INTERVIEW

Wolfgang A. Schmid, Fachanwalt für IT-Recht, über die Rolle des Datenschutzbeauftragten

Datenschutz in Zeiten des Mobile Device Managements

Wie können private, mobile Endgeräte der Mitarbeiter sicher ins Unternehmensnetz integriert werden? Die Kompetenzen bei Einsicht und Verwendung der Daten müssen klar definiert sein, meint Rechtsanwalt Wolfgang A. Schmid im Gespräch mit IT-BUSINESS. Die Rolle des Datenschutzbeauftragten wird immer wichtiger. IT-BUSINESS / Das Interview führte Dr. Andreas Bergler

Zur Person

Wolfgang A. Schmid ist Rechtsanwalt und Fachanwalt für IT-Recht. Er beschäftigt sich seit vielen Jahren mit Rechtsfragen rund um Software und Hardware-Verträge, Internet und Datenschutz. Er bildet seit 2004 Datenschutzbeauftragte aus. Neben seiner anwaltlichen Tätigkeit in den Bereichen IT-Recht, Handels- und Vertragsrecht ist er bei verschiedenen Unternehmen als externer Datenschutzbeauftragter bestellt. Er ist Referent der Deutschen Anwaltsakademie für IT-Recht.

web | www.rechtsanwalt-schmid.com

ITB: Herr Schmid, Sie sind Datenschutzbeauftragter bei dem Augsburger Management-Software-Anbieter baramundi. Warum braucht Ihr Kunde das?

SCHMID: Ab einer Größe von zehn Mitarbeitern, schreibt das Gesetz vor, braucht jedes Unternehmen einen Datenschutzbeauftragten. Per definitionem darf ein Datenschutzbeauftragter nicht gleichzeitig der IT-Leiter sein. Er muss rechtlich, technisch, organisatorisch und betriebswirtschaftlich fundiert ausgebildet sein und ist darüber hinaus unkündbar. Es kann auch ein externer Spezialist sein. Hier bei baramundi und mir ist es so, dass wir schon seit vielen Jahren erfolgreich zusammenarbeiten. baramundi legt Wert darauf, nur Produkte im Portfolio zu führen, deren Arbeitsweise und Implementierung rechtlich einwandfrei gewährleistet sind. Dies betrifft in besonderem Maße die Lösungen Remote Control, Device Control, Energy Management und Mobile Devices sowie die Überwachung der Ausführung von Applikationen. Da bot es sich an, neben der juristischen Beratung bei der Produktentwicklung den organisatorischen Part mit zu übernehmen.

ITB: Wodurch muss ein betrieblicher Datenschutzbeauftragter qualifiziert sein?

SCHMID: Grundlegende Kenntnisse für Datenschutzbeauftragte können schon in zweitägigen Seminaren angeeignet werden. Die übliche Ausbildung dauert zehn bis zwölf Tage mit einer abschließenden Prüfung durch die jeweiligen Datenschutz-Aufsichtsbehörden in den Bundesländern. Der Düsseldorfer Kreis hat hier einige Kriterien zusammengetragen. Darunter fallen Grundkenntnisse zu den Rechten der Mitarbeiter und den einschlägigen Regelungen des Bundesdaten-

schutzgesetzes, BDSG, sowie Kenntnisse in den Datenschutz-Anforderungen in technischer und organisatorischer Hinsicht. Der Datenschutzbeauftragte muss zu entsprechenden Sachverhalten Stellung nehmen können und sollte regelmäßige Fortbildungsnachweise erbringen. Zum Beispiel sollte er sich auch durch Fachzeitschriften auf dem Laufenden halten.

ITB: Was hat er dann konkret im Unternehmen zu tun?

SCHMID: Er muss darauf achten, dass die Datenschutz-Bestimmungen tatsächlich umgesetzt werden. Das bezieht sich nicht nur auf das BDSG, sondern auch auf das Fernmeldegeheimnis und die TK-Überwachung bei VoIP-Anlagen oder auch die Nutzung privater Mails in den Unternehmen. Er muss dann beispielsweise darauf achten, dass bei einer privaten Nutzung der betrieblichen E-Mail-Infrastruktur nur Daten zur Sicherstellung des Geschäftsbetriebs erhoben werden, die dafür tatsächlich gebraucht werden. Er sollte darüber hinaus ein Datenschutz-Konzept für sein Unternehmen erarbeitet haben, dessen Einhaltung mindestens einmal im Jahr überprüft und reportet wird.

ITB: In welcher Hinsicht zeichnen sich die von Ihnen angesprochenen Produkte von baramundi rechtlich aus?

SCHMID: Mit der Lösung „Mobile Devices" lassen sich zum Beispiel die Sicherheitsrichtlinien eines Unternehmens auf die mobilen Endgeräte übertragen. Die Lösung garantiert die Compliance, die Einhaltung dieser Regeln …

ITB: Tun das nicht auch andere Endpoint-Security-Lösungen?

SCHMID: Ja, aber baramundi geht hier einen Schritt weiter. Denn der Hersteller beansprucht, der einzige deutsche Clientmanagement-Hersteller am Markt mit einer selbst entwickelten Mobile-Device-Management-Lösung zu sein.

ITB: Ja und?

SCHMID: Das macht einen großen Unterschied zu anderen Anbietern. Denn die kommen nämlich zumeist aus den USA. Laut Patriot Act müssen aber alle US-amerikanischen Lösungen so genannte Backdoors bereitstellen, die gewährleisten, dass staatliche Stellen im Zweifelsfall – den sie natürlich selbst definieren – auf Daten und Informationen zugreifen können, die über diese Systeme gemonitort werden. Solche eingebauten Möglichkeiten für den Zugriff von außen verstoßen in Deutschland gegen das Datenschutzgesetz. Bei der hier vorliegenden Lösung ist eine solche Art der Überwachung technisch nicht möglich. Als Datenschutzbeauftragter, der gleichzeitig Einblick in die Produktentwicklung hat, kann ich das attestieren.

ITB: Was bedeutet das für die Anwender?

SCHMID: Dass die Daten, die das „Mobile Devices"-System für das Monitoring zusammenstellt, nicht auf den einzelnen Mitarbeiter heruntergebrochen werden können. Die Informationen, die er überträgt, können ihm also nicht von dem System wieder zugeordnet werden. Für die Unternehmensführung hat dies eben den Vorteil, sowohl compliant zu sein, was die Einrichtung entsprechender Security-Maßnahmen und -Systeme sowie die Etablierung einheitlicher Sicherheitsstandards betrifft, als auch konform mit den hierzulande herrschenden Datenschutz-Bestimmungen zu gehen.

ITB: Das bedeutet für die Geschäftsführung, …

SCHMID: … dass sie mit der Einrichtung von adäquaten Sicherungsmechanismen für die Unternehmens-IT ihren Haftungsanforderungen Genüge getan hat. Denn die IT-Risikovorsorge gehört zu den Aufgaben eines ordentlichen Geschäftsmannes, und ein Mobile Device Management ist heute in den meisten Unternehmen unabdingbarer Part einer solchen Strategie.

ITB: Deutschland gilt im internationalen Vergleich derzeit als unangefochtener Spitzenreiter, was die Vorschriften zum Datenschutz betrifft. Was wird sich mit Einführung der europäischen Datenschutz-Grundverordnung ändern, die Anfang des Jahres auf Europa-Ebene diskutiert wurde?

SCHMID: Die Datenschutzrichtlinie 95/46/EG gibt zur Zeit gewisse Mindeststandards vor, an die sich die europäischen Staaten halten müssen. An ihrer Umsetzung wird derzeit aber immer noch gefeilt. Durch die europaweite Vereinheitlichung der von Ihnen angesprochenen Grundverordnung soll zum Beispiel auch das „Recht auf Vergessenwerden" verankert werden. Die europäischen Vorschriften heben jedoch den Datenschutz teilweise sogar auf. So könnte die Stellung des Datenschutzes und des damit Beauftragten geschwächt werden. Das Ganze soll allerdings erst in den kommenden Jahren spruchreif werden, und bis dahin werden auch außereuropäische, große Unternehmen an der Diskussion teilnehmen. □

Mobile Devices und Clients

Mit „baramundi Mobile Devices" lassen sich geltende Sicherheitsrichtlinien auf Smartphones, Tablets & Co. umsetzen. „baramundi Device Control" regelt den Zugriff auf Medien, Geräte oder Ports im Unternehmen und sorgt für einen regelkonformen Datenfluss an den Clients. Gleichzeitig gibt „baramundi Application Control" nach dem Whitelist-Prinzip nur genehmigte Anwendungen für den Einsatz im Unternehmen frei. Die Administration der Mobilgeräte läuft über das Client- und Server-Management der „baramundi Management Suite".

baramundi software AG
baramundi software AG
Beim Glaspalast 1
86153 Augsburg
Fon: +49 (821) 5 67 08-380
Fax: +49 (821) 5 67 08-19
request@baramundi.de
web | www.baramundi.de