Ausmaß ist überraschend", sagt Volker Wagner, Chef der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW). Man müsse davon ausgehen, dass unter den Daten auch sensible Informationen deutscher Unternehmen sind. Denn die Firmen verlagern zunehmend Daten auf externe Server. Und viele Anbieter, die diese Speicherkapazität und Rechenleistung anbieten, kommen aus den USA.

Entsprechend groß ist die Sorge, ausgespäht zu werden. Je mehr Daten zusammenkommen, „desto größer wird die Gefahr, dass Daten missbräuchlich verwendet werden", warnt Wagner. Aus diesem Grund fordert der IT-Branchenverband Bitkom Kanzlerin Angela Merkel auf, die Überwachung beim Besuch von US-Präsident Barack Obama kommende Woche anzusprechen. Private und unternehmenskritische Daten müssen geschützt werden, mahnt Bitkom-Präsident Dieter Kempf.

Die neue Dimension der Datenkontrolle könnte für die deutsche Wirtschaft aber auch positive Auswirkungen haben, glauben IT-Experten wie Ralf Koenzen. „Jetzt kann kein Manager mehr behaupten, er habe die Risiken nicht erkannt", sagt der Chef von Lancom Systems, einem deutschen Hersteller von Routern, die Internet-Netzwerke steuern. Koenzen hofft, dass die amerikanische Sammelwut zu einem Umdenken bei deutschen Firmen führt und man künftig bei ausländischen IT-Angeboten genauer hinschaut: „Wir brauchen wieder mehr eigene Lösungen und Technologien."

Selbst in den USA wächst die Kritik an dem Datenhunger der Regierung. Die Öffentlichkeit und insbesondere die US-Verbündeten „haben ein Anrecht auf volle Information", sagte US-Senator John McCain dem Handelsblatt. Er könne „nur hoffen, dass die deutsche Regierung über Art, Inhalt und Ausmaß dessen informiert worden ist, was US-Behörden mit Blick auf die Überwachung tun".

Die Datensammelwut, wer sie publik machte und was davon zu halten ist Seiten 4 bis 7, 32, 54

Handelsblatt

Handelsblatt Nr. 109 vom 11.06.2013 Seite 001

Seite 1 Tagesthema

> Wenn die NSA ihr Analyseraster auf ein Unternehmen ausrichten würde, könnte sie gute Informationen über die Geschäftspraktiken bekommen, etwa über Übernahmeversuche.
>
> **Sandro Gaycken**
> Institut für Informatik an der FU Berlin

Ärger über einen Freund

Fortsetzung von Seite 1

SAP versucht erst gar nicht zu beschwichtigen. „Wenn die Regierung in den USA von unserer Tochtergesellschaft dort Informationen haben will, dann haben wir keine andere Wahl“, sagt ein Sprecher des weltgrößten Herstellers von Firmensoftware. Aber das wüssten die Kunden dort auch.

Gewusst oder nicht gewusst - die Datensammelwut der US-Regierung sorgt in der deutschen Wirtschaft für Unruhe. Wem kann ich meine Daten anvertrauen? fragen sich Unternehmer angesichts der Vorkommnisse jenseits des Atlantiks. Und Bernhard Rohleder, Hauptgeschäftsführer des IT-Branchenverbands Bitkom, glaubt: „Es ist nicht auszuschließen, dass in Deutschland ansässige IT-Unternehmen von der aktuellen Verunsicherung hinsichtlich des Datenschutzes in anderen Regionen der Welt profitieren.“

Es geht um das sogenannte Cloud-Computing. Dabei werden sowohl die Programme als auch die Daten in Rechenzentren gespeichert und über das Internet abgerufen. Große Cloud-Anbieter wie Hewlett-Packard, IBM oder Amazon kommen aus den USA. Schon seit einiger Zeit gibt es Zweifel, dass sie ihre Daten ähnlich wie die deutschen Rivalen T-Systems oder Datev vor dem Zugriff amerikanischer Behörden schützen können. Grund für die Zweifel ist der 2011 verlängerte „Patriot Act“. Nach diesem Gesetz dürfen US-Behörden bei Gefahr für die nationale Sicherheit Daten abfragen. Dabei ist es den IT-Konzernen noch nicht einmal erlaubt, ihre Kunden über den Zugriff zu informieren.

Die betroffenen IT-Firmen betonen zwar ihre Integrität. Unternehmen, die Cloud-Produkte nutzen, könnten sicher sein, dass deutsche Daten in Deutschland blieben, heißt es bei IBM. „Weitergegeben werden Daten nur in ganz wenigen Ausnahmen, etwa wenn ein Straftatbestand vorliegt“, sagte ein Sprecher.

Aber Zweifel bleiben - gerade bei deutschen Unternehmen. „Unsere Kunden fragen häufiger, ob die Daten in Deutschland und damit sicher seien“, bestätigt der SAP-Sprecher. Solche Sicherheiten garantieren zu können wird zu einem Verkaufsargument. Und das gilt auch, wenn es um die Hardware geht, also die Geräte. Denn es sind längst nicht nur autoritäre Regierungen wie die in China, die ihre Unternehmen zwingen, in ihren Produkten eine Hintertür für Spionage einzubauen. Auch die US-Regierung macht das seit längerem.

So ist bekannt, dass Cisco, ein amerikanischer Router-Spezialist, in seinen Geräten solche Spionagemöglichkeiten installiert. Der Konzern verweist auf seiner Webseite ausdrücklich auf die Vorgaben der US-Behörden, die unter dem Stichwort Calea publiziert wurden. Der wesentlich kleinere Cisco-Rivale Lancom aus Aachen hat seine Geräte deshalb bewusst vor kurzem durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen. Damit seien solche Zugriffe ausgeschlossen, sagt Lancom-Geschäftsführer Ralf Koenzen, der nun auf neue Kunden hofft.

Die Vorgänge in den USA einfach zu ignorieren, das kann sich kein deutsches Unternehmen erlauben. „Wenn die NSA ihr Analyseraster auf ein Unternehmen ausrichten würde, könnte sie gute Informationen über die Geschäftspraktiken bekommen, etwa über Übernahmeversuche“, warnt Sandro Gaycken vom Institut für Informatik an der Freien Universität Berlin.

Tatsächlich schafft der rasante Fortschritt der Technologien ganz neue Möglichkeiten. „Je mehr Daten vorliegen, desto genauer wird ein Personenprofil“, sagt Timo Kob, Vorstand der Sicherheitsberatung HiSolutions AG. So kann der US-Geheimdienst mit Hilfe von Software nicht nur speichern, wer wann welche Mail an wen verschickt. Bei angehängten Fotos startet auch die Gesichtserkennung und hinterlegt, wer auf dem Foto zu sehen ist und wo diese Person sonst noch auftaucht. Und was bei Personen geht, funktioniert auch bei Firmen. Sönke Iwersen, Ina Karabasz, Jens Koenen, Susanne Metzger

DIE MACHT DER NSA

Es ist ein Abschnitt im Überwachungsgesetz FISA, der dem US-Geheimdienst NSA weitreichende Befugnisse gibt. Wenn die National Security Agency Informationen über Nicht-Amerikaner von Konzernen wie Google oder Facebook einsehen will, muss er sich dafür die Genehmigung eines eigens für solche Fälle eingerichteten, geheim tagenden Sondergerichts besorgen. Die Genehmigung hat die NSA bislang immer bekommen. Das Gericht verpflichtet die betroffenen Unternehmen somit, sämtliche Informationen oder andere benötigte Hilfe an die NSA weiterzugeben. Im Gegenzug werden die Unternehmen für ihre Leistung entschädigt und sind immun gegen mögliche Klagen. Alle Gerichtsverfahren und richterlichen Entscheidungen in diesem Zusammenhang sind völlig intransparent.