Daten in der Cloud – aber sicher!

Datenschutz und Datensicherheit mit Dirk-Michael Mülot

Die rasanten technologischen Entwicklungen erfordern heute mehr denn je ebenso schnelle Entscheidungen von den Unternehmern. Ein Fehltritt oder insbesondere auch passives Verhalten können ein erfolgreiches Unternehmen genau so schnell in den Abgrund führen, weil die Konkurrenz intelligenter agiert hat. Die Datenschutzskandale der letzten Monate zeigen aber auch – es ist oft ein schmaler Grad zwischen effizienten Maßnahmen und der Verletzung deutscher Datenschutzbestimmungen.

Dirk-Michael Mülot – forSYSTEMS-Experte für Datenschutz – gibt Ihnen hier einige kurze Hinweise zum Thema Cloud-Computing. Bei diesem Thema sollten Sie aber immer unbedingt die Meinung eines Experten zu genau Ihrem Projekt einholen. Ist erstmal ein Datenleck da, ist der Schaden, insbesondere auch der Imageschaden, kaum wieder gutzumachen.

Dem Thema Cloud-Computing können sich Unternehmen, insbesondere Franchise-Unternehmen, wo eine hohe Vernetzung der Partner schon systembedingt angestrebt wird, heute kaum noch verschließen. Doch als eigenständige Unternehmen im Franchise-System lauern gerade hier juristische Fallstricke.

Insgesamt können wir in der forSYSTEMS solch komplexe Themen immer nur kurz anreißen, für Rückfragen wenden Sie sich bitte direkt an unsere Experten.

DATENSCHUTZ IN DER CLOUD

Keine Angst, **Cloud Computing** ist im Prinzip alter Wein in neuen Schläuchen. Denn mit Cloud Computing – oder verkürzt einfach nur „der Cloud" – wird allgemein die bedarfsgesteuerte Bereitstellung von Datenverarbeitungsressourcen jeglicher Art über das Inter- oder Intranet auf Basis einer nutzungsbezogenen Abrechnung bezeichnet. Und genau dies wird in der Wirtschaft schon seit vielen Jahren praktiziert. Grundsätzlich können drei technische Realisierungen von Cloud Computing anhand ihres Abstraktionsgrades unterschieden werden: **Infrastructure as a Service** (Iaas), **Platform as a Service** (PaaS) und **Software as a Service** (SaaS).

DATENSCHUTZRECHTLICHE PROBLEME

Als Geschäftsführer oder Vorstand haften Sie für unsichere Cloud-Anwendungen – z.B. im Rahmen des GmbH-Gesetzes (§§ 42, 43 GmbHG) oder auch des Strafrechts (hier gem. § 14 StGB). Grundsätzlich sollten Sie daher bei der Cloud-Sicherheit den Schwerpunkt auf Transparenz, Kontrolle und Automatisierung legen. Die Grundlage einer erfolgreichen und sicheren Cloud bildet die Umsetzung einer klar strukturierten Sicherheits-Roadmap mit dem richtigen Mix aus Funktionalitäten zum Schutz der grundlegenden Technologien und zur Einhaltung der gesetzlichen Vorgaben aus den diversen Rechtsbereichen.

BITTE VERMEIDEN – DATENSCHUTZFALLSTRICKE

Ein klassischer Fall, der direkt zur „Selbstanzeige gem. § 42 a BDSG" führen musste:

HILTON-MARKETINGTEAM VERSCHICKT MAILING AN OFFENEN VERTEILER

Laut „Projekt Datenschutz" (www.projekt-datenschutz.de) versendete das Marketingteam der Hotelkette Hilton ein Mailing mit einem offenen Verteiler an knapp 1.000 Teilnehmer eines Gewinnspiels, das sich auf den Hilton Honors Adventskalender bezog. Somit konnten alle Empfänger sehen, wer sich in dem Mailverteiler der Hotelkette für das Gewinnspiel befand.

Dirk-Michael Mülot | Freier Sachverständiger für Datenschutz und Datensicherheit
Kontakt *Telefon +49 (0)5248-8235430, Fax +49 (0)5248-8235431, E-Mail buero@muelot-graf.de*
Adresse *Stammsitz Büro Langenberg, Westfalenweg 2, 33449 Langenberg*
Website *www.muelot-graf.de*

Insbesondere ist beim Cloud-Betrieb darauf zu achten, dass folgende Fragen vor der Inbetriebnahme klar und eindeutig beantwortet werden können:

- Muss ich mit dem Cloud-Betreiber (Auftragnehmer) einen Vertrag zur Auftragsdatenverarbeitung gem. § 11 BDSG abschließen?
- Hier gilt es zu beachten, dass auch eine Konzernschwester oder ein Franchisenehmer ggf. eine juristisch eigenständige „verantwortliche Stelle“ (i.S.d. § 3 (7)BDSG) ist.
- Habe ich diesbezüglich bereits meinen betrieblichen Datenschutzbeauftragten in Kenntnis gesetzt?
- Hat der betriebliche Datenschutzbeauftragte eine Vorabkontrolle gem. § 11 (2) BDSG durchgeführt und die Ergebnisse sauber dokumentiert?
- Ist der Beschlagnahmeschutz beachtet worden (§ 97 StPO)?
- Wo liegen meine Daten und Systeme physikalisch? Innerhalb Deutschlands, innerhalb der EU oder in einem Drittstaat? Dann müssen ggf. spezielle Regelungen beachtet werden.
- Habe ich die speziellen Anforderungen des Datenschutzgesetzes (hier besonders § 9 BDSG zzgl. Anlage Nr.1) zu den technisch-organisatorischen Maßnahmen berücksichtigt?

Nicht zuletzt sollte aber auch die Frage erörtert werden, ob und inwieweit das Unternehmen von einem einzelnen externen Anbieter „abhängig“ wird.

Im Hinblick auf den Datenschutz sollten folgende Mindestanforderungen beachtet werden:

- Verwalten Sie Identitäten und Benutzerzugriff
  - Schützen Sie den Benutzerzugriff auf Cloud-Assets. Richten Sie ein System zur Verwaltung der Identitäten von Benutzern und des Zugriffs auf Ressourcen ein.
- Scannen Sie das Netz und schützen Sie dieses vor Bedrohungen
  - Sichern Sie die IT-Infrastruktur ohne Beeinträchtigung der Systemleistung.
  - Schützen Sie Server, Endpunkte und Netzwerke gegen Bedrohungen.
- Überwachen und überprüfen Sie Anwendungen und Daten
  - Stellen Sie sichere mobile Anwendungen und Webanwendungen bereit und überwachen Sie den Datenzugriff in Echtzeit.
  - Implementieren Sie die Echtzeitüberwachung von Daten sowie die proaktive Bewertung von Anwendungen.
- Sicherheitsdatenbeschaffung innerhalb der Cloud
  - Implementieren Sie lückenlose Sicherheit in Ihrer Cloud. Richten Sie eine Plattform mit Echtzeit-Korrelation und -Erkennung für die gesamte Cloud ein.

DATENSCHUTZ-GLOSSAR

In dieser Ausgabe passend zu unserem Datenschutzfallstrick:

§ 42A INFORMATIONSPFLICHT BEI UNRECHTMÄSSIGER KENNTNISERLANGUNG VON DATEN

Stellt eine nicht öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3Absatz9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
4. personenbezogene Daten zur Bank- und Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen.

Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme.

Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.