Rasche Information

Die Herausforderungen durch die Datenschutzgesetz-Novelle 2010 waren ein zentrales Thema beim 8. Security Forum des Hagenberger Kreises.

Nach § 24 Abs. 2a des Datenschutzgesetzes (DSG) 2000 in der seit 1.1.2010 geltenden Fassung durch die Novelle BGBl I 2009/133 hat der Auftraggeber, wenn ihm bekannt wird, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

Fachhochschule Hagenberg: Veranstaltungsort der jährlichen IKT-Sicherheitskonferenz des Hagenberger Kreises.

„Diese Data Breach Notification Duty stammt aus dem US-amerikanischen Recht und ist über Großbritannien nach Europa gekommen“, erläuterte Mag. Patrik Kutschi, Forensic Manager bei *KPMG*. „Sie ist in den USA bereits zu einem eigenen Wirtschaftszweig geworden. Bei der Umsetzung haben Deutschland und Österreich in Europa eine Vorreiterrolle übernommen.“

Wer diese Informationspflicht verletzt, begeht eine Verwaltungsübertretung nach § 52 Abs. 2 Z 4 DSG, die mit Geldstrafe bis zu 10.000 Euro bedroht ist. „Damit aber ist es nicht getan“, sagte Kutschi. „Bewusstes Negieren der Pflicht könnte zivilrechtlich als eigenständige rechtswidrige Handlung gesehen werden, aus der ein direktes Verschulden abgeleitet werden kann.“ Auch wenn das Unternehmen selbst als Opfer anzusehen wäre, trifft es die zivilrechtliche Schadensminimierungspflicht nach § 1304 ABGB: Das Unternehmen muss alles unternehmen, um den Eintritt oder die Vergrößerung des Schadens für den Betroffenen zu verhindern. Insofern liegt ein Schutzgesetz im Sinn des § 1311 ABGB vor. Bei Verletzung der Schadensminimierungspflicht kann der Versicherer die Deckung des Schadens verweigern. Als Beispiel führte Kutschi an, dass von einem liechtensteinischen Gericht zumindest in erster Instanz einem deutschen Staatsbürger der Betrag von 7,3 Millionen Euro als Entschädigung zugesprochen wurde. Seine Vermögensdaten hatten sich auf einer „Steuer-CD“ befunden, deren darauf enthaltene Daten zu Erhebungen der deutschen Finanzbehörden und entsprechenden Finanzstrafen geführt hatten. Wäre er, so die Argumentation des Klägers, vom Finanzinstitut vom „Datenklau“ verständigt worden, hätte er durch rechtzeitige Selbstanzeige Straffreiheit oder eine geringere Bestrafung erlangen können. Nicht nur der versehentlich zurückgelassene Laptop, sondern auch die CD oder DVD, der verlorene USB-Stick, oder der zur Reparatur gegebene PC werden, wenn sie personenbezogene Daten enthalten, aus dem Blickwinkel dieser Verständigungspflicht gesehen werden müssen. Inwieweit ein Passwortschutz oder eine Verschlüsselung der gespeicherten Daten ausreichen, wird sich wahrscheinlich erst aus der Judikatur ergeben.

„Unternehmen sind gut beraten, ein effektives Informationssicherheitsmanagement zu implementieren, besondere Risikobereiche zu identifizieren, die Versicherungsbedingungen zu überprüfen und eine rasche Reaktion im Anlassfall sicherzustellen“, stellte Kutschi fest. „Dazu gehört auch die Entwicklung eines „Data Breach Response Plans“, die Einsetzung eines „Data Breach Response Teams“ und die Durchführung einer ‚Feuerübung‘.“

Was die ebenfalls durch die DSG-Novelle 2010 erfolgte Regelung der privaten Videoüberwachung betrifft, wies Kutschi auf die Ausweitung der Bestimmung des § 52 Abs. 4 DSG hin, wonach nunmehr auch der Verfall von Bildübertragungs- und Bildaufzeichnungsgeräten ausgesprochen werden kann, wenn diese Gegenstände mit einer Verwaltungsübertretung nach § 52 Abs. 1 oder 2 in Zusammenhang stehen. Diese Nebenstrafe kann somit auch verhängt werden, wenn eine Videoüberwachung nicht gemäß den Bestimmungen der §§ 17 ff DSG gemeldet wurde, was eine Verwaltungsübertretung nach § 52 Abs. 2 Z 1 DSG darstellt. Von der Meldepflicht ausgenommen ist eine (private) Videoüberwachung in Fällen der Echtzeitüberwachung oder wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt (§ 50c Abs. 2 Z 1 und 2). – Nach der zwischenzeitig erfolgten Rechtsentwicklung (Änderung der Standard- und Muster-Verord-

FOTO: KURT HICKISCH

DIGITALE SICHERHEIT

Hagenberger Kreis

Der Verein „Hagenberger Kreis zur Förderung der digitalen Sicherheit“ wurde im Jahr 2002 von Studenten des Fachhochschulstudiengangs „Computer- und Mediensicherheit“ in Hagenberg, OÖ, gegründet. Ziel des Vereins ist es, das Sicherheitsbewusstsein im IKT-Bereich vor allem in Unternehmen, aber auch in privaten Haushalten zu heben. Zu diesem Zweck veranstaltet der Verein seit 2003 alljährlich an der FH Hagenberg das Security Forum. Am 8. Security Forum am 24. März 2010 nahmen etwa 150 Interessierte teil; am 25. März gab es Workshops. Das Motto der Veranstaltung: „Achtung: Fehlende IKT-Sicherheit fügt Ihnen erheblichen Schaden zu.“

www.hagenbergerkreis.at
www.securityforum.at

Patrik Kutschi: „Firmen sollen Datenschutzplan entwickeln.“

nung 2004 durch BGBl II 2010/152, in Kraft seit 28. Mai 2010) fällt die Videoüberwachung von Banken; Juwelieren, Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmied; Trafiken; Tankstellen und bebauten Privatgrundstücken (samt Hauseingang und Garage) als SA032 der Anlage 1 unter die StMV 2004, sofern die Datenanwendung in dem dort vorgegebenen Rahmen erfolgt. Datenanwendungen, die einer Standardanwendung entsprechen, sind nicht meldepflichtig (§ 17 Abs. 2 Z 6 DSG; § 1 Abs. 1 StMV).

Besonderes Augenmerk ist auch auf die Strafbestimmung des § 52 Abs. 2 Z 2 DSG zu legen: Wer Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 Abs. 1 eingeholt zu haben, begeht eine Verwaltungsübertretung, die mit einer Geldstrafe bis zu 10.000 Euro zu ahnden ist. Dies ist zu beachten in Fällen des Outsourcing von Datenverarbeitungen in Staaten außerhalb des Europäischen Wirtschaftsraums bzw. in solche, die über keinen angemessenen Datenschutz verfügen (§ 12 Abs. 1 und 2; Datenschutzangemessenheits-Verordnung – DSAV, BGBl II 1999/521). Ein „Konzernprivileg“, dass innerhalb eines Konzerns Daten ohne Rücksicht auf den Ort der tatsächlichen Verarbeitung verarbeitet werden dürften, gibt es nicht. Vollends problematisch wird es, wenn Daten „in the cloud“ verarbeitet werden, also im Internet, ohne dass lokalisierbar ist, wo gerade die Verarbeitung erfolgt.

„Auch wenn man eine Bedrohung nicht spürt, ist sie trotzdem da“, referierte Oberst Mag. Walter Unger, Leiter der IKT-Sicherheit des Abwehramts des BMLVS, und betonte die Wichtigkeit der Sicherung kritischer Infrastrukturen wie etwa im Bereich Energie, Transport, Telekommunikation, die das Rückgrat der Informationsgesellschaft bilden. Außerdem warnte er vor dem zu sorglosen Umgang mit personenbezogenen Daten in sozialen Netzwerken: „Das Netz gibt Daten nie wieder her“.

Kurt Hickisch

FOTO: KURT HICKISCH