Datenschutzrecht und Big Data

Beim „Security-Forum“ des Hagenberger Kreises am 17. und 18. April 2013 in der Fachhochschule Hagenberg, Oberösterreich, wurde unter anderem erörtert, wie das Sammeln und Verarbeiten großer Datenmengen mit dem Datenschutzgesetz vereinbar ist.

Ing. Roland Ledinger, Leiter des Bereiches IKT-Strategie des Bundes im Bundeskanzleramt, zeigte in seiner Keynote die strategische Dimension von Cybersecurity auf. Weltweit gibt es über 900 Millionen Facebook-User, davon 2,5 Millionen in Österreich. Das Internet nutzen zwei Milliarden Menschen. Es bestehen fünf Milliarden Handyverträge. Jeder Österreicher hat statistisch 1,5 Handys. 200 Milliarden E-Mails werden täglich verschickt. Der tägliche Datenzuwachs beträgt 15 Petabytes. In Deutschland waren 2010 durchschnittlich 350.000, in Spitzenzeiten bis zu 700.000 Rechner Teil eines Botnetzes.

Bei dieser Bedeutung des Cyberspaces als Informations- und Kommunikationsraum, sozialem Interaktionsraum, Wirtschafts- und Handelsraum sowie Steuerungs- und politischem Partizipationsraum kommt der Cyber-Sicherheit, der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten, der Legalität, Datensicherheit und dem Schutz der Privatsphäre, eine überragende Bedeutung zu.

Beginnend mit einer Auftaktveranstaltung am 16. November 2011 mit über 200 Teilnehmern aus den verschiedenen Interessensgruppen („Stakeholdern“), hat Österreich begonnen, eine nationale IKT-Sicherheitsstrategie zu entwickeln. Aus der Auftaktveranstaltung haben sich fünf Arbeitsgruppen gebildet, die am 2. März 2012 im Bundeskanzleramt erste Ergebnisse vorgestellt haben. Präsentiert wurde die „Nationale IKT-Sicherheitsstrategie Osterreich“ bei einer Abschlussveranstaltung am 15. Juni 2012 im Bundeskanzleramt.

Roland Ledinger: „Der Umgang mit Informations- und Kommunikationstechnik kann heute als vierte Kulturtechnik bezeichnet werden.“

Mohamed Chawki: „Das Bedrohungsbild ändert sich ständig, da technische Fähigkeiten der Kriminellen steigen.“

Kernpunkte sind die Einrichtung einer Cyber-Sicherheits-Steuerungsgruppe, die Schaffung einer Struktur zur Koordination auf operativer Ebene, die Einrichtung eines übergreifenden Cyber-Krisenmanagements, die Stärkung bestehender Strukturen, die Festlegung von Mindestsicherheitsstandards und die Erstellung eines Code of Conduct, der unter anderem einen Informationsaustausch und Meldepflichten vorsieht.

Besonderen Nachholbedarf gebe es im Bildungswesen, berichtete Ledinger aus dem Strategiepapier. Neben Lesen, Schreiben und Rechnen könne der Umgang mit IKT heute als „vierte Kulturtechnik“ bezeichnet werden, die, verbunden mit IKT-Sicherheit, bereits in die Lehrpläne und den Unterrichtsalltag ab Volksschulniveau aufzunehmen sei und integraler Bestandteil des Unterrichts in allen Schultypen werden müsse. Voraussetzung für die Vermittlung von IKT-(Sicherheits)-Kompetenzen sei, diese Kompetenzen in die Ausbildung an pädagogischen Hochschulen und Universitäten aufzunehmen. Eine Schwerpunktbildung durch einen speziellen Schultypus, vergleichbar etwa Sport- und Musikschulen, wird empfohlen. IKT-Sicherheit wurde auch als wichtiger Bestandteil in der Erwachsenenbildung und Weiterbildung bezeichnet, auch für die Generation 65+.

Die „Österreichische Strategie für Cyber-Sicherheit“ wurde am 20. März 2013 von der Bundesregierung beschlossen. Auf EU-Ebene wurde von der Europäischen Kommission am 7. Februar 2013 der Entwurf einer *Netz- und Informationssicherheits-Richtlinie (NIS-RL)* vorgestellt, die derzeit in 15 Arbeitsgruppen behandelt wird. Als strategische Prioritäten werden angesehen die Erhöhung der Widerstandsfähigkeit der IKT-Systeme, die Eindämmung der Cyber-Kriminalität und der Ausbau der Cyber-Verteidigung, die Entwicklung von industriellen Cyber-Ressourcen sowie eine einheitliche Cyberstrategie auf internationaler Ebene.

FH Hagenberg: Veranstaltungsort des „Security Forums“.

„Big Data – Big Liability?“ Unter diese Frage stellte Dr. Lukas Feiler, Rechtsanwaltsanwärter bei der Wirtschaftskanzlei *Baker&McKenzie,* Wien, sein Referat. Der Begriff „Big Data“ umschreibt große, in der Regel unstrukturierte Datenmengen, aus denen, als eine Form des Data-Minings, mit Hilfe besonderer dafür entwickelter Algo-

Fotos: Kurt Hickisch

rithmen neue Erkenntnisse gewonnen werden. Die Daten selbst können aus den verschiedensten Quellen stammen, wie etwa Verkauf und Marketing, Finanz- und Rechnungswesen, Kundenbindungsprogramme, Produktmanagement, betrieblicher Korrespondenz, oder aus sozialen Medien, Audio- und Videomaterial, RFID-Scans, Geo-Daten oder aus einer Machine-to-Machine (M2M)-Kommunikation.

Der Verwendungszweck kann im Wirtschaftsleben darin bestehen, das Kundenverhalten zu prognostizieren, etwa, um Werbung personenbezogen, also mit möglichst wenig Streuverlusten, einzusetzen. Das kann auch zu Diskriminierungen führen: Wirtschaftlich leistungsfähigeren Personen wird man keine Rabattaktionen mehr anzubieten brauchen, und Stammkunden keine Gutscheinaktionen (Price Discrimination). Der tatsächliche Personalbedarf lässt sich durch Analyse der Verkaufsdaten leichter ermitteln.

Im Bereich des Risiko-Managements können frühzeitig Entwicklungen erkannt werden. Durch auftretende Anomalien können Kreditkarten-Firmen erkennen, ob die Kreditkarte eines Kunden kompromittiert wurde und unbefugt verwendet wird, sodass Transaktionen, für die das Unternehmen haften müsste, unterbleiben.

Der Verwendung von personenbezogenen Daten aus verschiedenen Anwendungen über deren ursprünglichen Zweck hinaus steht § 6 Abs. 1 Z 2 DSG 2000 entgegen. Anonymisierung hilft nur bedingt. Ein Personenbezug kann in vielen Fällen wieder hergestellt werden. Beispielsweise bilden Standortdaten das eindeutige Bewegungsmuster einer bestimmten Person ab. Damit gilt das Datenschutzgesetz weiterhin.

Angriffspunkte für Cyber-Terrorismus ist vor allem die kritische Infrastruktur, wie der Flug- und Schienenverkehr.

Foto: Dieter Höller

Dass sich alle Daten in einem einzigen System befinden, stellt des Weiteren ein Sicherheitsproblem dar. § 14 DSG schreibt risiko-adäquate Sicherheitsmaßnahmen vor. Neue Auswertungsmöglichkeiten schaffen neue Risiken. „Big data needs big security“. Wie kann in diesem System, in dem eine Zugriffsmöglichkeit auf alle Daten besteht, gewährleistet werden, dass jeder Anwender nur so weit zum Zugriff berechtigt ist, dass er seine Aufgaben erfüllen kann (§ 14 Abs. 2 Z 5 DSG), noch dazu, wo es sich oft um unstrukturierte und dynamische Daten handelt? Eine manuelle Rechtevergabe scheidet wohl aus. Denkbar wäre ein Sicherheitssystem, das auf Grund des bisherigen Nutzerverhaltens entscheidet, auf welche Datenkategorien zugegriffen werden darf (Access Management).

Paradigmenwechsel. Das DSG schreibt vor (u. a. § 27 Abs. 1), dass nicht mehr benötigte Daten zu löschen sind. Big Data sieht aber Daten nicht mehr als unnötigen Ballast an, sondern als zu bewahrenden Schatz, für den sich möglicherweise neue Verwendungsmöglichkeiten ergeben – zumal Speicherplatz fast nichts mehr kostet.

Diese neue Sichtweise widerspricht der Zweckbindung nach § 6 Abs. 1 Z 2 DSG, wonach personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen. Eine Speicherung auf Vorrat für undefinierte Zwecke ist demnach unzulässig. Jede Zweckänderung stellt eine neue Datenanwendung dar und begründet neue Registrierungs- und Zustimmungspflichten.

Das Anlegen eines Datenschatzes läuft auch dem Prinzip der Datensparsamkeit nach § 6 Abs. 1 Z 3 DSG zuwider, wonach die Verwendung von personenbezogenen Daten nur zulässig ist, soweit sie für den festgelegten Zweck wesentlich ist und über diesen Zweck nicht hinausgeht. Die Lösung sieht Feiler aus Unternehmenssicht darin, die Verarbeitungszwecke vorausschauend zu definieren, also nicht aus heutiger Sicht, sondern für welche Zwecke die Daten in drei Jahren verwendet werden können. Das sollte bei den Meldungen an die Datenschutzkommission und bei der Formulierung von Zustimmungserklärungen Betroffener berücksichtigt werden.

Bei Rückgriff auf Big Data ergeben sich ferner verschärft Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen ohne menschlichen Plausibilitäts-Check. An die Qualität und Vollständigkeit der Daten und deren Integrität sind besonders hohe Anforderungen zu stellen sowie die Datenquellen und ihr Sicherheitsstandard zu überprüfen. Nicht geeignete Datenquellen können eine zivilrechtliche Haftung gegenüber Vertragspartnern wegen Verletzung vertraglicher Nebenpflichten begründen.

Vollautomatisierte Entscheidungen sind nach § 49 DSG unzulässig, wenn sie für den Betroffenen rechtli-

che Folgen nach sich ziehen oder ihn erheblich beeinträchtigen und die Entscheidung auf Grund der automationsunterstützten Verarbeitung von Daten zur Bewertung einzelner Persönlichkeitsaspekte des Betroffenen erfolgt, etwa seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens. Ausnahmen sind zulässig, wenn die Wahrung der berechtigten Interessen des Betroffenen garantiert wird, beispielsweise durch die Möglichkeit, seinen Standpunkt geltend zu machen (§ 49 Abs. 2 Z 3 DSG). Bei zulässigen automatisierten Einzelentscheidungen ist dem Betroffenen auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form darzulegen (§ 49 Abs. 3). Als Beispiele für vollautomatisierte Entscheidungen, die rechtliche Folgen oder erhebliche Beeinträchtigungen für die Betroffenen bringen, nannte Feiler:

- die Entscheidung über die Nichtgewährung von Mitarbeiter-Boni auf Grundlage der errechneten Leistungsfähigkeit,
- eine Kreditverweigerung wegen errechneter Unzuverlässigkeit sowie
- Entscheidungen über Art des Implantats auf Grundlage der errechneten Lebenserwartung und der „Lebensfreude".

„Big Data stellt erhöhte Sicherheitsanforderungen und erfordert menschliche Kontrolle", betonte Feiler.

Cybercrime. Über Begehungsformen und die Verhinderung von Cybercrime referierte Dr. Mohamed Chawki, Experte auf dem Gebiet der HiTec-Kriminalität und Präsident der *International Association of Cybercrime Prevention (www.cybercrime-fr.org)*. Diese Non-Profit-Organisation mit Sitz in Paris hat zum Ziel, das Bewusstsein gegenüber Cybercrime zu heben. Diesem Zweck haben unter anderem internationale Konferenzen in Ägypten (2008), Brasilien, dem Libanon, in den USA (2010) und zuletzt 2012 in Frankreich gedient.

Cyber-Kriminalität: Die hauptsächlichen Bedrohungen sind Cyber-Spionage, Angriffe gegen Finanzdienstleistungen und Identitätsdiebstahl.

Der sich ständig vergrößernde Umfang des Cyberspaces, über den zwölf Prozent des weltweiten Handels abgewickelt werden, lässt die Möglichkeiten für Cyber-Kriminalität anwachsen. Für den Cyber-Raum typisch ist die Möglichkeit automatisierter Angriffe, die Attacken profitabler machen sowie, dass die Täter aus der Entfernung agieren können und die Verbreitung von Angriffstechniken ist leichter und schneller möglich ist. Die hauptsächlichen Bedrohungen sieht Chawki im Cyber-Terrorismus, in der Cyber-Spionage, in den Botnetzen und Angriffen gegen Finanzdienstleistungen, wie Phishing und Identitätsdiebstahl.

Angriffspunkte für Cyber-Terrorismus sei vor allem kritische Infrastruktur, wie der Flug- und Schienenverkehr. Das Netz ermögliche die Propaganda für terroristische Ziele, das Anwerben und die Ausbildung von Sympathisanten, das Sammeln von Informationen und die Kommunikation untereinander. Zur Bekämpfung des Phishings wurde 2003 die *Anti-Phishing Working Group (APWG)* als internationales Konsortium gegründet *(www.AntiPhishing.org)*. Identitätsdiebstahl kann weitreichende Folgen haben, wenn der eigene Name zur Erstellung gefälschter Dokumente, Eröffnung von Bankkonten oder Aufnahme von Krediten missbraucht wird.

Verdächtige E-Mails und Software sollten automatisch erkannt und blockiert und es sollten Möglichkeiten entwickelt werden, die Echtheit von E-Mails überprüfen zu können. Die Weitergabe sensibler Informationen an nicht vertrauenswürdige Empfänger sollte automatisch abgeblockt werden. In Anbetracht der steigenden technischen Fähigkeiten der Kriminellen müsste Bewusstsein dafür geschaffen werden, dass sich das Bedrohungsbild ständig ändere, und es müsste, auch in der Gesetzgebung, entsprechend darauf reagiert werden.

Florian Oelmaier: „Bei gezielten Spionage-Angriffen ist immer ein Innentäter im Spiel."

Lukas Feiler: „Big Data stellt erhöhte Sicherheitsanforderungen und erfordert menschliche Kontrolle."

Industriespionage. Florian Oelmaier von *Corporate Trust,* München *(www.corporate-trust)* zeigte anhand von Beispielen auf, wie Industriespionage-Angriffe vorbereitet werden. IT-Sicherheitsabteilungen bekämpfen fast zur Gänze nur Cybercrime („Laufen den Viren nach"), während Industriespionage nur zufällig erkannt werde. Bei gezielten Angriffen sei immer ein Innentäter im Spiel. Wegen der Gefahr der Rufschädigung werde über solche Vorfälle oft geschwiegen.

Kurt Hickisch

Hagenberger Kreis zur Förderung der digitalen Sicherheit: www.hagenberger-kreis.at; www.securityforum.at

FOTOS: KURT HICKISCH (2), EGON WEISSHEIMER