Bedingt mandantenfähig

Bei Konsolidierungen der IT-Infrastruktur oder Shared Cloud Services spielen „Corporate Separateness“ und Mandantentrennung eine oft unterschätzte Rolle.

Von **Michael Rath***

Um verteilte IT-Systeme zu zentralisieren und zu konsolidieren, aber auch aus reinen Kostengründen nutzen viele Unternehmen heute schon kooperative Betriebsmodelle. Dazu zählen Shared beziehungsweise Public Cloud Services oder gemeinsame Rechenzentren. Doch vor allem die Großkonzerne stoßen dabei auf ein Problem: Aufgrund der Anforderungen des Datenschutzes und der „Corporate Separateness“ sehen sie sich mit erhöhten Anforderungen an die Mandantenfähigkeit der Systeme konfrontiert. Die gemeinsame Nutzung einer „geteilten“ Infrastruktur unterliegt strengen Vorgaben an die Trennung der (personenbezogenen) Daten.

Behördliche Orientierungshilfe

Im Rahmen ihrer 84. Konferenz haben die deutschen Datenschutz-Aufsichtsbehörden am 7. und 8. November des vergangenen Jahres in Frankfurt an der Oder eine Orientierungshilfe zur Mandantenfähigkeit von IT-Systemen verabschiedet. In dieser Empfehlung werden die Schritte dargestellt, die aus Datenschutzsicht notwendig sind, um eine ausreichende Trennung von DV-Verfahren zu überprüfen. Darüber hinaus liefert sie konkrete Hinweise, wie sich Datenschutz- und Informationssicherheits-Management-Systeme (DSMS/ISMS) ausgestalten lassen. Nachfolgend sind diese Vorgaben zusammengefasst.

Definition Mandantentrennung

Der Begriff „Mandantenfähigkeit“ bedeutet, dass es dem Unternehmen und den von ihm eingesetzten IT-Systemen möglich sein muss, die Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit (im Fachjargon: Data Segregation) lassen sich beispielsweise die Daten unterschiedlicher Abteilungen eines Unternehmens oder verschiedener Kunden eines Rechenzentrums getrennt speichern und verarbeiten.

Corporate Separateness

Die Notwendigkeit zur Mandantentrennung ergibt sich für Konzerngesellschaften nicht nur aus den Datenschutzgesetzen der Länder, sondern auch aus dem gesellschaftsrechtlichen Prinzip der „Corporate Separateness“. Dieser Grundsatz besagt in etwa, dass jede Gesellschaft oder rechtliche Person als eigenständig zu behandeln ist.

Ausnahmen gelten im Konzernrecht unter anderem dann, wenn ein Unternehmen eines oder mehrere andere dominiert, also wenn zwischen den Unternehmen ein Beherrschungs- oder Gewinnabführungsvertrag besteht (Verlustausgleichspflicht). Im Allgemeinen geht es aber effektiv darum, die Eigenständigkeit von Gesellschaften anzuerkennen und zu beachten. So wird in diesem Zusammenhang auch von den Wirtschaftsprüfern verlangt, dass die Buchführungssysteme der Unternehmen streng getrennt werden müssen.

Datenverarbeitung im Konzern

Für Konzerne gibt es keine zwingenden Vorgaben, wie die gemeinsame Datenverarbeitung technisch ausgestaltet sein muss. Es wäre grundsätzlich auch denkbar, die IT-Systeme verschiedener Konzerngesellschaften in einem Rechenzentrum oder gar auf einem Server zu betreiben – sofern und solange eine physikalische oder zumindest logische Trennung gegeben und darüber hinaus die Einhaltung des Datenschutzes gewährleistet ist.

Es gibt kein Konzernprivileg. Also darf jedes Unternehmen (als datenschutzrechtlich verantwortliche Stelle) zunächst nur Zugriff auf „seine eigenen“ personenbezogenen Daten haben. Es sei denn, die Datenübermittlung an die andere Konzerngesellschaft ist jeweils legitimiert. Übergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur müssen grundsätzlich so beschaffen sein, dass sie keine Verarbeitung personenbezogener Daten eines anderen Unternehmens ermöglichen. Doch auch hier gilt eine Ausnahme: wenn die Datenverarbeitung etwa durch einen Auftragsdatenverarbeitungs-Vertrag oder konzerninterne Regelungen (Binding Corporate Rules) legitimiert ist.

Vorgaben der Aufsichtsbehörden

Eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten ist nach Ansicht der Datenschutzaufsichts-Behörden nur zulässig, wenn die Daten jeweils mandantenbezogen geführt werden. Darüber hinaus müssen sich Verarbeitungsfunktionen, Zugriffsberechtigungen (Segregation of Duties) und Konfigurationseinstellungen für jeden Mandanten eigenständig festlegen lassen.

Wie die Trennung der Datenverarbeitung konkret umgesetzt wird, sollte sich am Schutzbedarf der Daten orientieren. Handelt es sich um besonders sensible Daten, beispielsweise aus dem Gesundheitswesen, oder um streng vertrauliche Unterlagen, so

Foto: marog-pixcells/Fotolia

sind die aus der gemeinsamen Nutzung einer IT-Infrastruktur entstehenden Risiken möglicherweise zu hoch. Dann entfällt die Möglichkeit zur Infrastrukturkonsolidierung oder Nutzung von Public Cloud Services.

Zugriffsrechte und Konfigurationen

Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen, Verarbeitungsfunktionen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden. Zudem müssen mandantenspezifische Benutzerkennungen angelegt werden, um sicherzustellen, dass mit diesen Kennungen nur auf Daten des jeweiligen Mandanten zugegriffen werden kann. Notwendig sind also eine getrennte Berechtigungsvergabe und unterschiedliche Konfigurationsmöglichkeiten.

Der Admin darf nicht alles

Mandantenübergreifende Datenzugriffe sind weiterhin nur in begründeten Ausnahmefällen zulässig, so etwa für die erstmalige Einrichtung des mandantenspezifischen Berechtigungssystems und in Notfallsituationen. Die Vergabe von Admin-Berechtigungen ist deshalb restriktiv zu handhaben; Nutzern auf Anwendungsebene dürfen solche Rollen nicht zugeordnet werden. Doch gerade in der Cloud sind die Berechtigungskonzepte nicht immer streng differenziert.

IT-Compliance und Risikoanalyse

Unternehmen sollten daher unbedingt eine Risikoanalyse in Bezug auf die gemeinsame Nutzung von IT-Ressourcen vornehmen – nicht nur wegen datenschutzrechtlicher Anforderungen der Aufsichtsbehörden, sondern auch, um persönliche Haftung zu vermeiden. Die IT-Risikoanalyse dient – im Sinne der IT-Compliance – dazu, eine Überprüfung nachzuweisen: dass die Gefahren für die Rechte der Betroffenen durch angemessene technische und organisatorische Sicherheits- und Datenschutzmaßnahmen beherrscht werden können.

Zu beachten sind hierbei die speziellen Risiken für Vertraulichkeit, Integrität und Verfügbarkeit bei der Datenverarbeitung auf einer gemeinsamen IT-Infrastruktur. Auch das Verbleiben etwaiger Restrisiken darf nicht außer Acht gelassen werden. Auf dieser Grundlage werden dann die Maßnahmen in Bezug auf eine Trennung der Daten umgesetzt – hinsichtlich Datenhaltung, Datenverarbeitung und Datentransport. Die erfolgreiche Implementierung ist schließlich zu dokumentieren. *(qua)*

***Dr. Michael Rath** ist Fachanwalt für IT-Recht und Partner der Luther Rechtsanwaltsgesellschaft mbH in Köln.

CW KOMMENTAR

Heiliger Gral in den Händen der EU-Templer

Mit dem Kauf dieses Artikels erklären Sie sich mit unserer Cookie-Policy einverstanden.“ Diesem Satz begegnet man auf Online-Einkaufsplattformen neuerdings häufiger. Noch Fragen? Ach, Sie wollen diese Policy tatsächlich lesen? Sind Sie etwa der Typ, der AGB studiert, bevor er den „Buy“-Knopf drückt? Und der im Zweifelsfall lieber ein günstiges Angebot sausen lässt, als dass er Gefahr läuft, sich durchleuchten zu lassen?

Google, Facebook und Co. nehmen das Thema Datenschutz todernst. Wirklich!

Dann sind Sie ein Vorbild! Der mündige Bürger, der seine Rechte kennt und sie sich nicht für einen Rabattgutschein abkaufen lässt. Allerdings sind Sie in der Minderheit. Die meisten von uns fürchten zwar auch, dass unsere Wege durch das Web verfolgt, unsere Handlungen gespeichert und unsere Vorlieben analysiert werden. Aber nicht so sehr, dass wir deswegen Datenschutzerklärungen lesen oder gar ablehnen würden.

Und so interessiert es uns auch höchstens am Rande, dass die EU in diesem Jahr eine einheitliche Datenschutzvereinbarung erarbeiten will. Was soll dabei schon herauskommen? Diese Mühlen mahlen so langsam, dass die Realität das Regelwerk bei Inkrafttreten schon überholt haben dürfte. Zudem haben wir uns daran gewöhnt, unsere Bequemlichkeit einer intakten Privatsphäre vorzuziehen.

Sie, liebe Leserinnen und Leser aus den IT-Zentralen der Unternehmen, müssen sich wohl oder übel mit dem Datenschutz beschäftigen. Weil sich auch Ihr Business-Modell immer mehr in die digitalen Welten verlagert und Sie etwaigen Rechtsverstößen im eigenen Haus vorzubeugen haben.

Auch Google, Facebook und Co. nehmen das Thema todernst. Wirklich! Mit Sicherheit beschäftigen sie zahlreiche Juristen, die auch das strenge Bundesdatenschutzgesetz bis zum Äußersten ausreizen. Personen- und kontextbezogene Informationen in vielfacher Verknüpfung – das ist doch der heilige Gral, den die Werbewirtschaft erobern möchte. Wie lange werden die Tempelritter in der EU ihn wohl verteidigen können?

Karin Quack
Redakteurin CW

Edeka hat einen neuen IT-Vorstand

Michael Wulst übernimmt von Reinhard Schütte.

Bis dato war Michael Wulst einer von drei Geschäftsführern der IT-Tochter Lunar; nun übernahm der 61-jährige das IT-Ressort im Vorstand des Handelskonzerns Edeka. Sein Vorgänger Reinhard Schütte hat das Unternehmen verlassen.

Wie die COMPUTERWOCHE-Schwester „CIO“ aus Presseberichten folgert, war Schüttes Verhältnis zur Unternehmensspitze zuletzt gestört. Seine Verdienste sind eng mit dem Projekt „Lunar“ verknüpft. Dabei handelt es sich um die Einführung einer einheitlichen IT- und Prozesslandschaft auf SAP-Basis.

Jetzt der Einzelhandel

Das Fünfjahresprojekt fand Ende 2012 seinen Abschluss und kostete rund 350 Millionen Euro. Betrieben wird die neue Umgebung von der 500-köpfigen IT-Tochter.

Mit Wulsts Ernennung zum IT-Vorstand unterstreiche Edeka die strategische Bedeutung von Lunar, sagt Vorstandssprecher Markus Mosa. Nun soll der Schütte-Nachfolger die weitere Implementierung von Lunar auf der Einzelhandelsebene vorantreiben. Der genossenschaftlich geprägte Edeka-Verbund umfasst 4500 selbständige Kaufleute und sieben regionale Großhandelsbetriebe. *(qua)*