

Mobiler Datenschutz

Anforderungen an Datenschutz und IT-Sicherheit im Mobile Web

Jan Schneider, Rechtsanwalt und Fachanwalt für Informationstechnologierecht

Business-Anwendungen für Smartphones und andere mobile Endgeräte erobern die Geschäftswelt. Insbesondere für Cloud-basierte Dienste sehen Experten auch im Bereich „Mobility“ einen immensen Wachstumsmarkt. Doch der Einsatz mobiler Technologien in Unternehmen und Behörden unterliegt erhöhten Anforderungen an Datenschutz, IT-Sicherheit und Rechtskonformität.

Der Einsatz mobiler Systeme und Infrastrukturen kommt in einigen Bereichen der Geschäftswelt einer Revolution nahe: Die Intranets der Unternehmen sind für die Mitarbeiter jederzeit mobil erreichbar. Über das mobile Customer Relationship Management hat auch der im Außendienst tätige Vertrieb jederzeit Zugriff auf die für seine Arbeit wichtigen Kundendaten und Informationen, und zwar in der jeweils aktuell auf den unternehmenseigenen Servern gespeicherten Form. Auswärts akquirierte Aufträge können direkt im mobilen Endgerät erfasst und vom Kunden bei entsprechender Hardware sogar mittels digitaler Unterschrift rechtswirksam erteilt werden. Vor Ort beim Endkunden tätige Projektmitarbeiter können Zeit- und Leistungserfassungen sowie andere Informationen jederzeit, gegebenenfalls sogar in Echtzeit an ihr Unternehmen übermitteln, zum Beispiel die abrechnungsrelevante Erfassung von Telefonaten. Mittels mobiler Lösungen im Bereich der Ortung, Navigation und des Flottenmanagements weiß das Unternehmen schließlich jederzeit, wo sich seine Fahrzeuge befinden und kann über elektronische Fahrtenbücher und Lösungen zur Tourenpla-

nung und -verfolgung erhebliche Einsparungen realisieren.

All diesen Lösungen gemeinsam ist der Umstand, dass – auch sensible – Daten und Informationen außerhalb der unternehmensinternen Server auf mobiler Hardware gespeichert und verarbeitet sowie zwischen Servern und Endgeräten übertragen werden.

Risiko Datenschutz

Häufig sind auf geschäftlich eingesetzten mobilen Endgeräten auch vertrauliche Informationen gespeichert - einschließlich personenbezogener Daten, also solcher Angaben, mittels derer eine natürliche Person bestimmbar ist. Zum Beispiel der Name einer Person, deren Alter, Beruf, Post- oder E-Mail-Anschrift. Der Umgang mit personenbezogenen Daten unterliegt den strengen Anforderungen des Bundesdatenschutzgesetzes bzw. der für öffentliche Stellen geltenden Landesdatenschutzgesetze. Hiernach dürfen personenbezogene Daten grundsätzlich nur dann gespeichert, verarbeitet und an Dritte übertragen werden, wenn eine ausdrückliche gesetzliche Ermächtigungsnorm vorliegt oder - für die Praxis kaum

relevant – die Betroffenen in die betreffende Handlung, wie in die Datenübermittlung, ausdrücklich eingewilligt haben

Soweit das Unternehmen nach den gesetzlichen Vorgaben zur Speicherung der betreffenden personenbezogenen Daten berechtigt ist, dürfen die Daten grundsätzlich auch auf den mobilen Endgeräten der Mitarbeiter abgelegt werden. Immer mehr Softwarelösungen für mobile Endgeräte („Apps“), mobile Dienste und zunehmend auch ganze Betriebssysteme sind allerdings darauf angelegt, dass der Nutzer des Endgerätes seine Daten nicht mehr vollständig dort oder auf dem Server seines Unternehmens speichert, sondern bei einem Dritten wie einem Diensteanbieter oder dem Hersteller des Betriebssystems.

Die Daten liegen dann, dem aktuellen Technologietrend entsprechend, meist in der „Cloud“ und damit auf Servern, deren Ort in aller Regel gar nicht bekannt ist. Eine Übertragung personenbezogener Daten in das außereuropäische Ausland – wo die Server der Cloud-Provider häufig stehen – ist aber häufig unzulässig; eine Datenübertragung innerhalb Europas ist regelmäßig nur unter den strengen



Jan Schneider, Fachanwalt für IT-Recht und Partner des Düsseldorfer Büros der Sozietät SKW Schwarz Rechtsanwälte, beschäftigt sich seit über 10 Jahren mit rechtlichen Fragestellungen der Informationstechnologie.

Anforderungen einer sogenannten Auftragsdatenverarbeitung (§ 11 BDSG) erlaubt. Werden diese Anforderungen nicht erfüllt, was derzeit für viele Cloud-basierte mobile Anwendungen gilt, ist die Datenübertragung rechtswidrig. Das Gleiche gilt gegebenenfalls, wenn die betreffenden personenbezogenen Daten gesetzlichen Einschränkungen unterliegen, was zum Beispiel für Gesundheits- oder Steuerdaten der Fall ist.

Übrigens unterliegt auch der Datentransfer zwischen Konzernunternehmen den vorstehend umrissenen gesetzlichen Anforderungen. Eine mobile Lösung, mittels der die Mitarbeiter auf den Server eines anderen Konzernunternehmens zugreifen, muss daher in aller Regel ebenfalls den gesetzlichen Anforderungen an eine Auftragsdatenverarbeitung genügen, andernfalls wird die Nutzung dieser Lösung gege-

benenfalls wiederum rechtswidrig sein.

Persönliche Haftung droht!

Die Konsequenzen einer rechtswidrigen Datenübertragung an und von mobilen Endgeräten trägt nach Maßgabe der gesetzlichen Regelungen zunächst das Unternehmen, dessen Mitarbeiter die mobile Lösung einsetzen. Je nach konkretem Fall ist darüber hinaus eine persönliche Haftung der Geschäftsleitung oder der IT-Verantwortlichen gegenüber dem Unternehmen denkbar. Denn die Verantwortung für einen rechtskonformen Umgang mit Datenschutz und IT-Sicherheit liegt in aller Regel bei der Unternehmensleitung oder auch, je nach arbeitsvertraglich gestaltetem Verantwortungsbereich, bei den mit der Unternehmens-IT befassten Angestellten.

Die Erarbeitung, Durchsetzung und Aufrechterhaltung konkreter Maßnahmen zum Datenschutz und zur IT-Sicherheit im Bereich „Mobility“ – hierzu später mehr – ist damit mindestens Sache der IT-Verantwortlichen, in aller Regel sogar „Chefsache“.

Auch für den Bereich der IT-Sicherheit bringt der Einsatz mobiler Systeme und Infrastrukturen erhöhte Anforderungen. So sind mangelhaft geschützte Endgeräte immer häufiger Einfallstore für Viren, Würmer und andere Schadprogramme. Derartige „Malware“ greift oftmals nicht nur das Endgerät an, sondern auch die dahinterliegenden Netzwerkstrukturen des Unternehmens. Auf diese Weise werden unternehmensinterne Daten und Informationen gefährdet und können im schlimmsten Fall von einem Dritten abgegriffen, verändert oder vernichtet werden. Ein ähnliches Risiko birgt die Nutzung drahtloser Übertragungstechnologien wie beispielsweise Bluetooth oder WLAN.

Risiko IT-Sicherheit

Das aus mangelhafter IT-Sicherheit oder unzureichendem IT-Risikomanagement resultierende Haftungsrisiko für das Unternehmen und ggf. für dessen Geschäftsleitung bzw. IT-Verantwortliche bedingt für den Einsatz mobiler Technologien im Unternehmen zwingend eine Erweiterung der unternehmensinternen IT-Sicherheitsstrategie. Die mobilen Infrastrukturen sollten unbedingt als Bestandteil der unternehmensinternen IT verstanden und in diese eingegliedert werden.

Unter dieser Prämisse muss zunächst sichergestellt werden, dass Dritte keinen unbefugten Zugriff auf die auf den Endgeräten abgelegten Daten nehmen können. Des Weiteren gilt es, die Sicherheit der Datenübertragung und natürlich die Sicherheit der stationären IT-Systeme zu gewährleisten. In Ergänzung der „üblichen“ Schutzmaßnahmen wie Firewalls und Virens Scanner, die freilich auch die mobilen Endgeräte erfassen müssen, ermöglicht ein – unverzichtbares – zentrales Gerätemanagement („Mobile Device Management“) die zentrale und kontrollierte Installation der jeweils aktuellsten Schutzsoftware auf allen Endgeräten des Unternehmens.

Gleichzeitig erfordert die Nutzung der mobilen Technologien eine erhöhte Sensibilität der Nutzer hinsichtlich Datenschutz und IT-Sicherheit. Denn der beste technische Schutz lässt sich leicht unterwandern, wenn Nutzer unbewusst ihren Teil dazu beitragen. Beispielsweise indem sie die Bluetooth-Funktion durchgängig aktiviert lassen, herstellereitig vorgegebene Passwörter nicht ändern oder gar auf einen wirksamen Passwortschutz ihrer Endgeräte ganz verzichten. Das kann im Falle eines Diebstahls oder Verlustes des Gerätes fatale Konsequenzen haben kann.

Häufig wissen die Mitarbeiter des Unternehmens auch gar nicht, wel-

che Daten sie auf ihren mobilen Geräten oder in der Cloud überhaupt speichern dürfen, und welche Daten unbedingt allein auf den unternehmenseigenen Servern vorgehalten und lediglich kurzzeitig zur Anzeige auf dem Endgerät zwischengespeichert werden sollten. Die aktuellen Möglichkeiten wirksamer Datenverschlüsselung sind oftmals nicht bekannt oder werden schlicht nicht genutzt. Auch fehlt es häufig an einer ausreichenden Datensicherungsstrategie. Lösungen zur Fernlöschung von Daten nach Verlust des Endgerätes werden oftmals nicht eingesetzt, obwohl hierdurch das Risiko des Datendiebstahls für das Unternehmen erheblich verringert werden kann.

Schulungen der Mitarbeiter und die Gestaltung verbindlicher Unternehmensrichtlinien für den Bereich „Mobility“, die derartige Themen umfassend und unter Berücksichti-

gung des jeweils aktuellen Standes der Technik abbilden, leisten mithin einen wertvollen Beitrag zur IT-Sicherheit.

Rechtliche Risiken begrenzen!

Derartige Schulungen und Richtlinien sollten idealerweise auch den erlaubten Einsatzbereich der beruflich benutzten Endgeräte eng begrenzen und die Mitarbeiter hinsichtlich der Risiken anderweitiger Nutzungen sensibilisieren. Moderne Smartphones etc. erlauben mit ihrer stetig zunehmenden Funktions- und Einsatzvielfalt zum Beispiel den Erwerb von Produkten über „Mobile Commerce“, den Download von Apps und Inhalten über diverse Online-Quellen, die Nutzung von Instant-Messengern und Chat-Clients sowie die Teilnahme an Online-Communities.

Rechtliche Risiken solcher Nutzungen sind beispielsweise das nicht autorisierte und damit gegebenenfalls rechtswidrige Abrufen oder Verbreiten fremder Inhalte wie Songs, Videodateien oder gar Pornografie, die Installation von Software aus unsicherer Quelle, die – gegebenenfalls strafbare – Verletzung von Persönlichkeitsrechten oder die leichtfertige Offenlegung privater oder unternehmenseigener Informationen innerhalb von Businessportalen oder Social Communities.

Derartige Nutzungsmöglichkeiten von mobilen Endgeräten, so verlockend sie auch sein mögen, bergen erhebliches Risikopotential und haben auf beruflich genutzten Endgeräten in aller Regel nichts zu suchen. Einmal mehr ist es Sache des Unternehmens, für eine verantwortungsbewusste Nutzung der unternehmenseigenen mobilen Technologien Sorge zu tragen. ■

Neu erschienen: Die kompletten Ergebnisse jetzt bestellen



IT-Grundschutz



Bundesamt
für Sicherheit in der
Informationstechnik



research
an der Universität
Regensburg GmbH

Studie IT-Sicherheitsstandards und IT-Compliance:

Ergebnisse jetzt verfügbar

294 Anwender aus der Praxis bewerten den Stellenwert der IT-Sicherheit als sehr hoch. Jedoch gaben 18 % der IT-Sicherheit lediglich eine mittlere und 7 % sogar eine niedrige bis sehr niedrige Priorität. Nur ca 5 % der Teilnehmer haben einen Zertifizierungsprozess abgeschlossen.

Die kompletten Ergebnisse jetzt bestellen:

80 Seiten, A4 gebunden, zahlreiche Grafiken und Tabellen,
295,00 € zzgl. Versandkosten

www.grundschutz.info/studie oder per Telefon: +49 6725 9304-0

Die Umfrage entstand in Zusammenarbeit der Zeitschrift „Informationsdienst IT-Grundschutz“ mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und ibi research.

Vorstellung der Studienergebnisse 2010



Gratisabruf Video-Slideflow:
www.grundschutz.info/webcast