Roland Steidle; Ulrich Pordesch *

Wider das anarchistische IT-Outsourcing! Webdienste und Informationssicherheit

- Ein Beitrag zu Dropbox & Co. im Unternehmen -

Webdienste wie Dropbox, Doodle, YouSendIt, Facebook oder Twitter, umgangssprachlich auch Web 2.0-Dienste oder Cloud-Dienste genannt, werden auch für betriebliche Zwecke durch Mitarbeiter eines Unternehmens eingesetzt. Die IT-Abteilungen der jeweiligen Unternehmen werden jedoch nur selten über die Nutzung und die verwendeten Endgeräte informiert, geschweige denn können sie Anbieter und Nutzung steuern oder unter dem Blickwinkel des Sicherheitsmanagements überwachen. Aus ihrer Sicht stellt sich diese Form der mitarbeiterinitiierten Auslagerung als anarchistisches Outsourcing bzw. als Teil einer unerwünschten „Schatten-IT" dar, vorbei an allen betrieblichen Einheiten wie der IT-Administration, dem Einkauf oder auch dem Betriebs- und Personalrat. Häufig bleibt ein Ohnmachtsgefühl, wenn betriebliche Infrastruktur und Aufgaben durch Mitarbeiter auf Webdienste ganz oder teilweise verlagert werden.

Der folgende Beitrag untersucht die Risiken einer solch unkontrollierten Nutzung bezüglich der Informationssicherheit und der Erfüllung rechtlicher Anforderungen und zeigt Wege auf, die Risiken durch bestimmte Maßnahmen zu mindern.

Daneben enthält der Beitrag Ausführungen zum Aufbau eigener Alternativdienste, zu einem möglichen Prüfungsprozess und stellt zudem einen exemplarischen Quickcheck zur Verfügung, mit dem wichtige Punkte bei der Prüfung eines Webdienstes abgefragt werden können.

Der Beitrag ist im Rahmen von Untersuchungen und Vorträgen für die Fraunhofer-Gesellschaft e.V. und ihre IT-Sicherheitsbeauftragten entstanden. Einige Ausführungen des Beitrags gelten daher in besonderer Weise für Unternehmen, die in einem wissenschaftlichen Umfeld tätig sind, grundsätzlich aber auch allgemein für alle Unternehmen. Die Autoren arbeiten weiter in diesem Themenfeld und freuen sich deshalb über Anregungen zum Beitrag.

Dr. Roland Steidle: steidle@mainfort.eu
Dr. Ulrich Pordesch: ulrich.pordesch@zv.fraunhofer.de

* Dr. Roland Steidle ist Fachanwalt für Informationstechnologierecht in Frankfurt am Main. Dr. Ulrich Pordesch ist IT-Sicherheitskoordinator der Fraunhofer Gesellschaft e.V.

Inhaltsverzeichnis

Zusammenfassung

Über das World Wide Web werden immer mehr anwendungsorientierte Dienste angeboten, mit denen Nutzer Daten verarbeiten und Nachrichten austauschen können. Dabei werden Daten außerhalb der betrieblichen IT-Infrastruktur beim Diensteanbieter oder in einer Cloud aufbewahrt und verarbeitet.

Es gibt eine zunehmende Vielzahl von Diensten, die sich hinsichtlich der hauptsächlich erbrachten Funktionalität klassifizieren lassen, beispielsweise in Online-Speicher, Terminfindungsdienste, Literatur- und Referenzdienste oder Social Network Dienste. In vielen Unternehmen sind unter anderem Doodle und Dropbox bei Mitarbeitern sehr gefragt.

Vorteile der Webdienstenutzung bestehen im einfachen Zugang zu neuen, innovativen Angeboten und Funktionen, die firmenintern nicht oder nur verzögert bereitgestellt werden, sowie in der Möglichkeit, die Dienste oft kostenfrei nutzen zu können. Andererseits bestehen auch **Risiken** für die Informationssicherheit und die Erfüllung diesbezüglicher Rechtsvorschriften:

- *Unzulässige Nutzung*: Die Verarbeitung von Daten durch Dritte kann gegen Vorgaben in Kooperationsvereinbarungen oder Zuwendungsbestimmungen verstoßen, z.B. gegen NDAs, Vorgaben zum Leistungsort oder das Verbot von Subunternehmern. Verstöße können Vertragsstrafen auslösen. Die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage kann Bußgelder nach sich ziehen. Hohe Strafen haben Verstöße gegen den amtlichen Geheimschutz oder Exportkontrollvorschriften zu Folge.
- *Verlust von Know-How:* Forschungsergebnisse, Geschäftsgeheimnisse oder vertrauliche Vertragsbeziehungen bilden das Know-How vieler Unternehmen. Durch Weitergabe oder versehentliches Publizieren kann Know-How verloren gehen.
- *Verlust von Rechten*: Durch das unreflektierte Einverständnis in problematische Nutzungsbedingungen (AGB) können verschiedene Rechte verloren gehen. Bspw. können einem Webdienst Nutzungsrechte an Inhalten eingeräumt oder Gewährleistungs- und Schadensersatzrechte ausgeschlossen werden.
- *Datenmissbrauch*: Der Diensteanbieter oder der Betreiber können Kundendaten missbrauchen. Sie können die Daten bspw. an Dritte verkaufen. Unter Umständen erzwingen auch Sicherheitsbehörden des Landes, in dem Anbieter bzw. Betreiber ihren Sitz haben, diese dazu, Daten herauszugeben. Die Daten könnten dann bspw. zur Wirtschaftsspionage missbraucht werden.
- *Unerwünschte Datenverwendung:* Neben illegalen Missbrauchsszenarien sind auch legale aber unerwünschte Datenverwendungen möglich, bspw. wenn Gerichte im Ausland Zugriffe gestatten, die ein Nutzer nach deutschem Recht nicht erwartet.
- *Unsichere Dienstgestaltung*: Webdienste sind meistens nicht auf Sicherheit und betriebliche Erfordernisse designt und daher anfällig gegenüber Hackerangriffen von außen oder Missbrauch durch andere Nutzer. Auch so können Daten in falsche Hände gelangen.
- *Gefährdung der IT-Infrastruktur:* Die eigene IT kann gefährdet werden, wenn zur bequemen Nutzung der Dienste Browsersicherheitseinstellungen reduziert, unsichere Plug-Ins installiert oder Firewalls getunnelt werden.
- *Benutzungsfehler:* Daten oder Know-How können unkontrolliert abfließen, wenn Nutzer die teils sehr mächtigen Funktionen nicht richtig verstehen und einsetzen. So können z.B. interne Kontaktdaten versehentlich weitergegeben oder veröffentlicht werden.
- *Mangelnde Verfügbarkeit:* Je mehr Daten extern vorgehalten werden, um so größer wird das Risiko mangelnder Verfügbarkeit. Dies kann bspw. zum Problem werden, wenn ein Dienst zur Datenarchivierung insolvent wird und lokal keine Datenkopien existieren.
- *Datenleichen und -zombies:* Vergessene Benutzerkonten, auf denen Firmendaten dauerhaft lagern oder noch Kommunikation stattfindet, können ein Eigenleben entwickeln.

- *Probleme der Rechtsdurchsetzung:* Rechte, bspw. Schadensersatzansprüche bei Missbrauch, sind nicht durchsetzbar, wenn Anbieter oder Betreiber ihren Sitz im Ausland haben.

Um den Risiken zu begegnen, müssen IT-Management, IT-Sicherheitsbeauftragte, aber auch Projektverantwortliche und Nutzer angemessene **Maßnahmen** ergreifen:

- *Prüfung der Zulässigkeit und Einwilligung*: Vor Nutzung eines Webdienstes müssen bestehende Verträge mit Kunden geprüft werden, ob der Einsatz zulässig ist. In Zweifelsfällen sind immer die Zustimmung der beteiligten Firmen und eine Datenschutz-Einwilligung der betroffenen Mitarbeiter einzuholen.
- *Abschätzung des Schadenspotentials:* Vor der Nutzung sollten mögliche Schäden abgeschätzt werden, v.a. bei wenig bekannten Diensten und bzgl. eines möglichen Datenmissbrauchs.
- *Prüfung des Diensteanbieters und -betreibers*: Anbieterseriosität, Standort (möglichst in der EU) und Sicherheitsprobleme sollten durch Internetrecherchen geprüft werden. AGB und Datenschutzhinweise sind immer auf Auffälligkeiten zu prüfen.
- *Prüfung von Alternativen*: Es ist zu prüfen, ob es eigene Diensteangebote oder solche von Kooperationspartnern gibt, mit denen sich die gewünschte Funktionalität erreichen lässt. Diensteangebote sind vergleichend zu bewerten.
- *Verbot und Unterbindung der Nutzung*: Dienste, die ein hohes Schadensrisiko haben, zu denen es Alternativen gibt oder deren Nutzung nicht durch bspw. einen Auftraggeber verlangt wird, sollten nicht genutzt und ggf. verboten werden. Verbote können auch technisch, z.B. mit Webfiltern oder Next Generation Firewalls, durchgesetzt werden. Möglich ist auch eine Nutzung unter einschränkenden Bedingungen.
- *Eigene Sicherheitsmaßnahmen, v.a. Verschlüsselung:* Es sollte versucht werden, durch eine echte Ende-zu-Ende-Verschlüsselung von Daten, die Verwendung von Pseudonymen, lokale Datensicherungen und andere Maßnahmen Schadensrisiken auszuschließen.
- *Vertragsabschluss*: Werden personenbezogene Daten zur hilfsweisen und automatisierten Verarbeitung ohne vorherige (schlüssige) Einwilligung Betroffener an den Dienst gesendet, ist ein schriftlicher Auftragsvertrag mit dem Anbieter abzuschließen. Ebenso, falls besonders sensible Daten von einem Dienstleister verarbeitet werden, um eine Anbietersteuerung/Kontrolle zu ermöglichen. Ebenso, falls ein Angebot entgeltlich erbracht wird.
- *Awareness:* Mitarbeiter sollten durch gezielte Aktionen sensibilisiert und geschult werden.
- *Eigene Angebote:* Für wichtige und vielfach genutzte Webdienste, die Firmendaten verarbeiten, sollten entsprechende eigene Angebote bereitgestellt werden bzw. erhalten bleiben.

Bei eigenen Dienste-Angeboten, welche in größeren Unternehmen sinnvoll sein können, ist insbesondere zu beachten:

- Die Angebote sollten bei öffentlich geförderten Unternehmen nur von Mitarbeitern und Kooperationspartnern genutzt werden können. In diesen Fällen dürfen Angebote nicht in Konkurrenz gegenüber Diensten der freien Wirtschaft stehen.
- Im Übrigen sollte eine Risikobegrenzung durch eine beschränkte Nutzerzahl erreicht werden.
- Die Schadenspotentiale und daraus resultierende Sicherheits-Anforderungen sind dienstspezifisch zu bewerten.
- Es sind Sicherheitsprüfungen und -konzepte festzulegen.
- Es sind sichere Programmierstandards vorzugeben.
- Daten sollten verschlüsselt gespeichert werden. Auch der Login und die Datenübertragung sollten verschlüsselt erfolgen. Wenn möglich sollte eine Ende-zu-Ende Verschlüsselung für Nutzer angeboten werden, ggf. über ohnehin vorhandene Mitarbeiterzertifikate.
- Der Betrieb sollte auf eigenen bzw. selbst kontrollierten Servern erfolgen.
- Impressum, Datenschutzhinweise und Nutzungsbedingungen sind festzulegen.
- Gegenüber Externen sind Gewährleistung und Haftung auszuschließen. Externe sind auf die Einhaltung der übrigen Regelungen für die eigene IT-Infrastruktur zu verpflichten.
- Mitbestimmungs- und Informationsrechte des Betriebs-/Personalrats sind zu beachten.

1 Einleitung

1.1 Webdienste

Als „Webdienste" werden im Folgenden Dienste verstanden, die über das World Wide Web angeboten werden und mit denen Internet-Nutzer über den Webbrowser Anwendungen nutzen und dabei Daten verarbeiten und Kommunikationsverbindungen herstellen können.

Webdiensten ist gemein, dass die Daten außerhalb der Unternehmens-IT-Infrastruktur gespeichert und verarbeitet werden, in einem Rechenzentrum des Diensteanbieters, eines vom Diensteanbieter unabhängigen Betreibers oder in auf der Welt verteilten Cloud-Rechenzentren.

Im Unterschied zum klassischen Application Service Providing (ASP) sind Webdienste häufig kostenlos bzw. werbefinanziert, auf Endnutzer statt Unternehmen ausgelegt, multimedial, weisen Schnittstellen zu anderen Webdiensten auf und bieten dem Nutzer Funktionen, ohne dass er sich selbst um die Erstellung/Beschaffung geeigneter Software und deren Betrieb in einem Rechenzentrum kümmern muss.

Diese von Mitarbeitern und Projekten meist in eigener Regie ohne Beteiligung der lokalen IT ausgewählten und genutzten Webdienste stehen im Fokus der folgenden Betrachtung.

Neben dem Zugang über den Webbrowser wird der Zugang zum Dienst und seinen Funktionen häufig auch über Plug-Ins in Anwendungsprogrammen angeboten. Teilweise werden die Dienste auch zum integralen Bestandteil von Anwendungsprogrammen. So wird beim E-Mail-Client Thunderbird standardmäßig eine Funktion angeboten, die zum Versenden von großen Dateien Dropbox nutzt.

1.2 Diensteklassen

Webdienste bieten ihren Nutzern bestimmte Datenverarbeitungs- oder Kommunikationsfunktionen. Die Dienste sind meist auf bestimmte Funktionen fokussiert bzw. auf diese beschränkt, so dass anhand der Funktionen auch Diensteklassen gebildet werden können, um Risiken und Maßnahmen speziell zu betrachten:

- *Publikations-Dienste* wie etwa Science Blogs, YouTube, Picasa
- *Soziale Netzwerke* wie etwa Facebook, Google+, Xing
- *Kollaborations-Dienste* wie etwa Microsoft 365 oder EMDesk
- *Dokumentenerstellungs-Dienste* wie etwa Google Docs oder Mind Manager
- *E-Mail-Dienste* wie etwa Google gmail oder gmx.de
- *Webkonferenz-Dienste* wie etwa WebEx (Cisco) oder Skype (MS)
- *Datensynchronisierungs-Dienste* wie Dropbox oder Wunderlist
- *Speicher-, Archivierungs- und Backup-Dienste* wie Crypto Heaven oder Mozy
- *Terminfindungs-Dienste* wie etwa der DFN-Terminplaner oder Doodle
- *Dateiübertragungs-Dienste* wie Gigamove oder Yousendit
- *Dienste zur Literaturverwaltung* wie etwa RefWorks oder Mendeley
- *URL Shortener* wie etwa Is.gd oder mcaf.ee
- *Social Bookmarking-Dienste* wie etwa Mister Wong oder Delicious
- *Dienste für Online Umfragen* wie etwa Easy-Feedback oder EFS-Survey
- *Such- und Recherche-Dienste* wie etwa Google Alerts
- *Webtracking-Dienste* wie Etracker oder Google Analytics

1.3 Einsatz im Unternehmen

Auch in Unternehmen werden immer häufiger Webdienste verwendet. Dies ist den IT-Administratoren und den IT-Sicherheitsbeauftragten aus ihrer täglichen Erfahrung bekannt:

- Die **Verwaltung** nutzt bspw. für PR und Öffentlichkeitsarbeit Soziale Netzwerke und unterhält eigene Facebook- und Twitter-Seiten, über die sie Neuigkeiten kommuniziert, in Kontakt zu anderen Nutzern tritt und Stellenanzeigen publiziert. Grund für die Nutzung ist vor allem, dass bestimmte Zielgruppen über Soziale Netzwerke leichter erreicht werden können.
- In **Projekten mit mehreren Beteiligten** (z.B. Auftraggeber, Kooperationspartner) kommen Dienste zum Einsatz, die die Zusammenarbeit erleichtern sollen. So werden Kollaborationsplattformen, Webkonferenz-Dienste und Terminfindungs-Dienste eingesetzt. Besonders wichtig sind auch Dateiübertragungs-Dienste, welche die (Zwischen)Speicherung und den Austausch sehr großer Datenmengen erlauben. Gerade bei der Zusammenarbeit wird die Nutzung solcher Dienste von Externen häufig gewünscht.
- **Mitarbeiter** nutzen für ihre Arbeit u.a. Dienste zur Literatur- und Referenzverwaltung, Publikations-Dienste wie Weblogs und Suchmaschinen zur Recherche. Breit genutzt werden Google und seine Dienste sowie Dienste zur Referenzverwaltung wie Mendeley.
- Um Daten zwischen verschiedenen **Geräten** verfügbar zu haben und zu synchronisieren, werden Online-/Cloud-Speicher, Archivierungs-Dienste und Synchronisations-Dienste eingesetzt. Beispiele sind ICloud von Apple als in IPhone und IPad integriertem Angebot sowie der Webdienst Dropbox.

2 Risiken

Im Folgenden werden Risiken für die Informationssicherheit und für die Erfüllung in diesem Zusammenhang relevanter rechtlicher Anforderungen dargestellt. Risiken sind sehr vielfältig und hinsichtlich vieler Dimensionen, wie Komponenten, Ursachen, Schäden, Folgen darstellbar. Nachfolgend werden, wie im BSI-Grundschutz ohne Anspruch auf Überschneidungsfreiheit, wichtige Risiken dargestellt. Alle Risiken werden jeweils kurz in einem Kästchen zusammengefasst und danach ausführlich dargestellt. Die Risiken sind je nach Diensteklasse oder Dienst unterschiedlich relevant und ausgeprägt. Eine Spezifizierung wird in weiteren Bewertungspapieren zu konkreten Klassen oder Diensten vorgenommen.

2.1 Unzulässige Nutzung: Gesetzes- und Vertragsverstöße

Die Nutzung eines Webdienstes kann aus folgenden Gründen unzulässig sein:

- Unmittelbares Verbot in einem Vertrag („Webdienste dürfen nicht eingesetzt werden“)
- Mittelbares Verbot in Vertrag (NDA, Ort der Leistung, Subunternehmer, Nutzungsrechte)
- Verstoß gegen AGB des Dienstes (z.B. nur Privatlizenz kostenlos)
- Fehlen einer Datenschutz-Grundlage bei Übermittlung personenbezogener Daten
- Verstoß gegen gewerbliche Schutzrechte, Urheberrechte, Namensrechte
- Verstoß gegen Vorschriften zur Exportkontrolle
- Verstoß gegen interne Regelungen des Unternehmens (z.B. Betriebsvereinbarung)
- Verstoß gegen Mitbestimmungsrechte der Personalvertretung

2.1.1 Verstoß gegen Verträge mit Projektpartnern und Auftraggebern

Die Einschaltung eines Webdienstes durch ein Unternehmen kann, unabhängig von der Art der an den Webdienst übermittelten Daten und Informationen, gegen vertragliche Vereinbarungen mit Projektpartnern oder Auftraggebern verstoßen. Ist der Auftraggeber die öffentliche Hand, ist auch ein Verstoß gegen Nebenbestimmungen zu einem Zuwendungsbescheid möglich.

Hintergrund solcher Verbote ist, dass ein Projektpartner oder Auftraggeber eigenen Rechtspflichten unterliegen oder eigene berechtigte Interessen haben kann, zu kontrollieren, wer in die gemeinsame Zusammenarbeit eingebunden ist. Häufig werden Verstöße gegen vertragliche Regelungen mit Vertragsstrafen sanktioniert oder führen zu Kündigungsrechten.

Direkte Verbote, bspw. eine Regelung, nach der die Übermittlung von Daten an Webdienste explizit untersagt ist, sind sehr selten.

Häufiger sind **indirekte Verbote** bzgl. der Webdienstenutzung, die sich aus Bestimmungen zur konkreten Leistungserbringung durch die einzelnen Projektpartner ergeben. Entscheidend ist hierbei, wer konkret welche Leistung nach dem Vertrag schuldet, da sich vertragliche Pflichten immer nur auf die konkret geschuldete Leistung beziehen. Typische Vereinbarungen können dann Fragen des Leistungsorts, der Einschaltung von Subunternehmern, der Vertraulichkeit und der Zuordnung von Rechten an Projektergebnissen betreffen. Wenn sich beispielsweise ein Unternehmen zur Speicherung der Projektdaten oder zur Terminkoordination verpflichtet hat, etwa im Rahmen der Unterhaltung eines Projektbüros, so gelten für genau diese Leistungen die Regelungen des Vertrags. Ist weiterhin bspw. die Einschaltung von Subunternehmern von einer Zustimmung abhängig, dürfen geschuldete Leistungen nicht einfach mit Hilfe eines beauftragten Webdienstes erbracht werden.

Ist gar **nichts in einem Vertrag** zu Webdiensten oder zur Art und Weise der geschuldeten Leistungen geregelt, so ist die Einschaltung eines Webdienstes eine neue, nicht vertraglich vorgesehene Art der Zusammenarbeit. Auch in diesem Fall kann gegen vertragliche Regelungen verstoßen werden,

bspw. wenn ein Vertrag festlegt, dass die in ihm enthaltenen Regelungen die Zusammenarbeit abschließend regeln und Änderungen oder Ergänzungen einer bestimmten Form bedürfen, meist der Schriftform.

Typische Themenfelder für indirekte Verbote sind:

Leistungsort

Häufig enthalten Verträge Regelungen, die einen bestimmten Leistungsort vorschreiben. Ohne eine solche Regelung ist die Leistung nach dem Gesetz am Ort der Niederlassung des Schuldners zu erbringen, d.h. i.d.R. bei dem beauftragten Institut (s. § 269 BGB). Ohne Zustimmung des Projektpartners oder Auftraggebers kann dann nicht ohne weiteres ein Teil einer geschuldeten Leistung an einem anderen Ort erbracht werden, bspw. die Datenspeicherung bei einem Hosting-Provider.

In Verträgen mit IT-Bezug werden zur Absicherung häufig Regelungen getroffen, die eine Leistungserbringung auf dem Gebiet der Bundesrepublik Deutschland vorsehen oder weitergehend, dass IT-Infrastruktur wie Server zur Datenspeicherung an einem bestimmten Standort stehen müssen. Ohne Zustimmung der Projektpartner/ Auftraggeber dürfen Arbeitsinhalte dann nicht an einen Webdienst mit anderem Leistungsort übermittelt werden, auch nicht vorübergehend.

Subunternehmerregelungen

Ein Vertragspartner darf darüber hinaus nicht ohne Weiteres geschuldete Leistungen an Subunternehmer auslagern. Entscheidend ist, wer was konkret schuldet. Typischerweise sehen Projektverträge vor, dass entweder von vornherein für bestimmte Leistungsteile Subunternehmer eingesetzt werden dürfen, die dann meistens schon konkret benannt sind, oder dass der Einsatz jeglicher Subunternehmer einer vorherigen ausdrücklichen Zustimmung bedarf. Andernfalls wäre es für einen Projektpartner nicht ersichtlich, welche Parteien noch im Projekt involviert und wo Informationen gespeichert sind.

Vertraulichkeitsvereinbarungen (NDA)

Durch die Übermittlung von Daten an einen Webdienst kann es letztlich zu einem Verstoß gegen Vertraulichkeitsvereinbarungen (Non Disclosure Agreement) kommen. Oftmals erklären Vertraulichkeitsvereinbarungen schlicht „alle gegenseitig ausgetauschten Informationen" als vertraulich, um zu vermeiden, dass jeweils bestimmt und bezeichnet werden muss, ob etwas vertraulich ist. In diesem Fall ist jede Bekanntgabe von Informationen an andere als die Projektpartner ein Verstoß, auch bei augenscheinlich nicht sensiblen Informationen.

Zu beachten ist ferner, dass sich ein Projektpartner auch nicht unbedingt auf ihm nicht nachvollziehbare technische Sicherungen wie div. Verschlüsselungen zur Vermeidung einer Offenlegung verweisen lassen muss. Zwar werden bestimmte Verschlüsselungen als ausreichend für eine Anonymisierung von Daten i.S.d. gesetzlichen Datenschutzes angesehen. Jedoch gilt in vertraglichen Beziehungen vorrangig der vereinbarte Parteiwille. Ist die Weitergabe von Daten nach dem Parteiwillen in einem NDA verboten, so kann das Verbot nicht von einem Vertragspartner einseitig durch Verwendung bestimmter technischer Hilfsmittel aufgehoben werden. Denn der andere Vertragspartner darf sich auf den Vertrag verlassen und muss sich nicht auf bestimmte Verschlüsselungen verweisen lassen, welche er ggf. nicht einmal nachvollziehen kann. Diese sind gerade bei Webdiensten häufig weder ausreichend stark, noch schützen sie vor einer Kenntnisnahme des Dienstes selbst. Verstöße gegen Vertraulichkeitsvereinbarungen sind oft mit Vertragsstrafen abgesichert.

Abweichende Zuordnung von Nutzungsrechten gem. den AGB des Dienstes

Ein typisches Problem kann auftreten, wenn nach den Nutzungsbedingungen des Dienstes (nachfolgend auch „AGB" oder „EULA" genannt) dem meist kostenlosen Webdienst zu seiner Finanzierung bestimmte Nutzungsrechte eingeräumt werden. Dies betrifft bspw. Rechte an der über seine Systeme geführten Kommunikation oder an bei ihm eingestellten Daten und Informationen (E-

Mailauswertung nach Stichworten, Rechte an textuellen Threads, publizierten Bildern oder Videos oder ein Recht, angemeldete Firmenkunden als Referenzen benennen zu dürfen etc.).

Die aus Sicht des Nutzers oftmals intransparente bzw. von ihm unbeabsichtigte Einräumung von Nutzungsrechten kann, so sie AGB-rechtlich wirksam ist, verschiedene Folgen haben (In wie weit dies AGB-rechtlich zulässig ist, ist im Einzelfall oft unklar, v.a. da auch ausländisches Recht zu berücksichtigen sein kann. In jedem Fall bleibt eine Rechtsunsicherheit, welche Projektpartner nicht hinnehmen müssen):

- Sie kann zum einen den Projektvereinbarungen zur Zuordnung der Nutzungsrechte im Verhältnis der Projektpartner widersprechen und deren spätere Verwertungsmöglichkeiten beeinträchtigen, bspw. wenn Auftraggeber ausschließliche Rechte fordern aber einzelne Rechte vorab einem Webdienst eingeräumt wurden.
- Sie kann weiterhin im Widerspruch zu den Vorgaben eines Auftraggebers stehen, v.a. bei öffentlich geförderten EU-Projekten, bei denen häufig alle erarbeiteten Ergebnisse der Öffentlichkeit zustehen müssen und nicht vorab an einen Webdienst abgetreten werden dürfen.

2.1.2 Verstoß gegen Nutzungsbedingungen mit dem Dienst (AGB)

Weiterhin kann durch die Nutzung eines Webdienstes auch gegen die Nutzungsbedingungen des Dienstes selbst verstoßen werden. Die Nutzungsbedingungen eines Webdienstes können eine Vielzahl von für ein Unternehmen nachteiligen Regelungen enthalten, auf die in diesem Zusammenhang nicht umfassend eingegangen werden kann. Besonders wichtig ist:

Erlaubnis kostenloser Nutzung nur zu privaten Zwecken

Teilweise räumen Webdienste ein Recht zur kostenlosen Nutzung nur für die Privatnutzung ein, nicht aber für eine geschäftliche Verwendung. Bekanntes Beispiel hierfür sind z.B. für Private kostenlose Viren-Scanner. In diesen Fällen erfolgt die kostenlose bzw. nicht lizenzierte Nutzung für ein Unternehmen unrechtmäßig und führt zu einem Lizenzverstoß. Mögliche negative Rechtsfolge sind Auskunfts-, Unterlassungs- und Schadensersatzansprüche des Rechteinhabers, sprich des Software-Herstellers.

2.1.3 Verstoß gegen gesetzliche Datenschutz-Anforderungen

Das Datenschutzrecht schützt das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung natürlicher Personen. Es schützt dies durch ein **generelles Verbot** der Verwendung personenbezogener Daten, es sei denn, **es besteht eine legitimierende Rechtsgrundlage**. Diese kann eine gesetzliche Grundlage oder eine Einwilligung sein. Werden dagegen keine personenbezogenen Daten verarbeitet, ist das Datenschutzrecht schon nicht anwendbar.

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG **alle Einzelangaben** über persönliche oder sachliche Verhältnisse einer bestimmbaren natürlichen Person. Beispiele sind Namen, Adressen, E-Mail-Adressen, Telefonnummern, Geburtsdaten und nach vorwiegender Ansicht auch (dynamische) IP-Adressen. Das Datenschutzrecht differenziert (abgesehen von Ausnahmen aufgrund von EU-Richtlinien) im Grundsatz nicht danach, ob Daten als besonders „schützenswert" beurteilt werden - anders als bspw.das Wettbewerbsrecht beim Schutz von Geschäftsgeheimnissen. Grund hierfür ist, dass das Datenschutzrecht nicht vorrangig die Daten, sondern die Identität eines Menschen in bestimmten Kontexten schützt. Wird bspw. ein vorgeblich harmloses Datum wie der Namen auf einer Fahndungsliste genannt, so entwickelt es für den Betroffenen höchste Bedeutung. Wird bspw. eine IP-Adresse auf einer Liste von Personen mit bestimmten negativen Eigenschaften genannt, gilt nichts anderes. Dies berücksichtigend, hat das Bundesverfassungsgericht schon 1983 festgestellt, dass es „unter den Bedingungen der modernen Datenverarbeitung kein harmloses Datum mehr gibt". Der Betroffene soll selbst wissen und entscheiden können wer was über ihn weiß („Selbstbestimmung"). Dies kann er nicht, wenn Daten ohne sein Wissen an Dritte weitergegeben werden.

Folgerichtig schützt das Datenschutzrecht selbst bei **öffentlich zugänglichen** Daten davor, dass diese frei gesammelt und elektronisch gespeichert werden dürfen, da die moderne elektronische Datenverarbeitung sowie die Kombination mit weiteren Datensammlungen Rückschlüsse über den Betroffenen erlaubt, die dessen Selbstbestimmung beeinträchtigen. Unabhängig von der Tatsache, dass bspw. bei Publikationsdiensten veröffentlichte Informationen aus technischer Sicht tatsächlich leicht gesammelt und ausgewertet werden können (weswegen man dringend davon abraten sollte, dies zu tun, wenn einem daran gelegen ist, die Daten für sich zu behalten), erlaubt das Datenschutzrecht im Grundsatz keine freie Verwendung öffentlich zugänglicher personenbezogener Daten. Vielmehr fordert es, selbst in dem begrenzten Umfang, indem die öffentliche Zugänglichkeit als Grundlage einer Datenverarbeitung ausnahmsweise herangezogen werden soll eine Interessenabwägung (so nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG für Beziehungen außerhalb von Verträgen). Diese fällt zumindest dann gegen eine Verarbeitungsbefugnis aus, wenn der Betroffenen einfach um seine Einwilligung gefragt werden könnte, bspw. ein befreundeter Wissenschaftler, der irgendetwas in einem Weblog publiziert hat. In gewisser Weise verhält es sich damit datenschutzrechtlich ähnlich wie beim Urheberrecht. Auch aus urheberrechtlicher Sicht geht die Rechtsprechung nicht davon aus, dass im Internet veröffentlichte Inhalte allein wegen der öffentlichen Zugänglichkeit frei verwendet werden dürfen.

Personenbezogene Daten können seitens der Mitarbeiter, aber auch seitens der Projektpartner oder deren Lieferanten vorliegen. Entscheidend ist immer, dass eine Eigenschaft einer natürlichen Person mit **gewisser Wahrscheinlichkeit zugeordnet** werden kann, d.h. die Wahrscheinlichkeit der Bestimmbarkeit genügt, auch wenn diese erst mit Hilfe Dritter gelingt und dies nicht völlig unwahrscheinlich ist. Aus diesem Grund werden bspw. auch (dynamische) IP-Adressen von den Aufsichtsbehörden als personenbezogen betrachtet. Deren Zuordnung ist nicht nur möglich, sondern in vielen Fällen aufgrund der Zusammenarbeit verschiedener Provider und Anbieter Gang und gäbe. Nicht entscheidend ist dagegen, ob die Eigenschaft irgendwie „brisant" ist (s.o.) und ob ein einzelner Mitarbeiter den Bezug zu einem Betroffenen herstellen kann, wenn es doch seiner Organisation gelingen kann.

Eine die Datenverarbeitung legitimierende **gesetzliche Rechtsgrundlage besteht im Rahmen von Vertragsbeziehungen häufig in § 28 Abs. 1 Satz 1 Nr. 1 BDSG** (Bundesdatenschutzgesetz), allerdings beschränkt auf 1) die Datenverarbeitung nur von Daten der Vertragspartner – also nicht bzgl. Daten Dritter, 2) nur zum Zweck der Vertragsdurchführung und 3) begrenzt auf den erforderlichen Umfang der Datenverarbeitung. Damit ist eine Verarbeitung unter Zuhilfenahme Dritter oder eine Verarbeitung zu anderen Zwecken als vertraglich vereinbart (z.B. zur Werbung des Webdienstes oder zur Verwertung durch Weitergabe vom Webdienst an dessen Partner) nicht möglich, sondern es bedarf einer **individuellen Einwilligung** der Betroffenen (zu den Anforderungen der Einwilligung s. die Maßnahmen unter Ziffer 3.1).

Nur zur Klarstellung sei aber nochmals darauf hingewiesen, dass in jedem Fall personenbezogene Daten verarbeitet werden müssen, damit das Datenschutzrecht überhaupt anwendbar ist. Gibt bspw. ein Mitarbeiter die E-Mail-Adresse eines befreundeten/kooperierenden Kollegen vorname.nachname@xy.de bei einem Webdienst an, etwa, damit über die Versandfunktion des Webdienstes eine Terminanfrage zugestellt werden kann, so bedarf es für diese Datenübermittlung einer Rechtsgrundlage. Nutzen nicht beide ohnehin schon den Dienst oder sind sonst über dessen Nutzung einig (rechtlich würde dies eine vertragliche Abrede bedeuten), bedarf es der vorherigen Einwilligung des Betroffenen. Würde der Mitarbeiter dagegen ein nur anonymes Kürzel eingeben, etwa die Initialen bei einem Terminfindungsdienst, und den Link zur Koordination selbst über seinen Mail-Client versenden, hätte der Dienst keine personenbezogenen Daten des Betroffenen bekommen, weswegen der Betroffene auch nicht vorher einwilligen müsste.

Outsourcing ohne schriftliche Auftragsvereinbarung

Sollen bestimmte Tätigkeiten im Rahmen eines „einfachen Outsourcing" ausgelagert werden, sind häufig Daten Externer/Dritter von der Auslagerung betroffen, mit denen weder ein Vertrag besteht (§ 28 BDSG) noch eine Einwilligung abgegeben wurde.

In den Fällen, in denen nur eine einfache technische Datenverarbeitung ausgelagert werden soll, in der der Auftragnehmer nur als „verlängerter Arm" des Auftraggebers **Hilfsleistungen** erbringt (kein Business Process Outsourcing), gilt: Das BDSG gibt eine legitimierende **gesetzliche Rechtsgrundlage** für die Datenübermittlung in **§ 11 BDSG (Auftragsdatenverarbeitung), ohne dass die Betroffenen einwilligen müssen** (dies ist der entscheidende Punkt. Liegt eine Einwilligung vor, darf im Grunde ohnehin alles mit den Daten der Einwilligenden gemacht werden und man benötigt keine gesetzliche Rechtsgrundlage. Allerdings sind bei solchen Auslagerungen die vielen erforderlichen Einwilligungen praktisch nicht einholbar). Hintergrund der Auftragsdatenverarbeitung ist, dass sich der Auftraggeber auf sein Kerngeschäft konzentrieren darf und automatisiert ablaufende Technik auslagern kann, ohne die Betroffenen fragen zu müssen. Dafür werden ihm die Handlungen seines Auftragnehmers wie eigene zugerechnet.

Die Auftragsvereinbarung hat verschiedene Anforderungen. Sie setzt v.a. voraus, dass der Auftragsverarbeiter den Weisungen und Kontrollen des Auftraggebers unterliegt, und dass zwischen Auftraggeber und Auftragnehmer eine **detaillierte schriftliche** Vereinbarung nach den Vorgaben des § 11 BDSG abgeschlossen wird. Schriftlich bedeutet im Rechtsverkehr handschriftlich unterzeichnet auf Papier. Dabei dient die Schriftform nicht nur der Beweissicherung für die Vertragspartner und der Fixierung des Vereinbarten (und damit gerade bei der Auftragsdatenverarbeitung, in der die Vertragspartner die Datenverarbeitung von Daten Dritter regeln, die nicht am Vertrag beteiligt sind, der Ermöglichung der Datenschutzaufsicht der Behörden), sondern erfüllt auch eine Warnfunktion. Die Hürde der Schriftform wird absichtlich gelegt, damit die Verantwortlichen eigenhändig und mit den klaren Haftungsfolgen bei Verstößen einen Vertrag abschließen müssen, was aufgrund der Zeichnungsbefugnisse und der dann nachvollziehbaren Verantwortung in einem Unternehmen erfahrungsgemäß mehr Sorgfalt und Aufwand erzwingt, als das in einem vollen Arbeitstag leicht mögliche „Wegklicken" elektronischer Erklärungen. Die Hürde der Schriftform ist also kein gesetzliches Relikt, sondern Absicht.

Da jedoch regelmäßig keine der vorab genannten Voraussetzungen bei Einschaltung eines Webdienstes erfüllt sind, scheidet eine Auftragsdatenverarbeitung als Legitimation der Übermittlung und Verarbeitung personenbezogener Daten meistens aus. Erste Anbieter stellen dem Nutzer allerdings schriftliche Vereinbarungen zur Verfügung, bspw. Google bzgl. Analytics (wobei speziell dort noch andere Datenschutzmängel bestehen, aber die Anbieter befinden sich auf dem „richtigen Weg") oder Microsoft bzgl. bestimmter Services/ Webdienste zu Office 365 oder Wired Minds.

Daneben kann zum Outsourcing von ganzen Geschäftsprozessen (BPO) auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG zurückgegriffen werden, der jedoch wegen der darin vorgesehenen Interessenabwägung im Einzelnen kompliziert anzuwenden ist und zudem restriktiv ausgelegt wird und in der Praxis mit erheblichen vertraglichen Vereinbarungen flankiert wird. Für den Einsatz bei Webdiensten ist er nur bedingt anwendbar. Es kann bei der Interessenabwägung insbesondere nicht davon ausgegangen werden, dass personenbezogene Daten von bekannten Projektpartnern oder bekannten Mitarbeitern ohne Weiteres an einen Webdienst übermittelt werden können, um eine an sich erforderliche und relativ leicht einholbare Einwilligung zu umgehen.

Verletzung des Erforderlichkeitsprinzips

Ein bei der Verarbeitung personenbezogener Daten immer zu beachtendes Grundprinzip ist das Erforderlichkeitsprinzip. Eine Datenverarbeitung ist nur dann erforderlich, wenn es keine sinnvolle und zumutbare Alternative zu ihr gibt. D.h., das allgemeine Erforderlichkeitsprinzip, das bei allen Verarbeitungsgrundlagen zu beachten ist, stellt eine relativ hohe Anforderung an eine per Gesetz (d.h. ohne Einwilligung) zulässige Datenverarbeitung. Zur Ermöglichung gezielter Werbung durch

einen Webdienst werden jedoch weit mehr personenbezogene Daten erhoben und verarbeitet, als zur reinen Vertragsdurchführung unbedingt erforderlich sind, was ohne Einwilligung der Betroffenen unzulässig ist. Schließt bspw. ein Mitarbeiter einen Vertrag mit einem Synchronisierungs- oder Cloud-Speicher-Dienst (Anm.: dies ist ein zweiseitiger Vertrag i.R.v. § 28 Abs. 1 Satz 1 Nr. 1 BDSG, der formfrei möglich ist, d.h. per Mausklick auf AGB des Dienstes. Es geht hier nicht um Auftragsdatenverarbeitung von Daten Dritter, welche schriftlich erfolgen muss), wonach der Dienst dessen eigene Daten online vorhalten soll, so wird der Dienst erfahrungsgemäß weit mehr Daten über seinen Nutzer erheben, als zum Datenspeichern und Synchronisieren erforderlich sind. Insbesondere wird er meistens auch das Surfverhalten protokollieren, um eine personalisierte Werbung zu ermöglichen. Dies ist nicht für die Erbringung der geschuldeten Leistung erforderlich, weswegen es zur Werbung einer Einwilligung bedürfte und nicht auf § 28 BDSG als Rechtsgrundlage zurückgegriffen werden kann.

Bezüglich eines Outsourcing gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG (Interessenabwägung) oder bei einfachen Hilfsdiensten gem. § 11 BDSG (Auftragsdatenverarbeitung), bei denen fraglich ist, ob aufgrund einer Vereinbarung zweier Parteien (bspw. Nutzendes Unternehmen mit einem Webdienst) auch Daten Dritter an den Anbieter gesendet werde dürfen, etwa Daten von Kooperationspartnern bei der Dokumentenverwaltung, der Speicherung von gemeinsamen Arbeitspapieren oder der Terminkoordination, ist ebenso fraglich, ob das Outsourcing dieser Funktionen auf den Webdienst erforderlich ist, sprich es keine zumutbaren Alternativen gibt: etwa eigene oder andere Dienste oder eine Tätigkeit wie bisher, z.B. eine Abstimmung per E-Mail, oder das Einholen einer Einwilligung. Dies wird meist der Fall sein, weswegen das Outsourcing wiederum eine Einwilligung erfordert.

Folge von Datenschutzverstößen

Erfolgt die Übermittlung und Verarbeitung personenbezogener Daten an bzw. bei einem Webdienst ohne eine legitimierende Rechtsgrundlage, insbesondere ohne Zustimmung der Projektpartner bzw. Einwilligung der betroffenen Mitarbeiter oder Betriebsvereinbarung, so kann darin eine Ordnungswidrigkeit oder eine Straftat gem. §§ 43, 44 BDSG liegen.

2.1.4 Verstoß gegen gewerbliche Schutzrechte, Namensrechte, Urheberrechte

Durch die Verwendung und Übermittlung bestimmter Daten, insbesondere deren Bekanntgabe und Publikation, können gewerbliche Schutzrechte verletzt werden.

Verletzung von Markenrechten und Unternehmenskennzeichen

Das Markengesetz (MarkenG) schütz gem. § 1 MarkenG Marken (Wort- und Bildmarken), geschäftliche Bezeichnungen (Unternehmenskennzeichen und Werktitel) sowie geographische Herkunftsangaben. Dem Rechteinhaber steht jeweils das ausschließliche Nutzungsrecht zu, d.h. er kann gegenüber einem unberechtigten Nutzer Auskunft und Unterlassung verlangen sowie Schadensersatz fordern.

Werden Dateien oder Informationen, die durch das Markengesetz geschützt sind, beispielsweise Logos, textuelle Unternehmenskennzeichen oder sonstige Grafiken, ohne Zustimmung des ausschließlichen Rechteinhabers an einen Webdienst übermittelt bzw. dort publiziert, so stehen dem Rechteinhaber die genannten Instrumente zur Sicherung seiner Rechte zu. Solche Konstellationen sind insbesondere dann denkbar, wenn Webdienste durch Verwendung von Logos etc. personalisiert bzw. für bestimmte Arbeitsgruppen spezifiziert werden. Insofern ist wiederum eine vorherige Zustimmung des Rechteinhabers erforderlich.

Verletzung von Namensrechten

Auch ohne den speziellen und weitgehenden Schutz des Markengesetzes sind die Namensrechte von natürlichen und juristischen Personen nach § 12 BGB geschützt. D.h. die Firma eines Unternehmens ist geschützt, auch wenn sie nicht als Marke registriert ist. Dem Berechtigten stehen im Falle

einer unberechtigten Nutzung wiederum die Rechte auf Auskunft, Unterlassung und Schadensersatz zu. Insofern gelten die Ausführungen zum Markenrecht entsprechend.

Verletzung von Urheber- und Nutzungsrechten

Soweit ein Unternehmen urheberrechtlich geschützte Inhalte von Dritten wie Projektpartnern oder Auftraggebern erhält (bspw. Logos, Präsentationen, Vertragsvorlagen oder Texte), dürfen diese nicht ohne Weiteres an einen Webdienst übermittelt und dort gespeichert oder gar veröffentlicht werden. Ohne Zustimmung des Projektpartners oder Auftraggebers und ohne eine die Nutzung konkretisierende Regelung ist davon auszugehen, dass eine Weitergabe an Dritte nicht zulässig ist.

Gleichermaßen bedarf es der Zustimmung der Rechteinhaber bei aus dem Internet heruntergeladenen Werken, soweit diese nicht aufgrund bestimmter ausdrücklicher Lizenzen frei verwendet werden dürfen.

Ein Verstoß gegen urheberrechtliche Vorgaben ist nach §§ 106 UrhG ff. mit einem Bußgeld belegt oder strafbewehrt.

2.1.5 Verstoß gegen Vorschriften zur Exportkontrolle

Teilweise verwenden Webdienste Technologien, die dem gesetzlichen Exportkontrollrecht unterliegen, v.a. im Bereich der Kryptographie. Der Versand kontrollierter Technologie (bspw. Hardware, Software, aber auch bestimmter Daten) in bestimmte Länder kann genehmigungspflichtig sein. Gleiches kann für die Nutzung im Gebiet bestimmter Ländern oder durch Angehörige dieser Länder sein. Bei Webdiensten kann etwa das Übertragen von Indizes in die Cloud oder das Ablegen von Daten auf den Servern bestimmter Länder untersagt sein. So unterliegt bspw. die Nutzung des Dienstes Dropbox und seiner Software nach den Dropbox-Nutzungsbedingungen Stand 2011 der Exportkontrolle der Vereinigten Staaten. Dropbox darf danach nicht von Personen aus Ländern verwendet werden, die unter einem US-amerikanischen Embargo stehen.

Die Folgen bei Verstößen gegen Exportkontrollvorschriften sind sehr streng. Sie umfassen neben der Untersagung der Nutzung Bußgelder, die persönliche ordnungsrechtliche Verfolgung und insbesondere den Ausschluss bei öffentlichen Ausschreibungen. Zudem gehen mit solchen Verstößen meist erhebliche Reputationsschäden bei öffentlichen Auftraggebern einher.

2.1.6 Verstoß gegen interne Regelungen

Die Einschaltung eines Webdienstes kann darüber hinaus auch gegen interne Regelungen eines Unternehmens verstoßen.

Verstoß gegen Betriebsvereinbarungen

Auch Betriebsvereinbarungen können dem Einsatz eines Webdienstes oder bestimmten Funktionen entgegenstehen, insbesondere soweit personenbezogene oder persönliche Daten von Mitarbeitern an einen Webdienst übermittelt werden.

So verbieten bspw. Betriebsvereinbarungen häufig die Verarbeitung von Personaldaten außerhalb der eigenen Räumlichkeiten, was den Austausch solcher Daten etwa über Dropbox ausschließt. Oder das Verbringen von personenbezogenen Daten in andere Systeme wird generell von der Zustimmung des Betriebs-/Personalrats abhängig gemacht.

Missachtung von Organisationsanweisungen

Organisationsanweisungen informieren vielfach über abgeschlossene Betriebsvereinbarungen und bestimmte Aspekte daraus. Sie können aber im Einzelfall auch Vorgaben enthalten, die die Nutzung von Webdiensten betreffen. Beispielsweise finden von einem Unternehmen typischerweise zum Selbstschutz verwendete Einkaufsbedingungen, welche bei einer Beauftragung von Subunternehmern über den formellen Einkauf regelmäßig verwendet werden, keine Anwendung im Verhältnis

zum Webdienst. Die Folge ist ein geltendes Regelwerk, das möglicherweise vollkommen von den sonst verwendeten Vorgaben abweicht.

2.1.7 Verstoß gegen gesetzliche Mitbestimmungsrechte

Der Einsatz eines Webdienstes kann zahlreiche Rechte des Betriebs-/Personalrats nach dem Betriebsverfassungsgesetz (BetrVG) auslösen, insbesondere Beteiligungs-, Mitwirkungs- und Mitbestimmungsrechte zur Planung und Ausgestaltung von Arbeitsplätzen, Betriebsorganisation und Technik

Zunächst steht dem Betriebs-/Personalrat über die Generalklausel des § 80 Abs. 1 Nr. 1 BetrVG ein allgemeines Mitwirkungsrecht zu. Er hat danach über die Durchführung der zugunsten der Arbeitnehmer geltenden gesetzlichen, tariflichen und sich aus Betriebsvereinbarungen ergebenden Bestimmungen zu wachen. Hierzu gehören in erster Linie das Arbeitsschutzrecht, aber auch datenschutzrechtliche Bestimmungen.

Wichtigstes Recht des Betriebs-/Personalrats bei der Einführung technischer Einrichtungen ist das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Danach besteht ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Nach Sinn und Zweck der Regelung geht die Rechtsprechung davon aus, dass es für die Anwendung bereits genügt, wenn die bloße **Möglichkeit** einer Überwachung besteht (entgegen dem Wortlaut „bestimmt sein"). Da dies über die Arbeitszeit bei praktisch allen technischen Hilfsmitteln der Fall ist und die Norm von den Gerichten sehr weit ausgelegt wird (z.B. auch für das Bezahlen mit einer Mitarbeiter-Chipkarte am Kaffeautomat oder bei der Nutzung von Webbrowsern), kommt dem Betriebs-/Personalrat nahezu immer ein Mitbestimmungsrecht beim Einsatz von IuK-Technologien zu. Dies gilt entsprechend beim Einsatz der meisten Webdienste. Bei den meisten Webdiensten besteht z.B. über die Möglichkeit, Zugriffszeiten zu erfassen, eine Kontrollmöglichkeit. Allerdings hat der Betriebs-/Personalrat sein Zustimmungsrecht für die bloße Kontrollmöglichkeit über die Surfspuren des Webbrowsers oftmals bereits durch eine Betriebsvereinbarung ausgeübt und zu den darin gegebenen Bedingungen zugestimmt. Einer gesonderten Zustimmung bedürfte es daher v.a. dann, wenn ein Webdienst weitere, neue Kontrollmöglichkeiten eröffnet, bspw. über neue Funktionen, oder bei einer grundlegenden Umgestaltung von Arbeitsabläufen und Prozessen (nicht nur das individuelle oder geringfügige Nutzen eines Webdienstes durch einen Mitarbeiter). Ein Beispiel für das Bestehen eines Mitbestimmungsrechts wäre die umfangreiche Nutzung eines Kollaborations-Dienstes, bei dem - ähnlich wie bei gemeinsamen Arbeitsplattformen anerkannt - ein Mitbestimmungsrecht bestünde, da Kollegen und Vorgesetzte über den Webdienst (nicht nur das Surfen) erfahren, wer wann was macht und bspw. welche Dokumente einstellt. Nutzt dagegen ein Mitarbeiter mit einem befreundeten Wissenschaftler einen Terminfindungsdienst wie Doodle, so können zwar (datenschutz)rechtliche Fragen betroffen sein, jedoch liegt keine Einführung einer neuen kontrollgeeigneten technischen Einrichtung vor, welche ein Mitbestimmungsrecht auslöst.

Um dem Betriebs-/Personalrat die Wahrnehmung dieser Rechte zu ermöglichen, ist er rechtzeitig und umfassend nach § 90 Abs. 1 BetrVG (ggf. bei grundlegender Änderung der Betriebsorganisation auch nach § 111 Satz 2 Nr. 4) zu unterrichten, also bereits im Planungsstadium. Erforderliche Unterlagen sind ihm vorzulegen.

Werden Webdienste ohne Konsultation des Betriebs-/Personalrats eingesetzt besteht daher die Gefahr, dessen Mitwirkungsrechte zu verletzen.

2.2 Drohender Verlust von Know-How und Geschäftsgeheimnissen

Bei der Nutzung von Webdiensten kann geistiges Eigentum beeinträchtigt werden:

- Preisgabe von Know-How
- Verlust eigener Geschäftsgeheimnisse
- Verlust von Geschäftsgeheimnissen Dritter (Projektpartner, Auftraggeber)
- Verlust der Patentfähigkeit durch Vorveröffentlichung

2.2.1 Preisgabe von Know-How

Viele Unternehmen verfügen über teilweise sehr spezielles Know-How. Der Begriff des Know-How ist allerdings ein eher praktischer Begriff denn ein juristischer. Im rechtstechnischen Sinn gibt es keinen „Know-How-Schutz". Der Begriff Know-How meint sämtliche Kenntnisse, die durch eine bestimmte Erfahrung oder ein spezielles Wissen erworben worden sind und mit denen der Inhaber ein bestimmtes Ergebnis erzielen kann. Geheimes Know-How ist darüber hinaus meistens ein geschütztes Betriebs- und Geschäftsgeheimnis (s.u.).

Grundsätzlich besteht die Gefahr, dass ein Webdienst bei der Nutzung von dem Know-How erfährt, sei es über Arbeitsinhalte, Verfahren und Methoden, fachlich kompetente Mitarbeiter oder Geschäftsbeziehungen zu Kommunikationspartnern. Solche Informationen können für den Webdienst aber auch Dritte finanziell werthaltig sein und Begehrlichkeiten wecken, an diese Informationen zu gelangen.

Aus juristischer Sicht ist einem unkontrollierten Abfluss von Know-How im Rahmen des IT-Sicherheitsmanagement entgegenzuwirken. Das IT-Sicherheitsmanagement verpflichtet als Teil des allgemeinen Risikomanagement den Vorstand/die Geschäftsleitung, den Bestand der Gesellschaft und deren finanzielle Situation zu erhalten. Die Risiken sind durch ein Erkennungssystem gezielt zu managen und zu bewerten, bspw. durch technische und juristische Prüfungen der Webdienste aber auch interne Dienst- und Organisationsanweisungen oder Handlungshilfen.

Nach den Grundsätzen des Risikomanagements kommt eine persönliche zivilrechtliche Schadensersatzhaftung in Betracht, wenn Risiken aus der Nutzung von Webdiensten nicht ausreichend überwacht werden und Risiken gegenüber nicht vorgebeugt wird. Dies ergibt sich für die Vorstände von Aktiengesellschaften und Geschäftsführer von GmbHs explizit aus dem Gesetz, gilt nach einhelliger Ansicht aber entsprechend für die Geschäftsleitung anderer Gesellschaftsformen, wenn die Unternehmen in entsprechendem Umfang am Markt auftreten.

2.2.2 Offenlegung eigener Betriebs- und Geschäftsgeheimnisse

Ein besonderer Schutz besteht für Betriebs- und Geschäftsgeheimnisse, welche über das allgemeine Know-How einer Gesellschaft hinausgehen. Der Begriff des Betriebsgeheimnisses umfasst insbesondere die technischen und organisatorischen Aspekte eines Geheimnisses, der Begriff des Geschäftsgeheimnisses v.a. kaufmännische, kommerzielle und finanzielle Aspekte. Häufig wird in der Praxis zwischen beiden Begriffen nicht differenziert. Gemeinsam ist beiden nach der Definition der Rechtsprechung, dass die geheim gehaltenen Tatsachen, Umstände und Vorgänge nur einem begrenzten Personenkreis bekannt sind, der Rechtsträger ein berechtigtes Interesse an der Nichtverbreitung hat, die Geheimnisse für Außenstehende wissenswert sind und deren Veröffentlichung dem Rechtsträger zum Nachteil gereichen kann. Betriebs- und Geschäftsgeheimnisse finden sich beispielsweise in den Ergebnissen wissenschaftlicher Arbeit, können sich aber auch auf geheimhaltungsbedürftige Vertragsbeziehungen oder Prozesse beziehen.

Betriebs- und Geschäftsgeheimnisse sind nach §§ 17, 18 des Gesetz gegen unlauteren Wettbewerb (UWG) v.a. gegenüber einer unbefugten Verwendung durch Beschäftigte des Geheimnisträgers und nach §§ 203, 204 Strafgesetzbuch (StGB) bzgl. bestimmter Berufsträger wie Rechtsanwälten oder

Ärzten geschützt, nämlich gegen die unbefugte Beschaffung, Mitteilung, Veröffentlichung und Verwertung. Ein Verstoß nach dem UWG setzt i.d.R. voraus, dass die Tathandlung zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, geschieht. Daher sind solche Verstöße durch Nutzer bei einer Übermittlung von Geheimnissen an einen Webdienst zwar denkbar, mangels der geforderten Zweckbestimmung aber praktisch eher selten.

Allerdings werden Betriebs- und Geschäftsgeheimnisse neben den gesetzlichen Vorschriften auch durch Vertraulichkeitsvereinbarungen in Arbeitsverträgen geschützt, ohne dass eine Verletzung der Schutzvorschrift bestimmte Zwecke wie den Wettbewerb oder Eigennutz voraussetzt. Ganz generell kann auch in Arbeitsverträgen die Bekanntgabe von Betriebs- und Geschäftsgeheimnissen an Dritte untersagt werden. Insofern besteht die Möglichkeit, dass Mitarbeiter durch die Übermittlung von Betriebs- und Geschäftsgeheimnissen der Gesellschaft an einen Webdienst einen arbeitsrechtlichen Verstoß begehen.

2.2.3 Offenlegung von Betriebs- und Geschäftsgeheimnissen Dritter

Weiterhin werden Betriebs- und Geschäftsgeheimnisse durch Vertraulichkeitsvereinbarungen zwischen Vertragspartnern geschützt. Durch Übermittlung von Betriebs- oder Geschäftsgeheimnissen eines Projektpartners oder durch Übermittlung gemeinsam erarbeiteter Geheimnisse kann es zu einem Verstoß gegen die Vertraulichkeitsvereinbarung kommen. An solche Verstöße sind häufig Rechtsfolgen wie Vertragsstrafen oder Kündigungsrechte geknüpft.

2.2.4 Verlust der Patentfähigkeit von Erfindungen durch Vorveröffentlichung

Der Wert wissenschaftlicher Arbeit mündet häufig in Patenten, die dem Erfinder das ausschließliche Nutzungsrecht an einer Erfindung geben und eine größtmögliche wirtschaftliche Verwertung der Erfindung ermöglichen. Bei einem nicht vom Unternehmen kontrollierbaren Webdienst besteht in besonderer Weise die Gefahr, dass erfindungsrelevante Daten nicht vertraulich gespeichert werden und an Dritte gelangen, welche die Daten dann publizieren. Dies kann bspw. bei Kollaborationsdiensten oder Online-Speicher-Diensten der Fall sein, die unsicher gestaltet sind und daher leicht von Hackern angegriffen werden oder die anderen Nutzern versehentlich Zugriffsrechte gewähren.

Mit einem Patent werden nach § 1 Patentgesetz (PatG) neue, technische Erfindungen geschützt, die auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind. Die Neuigkeit einer Erfindung ist grundsätzlich dann gegeben, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst dabei gem. § 3 Abs. 1 PatG alle Kenntnisse, die vor dem Stichtag schriftlich, mündlich, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind. Dies bedeutet, dass eine ggf. auch nur unabsichtliche Veröffentlichung von Arbeitsinhalten durch einen Webdienst neuheitsschädlich ist und die spätere Patentierbarkeit ausschließen kann. In diesem Fall bestehen zwar theoretisch Ersatzansprüche gegen den Webdienst, allerdings dürften diese praktisch leerlaufen, da gerade kostenlose Webdienste in der Regel keine Haftung übernehmen, eine regelmäßig hohe Haftung wie bei Patentstreitigkeiten nicht übernehmen können. Zudem müsste im Schadensersatzverfahren erst hypothetisch geklärt werden, ob für eine Erfindung ohne die Vorveröffentlichung überhaupt ein Patent erteilt worden wäre. Insofern stellt die Nutzung von Webdiensten, an die Inhaltsdaten übermittelt werden, gerade bei Projekten mit erwarteten Patenten ein erhebliches Risiko für die spätere Verwertung der Arbeit dar, das von juristischen Laien nur schwer erkannt wird.

2.3 Rufschädigung

Sicherheitsvorfälle bei einem Webdienst können den Ruf der Gesellschaft schädigen:

- Enttäuschte Erwartung an die Vertraulichkeit eines professionellen Unternehmens
- Aufträge gehen verloren

Letztlich kann insbesondere durch Vertraulichkeitsverletzungen bei einem Webdienst, etwa durch die unbeabsichtigte oder durch Hacker herbeigeführte Bekanntgabe von Daten, ein Reputationsschaden auch bei der nutzenden Gesellschaft als Nutzer entstehen. Dies schon deshalb, wenn bekannt wird, dass die Gesellschaft vertrauliche Daten, Betriebs- oder Geschäftsgeheimnisse oder personenbezogene Daten bei einem Consumer-Webdienst verarbeitet. Dabei ist zu berücksichtigen, dass Reputationsschäden aufgrund ihrer Auswirkungen auf beispielsweise künftige Beauftragungen oder Ersatzansprüche im Verhältnis zu Projektpartnern immer auch eine juristische Frage des Erhalts der finanziellen Situation in der Gesellschaft und damit des Risikomanagements sind. Reputationsschäden, die beispielsweise durch entsprechende Vorsorgeprozesse verhindert werden könnten, können auch eine persönliche Haftung der für das Risikomanagement verantwortlichen Geschäftsleitung begründen.

2.4 Verlust von Rechten

Es können Nutzungs- und Gewährleistungsrechte verloren gehen:

- Rechtseinräumung an übermittelten und publizierten Inhalten
- Rechtseinräumung am Nutzungsverhalten (Surfen)
- Meistens für Werbung, auch zugunsten Dritter (User generated Content)
- Kombination der Daten mit anderen Diensten und Drittanbietern
- Fingierter Verzicht auf gesetzlich bestehende Ansprüche jeglicher Art, v.a. keine Haftung

2.4.1 Einräumen von Nutzungsrechten für Werbung

Da Webdienste häufig kein Entgelt von den Nutzern verlangen und sich durch Werbung finanzieren, lassen sich die Anbieter relativ weitgehende Nutzungsrechte von den Nutzern einräumen. In Betracht kommen Nutzungsrechte an den übermittelten und/oder publizierten Inhalten (textuelle Threads, Bilder, Videos etc.), aber auch an dem Nutzungsverhalten, aus dem auf zahlreiche Eigenschaften für eine personalisierte Werbung des Nutzers geschlossen werden kann. Dabei ist zu bedenken, dass Webdienste zunehmend mehr Wert auf rechtliche Compliance zu ihren Gunsten legen, bspw. weil größere Anbieter an die Börse gehen oder aber Investoren zum Kauf suchen, weswegen die Rechteregelungen tendenziell umfangreicher und auch rechtlich stabiler werden, als zu Web 2.0-Gründerzeiten. Werden danach Nutzungsrechte einem Webdienst eingeräumt, kann ein Urheber sein alleiniges oder ausschließliches Nutzungsrecht verlieren. Dies kann von Bedeutung sein, wenn er sich gegenüber anderen, bspw. im Rahmen eines Projektes, verpflichtet hat, alle Rechte an den Ergebnissen an den Auftraggeber zu übertragen, da er ggf. nicht mehr über alle Rechte verfügt. Dies kann etwa dann der Fall sein, wenn ein in einem Projekt erstellter Film zu einer Simulation in You Tube veröffentlicht wurde oder ein Vortrag für einen Auftraggeber mit einem Webdienst erstellt und dort gespeichert wurde.

In diesem Fall können einem Auftraggeber Gewährleistungsrechte zustehen, bspw. Minderungs- oder Schadensersatzansprüche.

2.4.2 Verzicht auf gesetzliche Ansprüche, keine Haftung, keine Gewährleistung

Neben dem Verlust urheberrechtlicher Nutzungsrechte verliert ein Nutzer meistens auch alle Gewährleistungsansprüche bzgl. der mangelfreien Leistungserbringung durch den Dienst und seine Schadensersatzansprüche (falls durch die Nutzung ein Schaden entsteht). Kostenlose Webdienste können die Risiken und Ersatzansprüche nicht in ihr Geschäftsmodell einpreisen und schließen daher alle Ansprüche aus. Dies bedeutet, dass ein Nutzer den Dienst nur so nutzen kann, wie er gerade eben funktioniert („as is"). Üblicherweise geltende Rechtsansprüche scheiden gegenüber Webdiensten meist aus. Dies bedeutet, dass bspw. ein Webdienst, der alle Daten aus Versehen unwiderruflich löscht, kein Backup vorhält oder aufgrund unsicheren Designs von Dritten gehackt wird, nicht zur Verantwortung gezogen werden kann.

Ein Beispiel für erhebliche Nachteile bei fehlenden Gewährleistungen wäre ein Online-Umfragedienst, bei dem Daten, die im Rahmen einer für einen Kunden durchgeführten Umfrage verfälscht oder gelöscht wurden. In einem solchen Fall können Schäden gegenüber dem Webdienstanbieter kaum geltend gemacht werden.

2.5 Unsichere Dienstegestaltung

Ein Webdienst kann technisch unsicher aufgebaut sein:

- Unzureichende technische Sicherheit da oft kostenloser Consumer-Dienst
- Keine Verschlüsselung bzgl. Login und Datenübertragung (SSL)
- Keine E2E-Verschlüsselung der gespeicherten Daten
- Unsichere Software und Plug-Ins

2.5.1 Kein Design auf Sicherheit

Kostenlose und für Consumer designte Webdienste enthalten oft erhebliche Mängel bezüglich der Sicherheit. Sie sind nicht auf Sicherheit oder die Anforderungen eines geschäftlichen Betriebs in bekannter Weise ausgelegt, sondern beruhen auf Innovation, Spielerei und Anreizen, den Nutzer möglichst lange auf ihren Webseiten zu halten. Es gab und gibt daher immer wieder Fälle, in denen bspw. Nutzer eines Dienstes vorübergehend und ohne ersichtlichen Grund in die Nutzerkonten anderer Nutzer einsehen konnten, oder in denen sonstige gravierende Sicherheitsmängel bekannt wurden. Einen guten Überblick über typische Sicherheitsmängel bei Webanwendungen geben die OWAS (Open Web Application Security Project) Top 10 aus 2010:[1]

A1 – Injection
A2 – Cross-Site Scripting (XSS)
A3 – Fehler in Authentifizierung und Session Management
A4 – Unsichere direkte Objektreferenzen
A5 – Cross-Site Request Forgery (CSRF)
A6 – Sicherheitsrelevante Fehlkonfiguration
A7 – Kryptografisch unsichere Speicherung
A8 – Mangelhafter URL-Zugriffsschutz
A9 – Unzureichende Absicherung der Transportschicht
A10 – Ungeprüfte Um- und Weiterleitungen

[1] https://www.owasp.org/images/b/b8/OWASPTop10_DE_Version_1_0.pdf

2.5.2 Unzureichende Verschlüsselung bei Übertragung und Speicherung

Ein wichtiges Kriterium für die Sicherheit eines Webdienstes ist das Vorhandensein von Mitteln zur Verschlüsselung. Dabei sollten sowohl die Datenübertragung vom Nutzer zum Webdienst verschlüsselt werden (z.B. über SSL) als auch die beim Dienst gespeicherten Daten.

Die Datenübertragung ist zur Vermeidung von Problemen häufig eingeschränkt, etwa wird beim Login die SSL-Verschlüsselung per Default ausgeschaltet und Passworte werden evtl. im Klartext übertragen.

Die Verschlüsselung der Daten beim Dienste-Betreiber ist meist gar nicht vorgesehen. Wird sie angeboten, so werden die Schlüssel oft vom Diensteanbieter oder -betreiber selbst verwaltet oder der Diensteanbieter hätte indirekt die Möglichkeit, versteckt Benutzer in Schlüsselaustauschgruppen einzuschleusen. Eine Sicherheit gegen Zugriffe der Mitarbeiter des Dienstes und des Betreibers besteht daher meist nicht. Insofern müssen sensible Daten in jedem Fall mit eigenen Mitteln Ende-zu-Ende verschlüsselt werden, bspw. über Tools wie Truecrypt.

2.5.3 Unsichere Software und Plug-Ins

Letztlich bieten zahlreiche Webdienste eigene Software an, so dass der Dienst auch ohne einen Webbrowser oder aber mit weiteren Funktionen genutzt werden kann. In Betracht kommen Browser Plug-Ins oder eigene Applikationen. In wie weit diese sicher programmiert sind, ist zumindest für einen normalen Nutzer nicht nachprüfbar. Im Unterschied zu den gängigen und bekannten Anwendungen ist auch hier die Tendenz zu beobachten, dass Plug-Ins und Applikationen v.a. neu, innovativ und schnell auf den Markt kommen, dabei aber kein Schwerpunkt auf Sicherheitstechnik gelegt wird. Vor der Installation von Software zu betrieblichen Zwecken auf einem betrieblichen Gerät ist daher in jedem Fall die IT-Administration zu konsultieren.

2.6 Gefährdungen der eigenen IT

Ein unsicherer Webdienst kann die übrige IT-Infrastruktur gefährden:

- Kompromittieren der übrigen IT-Infrastruktur
- Einschleusen von Schad-Code/ Plug-Ins
- Tunneln von Firewalls

Sicherheitsmängel bei einem Webdienst betreffen nicht nur die Dienstenutzung oder das Endgerät des Nutzers, sondern können auch ein Einfallstor für weitergehende Angriffe auf die eigene IT sein.

So kann über unsichere Applikationen oder Plug-Ins weiterer Schadcode (Viren, Trojaner) eingeschleust werden, weil diese Software manipuliert oder fehlerhaft ist oder weil veraltete Versionen nicht aktualisiert wurden. Da die Datenverbindung einiger Webdienste die betrieblichen Firewalls tunnelt, d.h. nicht einsehbar ist, besteht auch kaum eine Kontrollmöglichkeit festzustellen, welche Daten über eine Webdienste-Software aus der Gesellschaft heraus versendet werden bzw. wie von außen auf interne IT-Ressourcen zugegriffen wird.

2.7 Datenmissbrauch und Weitergabe durch Betreiber oder Dritte

Daten des Nutzers können unerwünscht verwertet oder sogar illegal missbraucht werden:

- Unerwünschte oder nicht bekannte, aber grds. legale Verwertung durch den Dienst
- Illegale Verwertung durch den Dienst, z.B. bei Insolvenz oder durch Mitarbeiter
- Datenzugriff durch Hacker oder Zufallsfunde sowie anschließende illegale Verwertung
- Datenzugriff durch Konkurrenten aufgrund behördlicher Erlaubnis
- Datenzugriff durch Behörden und (Sicherheits-)Dienste
- Legitimation von Zugriffen nach ggf. ausländischem Recht (z.B. Patriot Act)

Die Daten der Nutzer sind das wichtigste Kapital eines kostenlosen Webdienstes. Jede Nutzung eines Dienstes hinterlässt eine Vielzahl von Datenspuren, die alleine oder zusammen mit anderen Daten für Dritte finanziell lukrativ sind. Dementsprechend groß sind auch potentiell die Begehrlichkeiten der Betreiber und Dritter, Daten zu verwerten.

2.7.1 Datenmissbrauch durch den Betreiber

Da sich viele Webdienste umfangreiche Nutzungsrechte an den Daten der Nutzer einräumen lassen, kann rechtstechnisch oft nicht von einem „illegalen Missbrauch" gesprochen werden - jedenfalls solange die entsprechende Nutzungsrechte-Einräumung in den AGB wirksam vereinbart wurde. Gleichwohl ist die meist sehr umfangreiche Verwertung den wenigsten Nutzern bewusst, da AGB entweder gar nicht gelesen werden oder aber so geschrieben sind, dass die Brisanz nicht klar zum Ausdruck kommt. Eine unerwünschte Verwertung liegt bspw. oft vor, wenn Daten an beliebige Dritte zu beliebigen Zwecken verkauft werden können, wobei solche AGB oft so formuliert sind, dass dies nicht offenbar wird. („... dürfen wir Ihre Daten auch an unsere Kooperationspartner übermitteln, soweit dies der Erbringung, Förderung, Finanzierung und Verbesserung unseres Angebots dient. Alle Kooperationspartner werden von uns angewiesen ...").

Daneben sind auch Fälle echten Missbrauchs denkbar, d.h. eine Datenverwendung außerhalb der AGB des Webdienstes. Bekannt sind Fälle, bei denen ein finanziell notleidender Dienst Daten verkauft, um einer drohenden Insolvenz zu entgehen, oder Fälle, in denen Mitarbeiter des Dienstes umfangreich Daten entwenden.

2.7.2 Datenmissbrauch durch Dritte

Häufig werden Daten auch von Dritten ausgelesen und verwertet, etwa von Hackern. Dabei werden insbesondere Kontodaten von Nutzern und solche, mit denen finanzielle Transaktionen ausgelöst werden können, zum Missbrauch gehackt, d.h. nicht nur, um bspw. eine schwache Sicherheit des Dienstes nachzuweisen. Daneben kommt ein Missbrauch zufällig zugänglicher Daten in Betracht, bspw. wenn ein Nutzer aufgrund diverser Schwachstellen Zugriff auf andere Accounts bekommt. So sind Fälle bekannt, bei denen Dropbox-Accounts über mehrere Stunden frei zugänglich oder Skype-Konten für andere angemeldete Nutzer leicht angreifbar waren.

2.7.3 Datenzugriff durch Nachrichtendienste und Sicherheitsbehörden

Neben Hackern können auch andere Unternehmen oder Konkurrenten, bspw. angebliche Rechteinhaber, aufgrund behördlicher oder gerichtlicher Entscheidungen legal Zugriff auf Daten bekommen, die bei einem Webdienst gespeichert sind. Dies ist zwar grds. auch nach deutschem Recht möglich, bspw. nach einem klagestattgebenden Urteil, jedoch sind die Zugriffsrechte im Ausland größtenteils unbekannt und teils deutlich weiter als nach deutschem Recht. Daher sind Zugriffe auf Daten bei einem Webdienst möglich, die nach deutschem Recht so nicht vorstellbar sind.

Letztlich können auch Behörden und Sicherheitsdienste selbst umfangreich in Daten bei einem Webdienst einsehen. Das Management von Microsoft UK hat bspw. ausdrücklich eingeräumt, dass aufgrund des Patriot Act auch Datenzugriffe durch US-Dienste auf Daten Europäischer MS-

Rechenzentren möglich sind. Manche Sicherheitsbehörden verfolgen zudem das offizielle Ziel der Wirtschaftsspionage. In aller Regel werden die Betroffenen über solche Datenzugriffe nicht informiert.

2.8 Benutzungsfehler

Ein intransparentes User Interface kann zu Fehlbedienungen führen:

- Versehentliches Offenbaren, Kopieren, Ändern oder Löschen von Informationen

Insbesondere neue und noch unbekannte Webdienste müssen von den Nutzern erst verstanden werden. Dabei sind Webdienste aufgrund ihres Interesses, möglichst viele Daten zu erhalten, oftmals per Default so eingestellt, dass ggf. unabsichtlich mehr Daten offenbart werden, als unbedingt notwendig.

Zu denken ist bspw. an Peer-to-Peer Funktionen, bei denen ganze Nutzerverzeichnisse automatisch freigegeben und zudem mit Daten des Endgeräts gefüllt werden, ohne dass dies einem Nutzer ausdrücklich bewusst wird. Oder aber an Freunde-Suchfunktionen in Sozialen Netzwerken wie Facebook, mit denen automatisch Kontaktdaten aus E-Mail-Clients ausgelesen werden. Teilweise sind Buttons so angeordnet, dass eine Fehlfunktion geradezu provoziert wird, etwa bestimmte Upload-Buttons zur Nutzung eines Cloud-Speichers. Umgekehrt sind häufig die Menüs und Buttons zum Löschen von publizierten Inhalten oder Accounts versteckt.

2.9 Mangelnde Daten- und Diensteverfügbarkeit

Eine Verfügbarkeit von Webdienst und Daten ist nicht sichergestellt:

- Möglichkeit zum jederzeitigen und unangekündigten Einstellen durch den Dienst
- Dienst wird aufgrund externer Vorgaben abgeschaltet
- Keine SLA/ keine Gewährleistung
- Kein Backup

Da die meisten Webdienste kostenlos sind, gewähren sie keine festen Verfügbarkeiten und Service Level. Die Gewährleistung ist wie die Haftung ausgeschlossen.

Zudem werden die meisten Dienste von wiederum weiteren Anbietern betrieben bzw. auf deren Infrastruktur gehostet, z.B. bei Amazon, aber auch bei kleineren Anbietern. Selbst bei Amazon kommt es immer wieder zu Downzeiten mit irreversiblen Datenverlusten. Auch bei T-Mobile USA/Sidekick gab es 2009 einen einwöchigen Ausfall mit unwiderruflichen Datenverlusten. Oder bei den über Megaupload gehostetet und für Kunden ggf. nicht nachvollziehbar weiterverlagerten Daten, deren Löschung von Subunternehmern aufgrund der drohenden Insolvenz von Megaupload gewünscht wird, ist mit unvorhersehbaren und endgültigen Datenverlusten zu rechnen. Im Unterscheid zu einem klassischen Outsourcing, bei dem der Nutzer alle Rechte entlang einer Kette von Dienstleistern vertraglich abgesichert und bei Nichteinhaltung einen finanziell durchsetzbaren (da versicherten) Ersatzanspruch bekommt, ist bei Webdiensten schon oft nicht einmal nachvollziehbar, wo Daten gespeichert und an wen sie in der Kette weiter verlagert werden.

Dazu kommt, dass manche Dienste selbst noch nicht wissen, in wie weit ihr Geschäftsmodell legal ist oder sich finanziell trägt. Da sie mit kurzfristigen Untersagungsverfügungen von Konkurrenten oder Behörden rechnen müssen, behalten sie sich das Recht vor, einen Dienst jederzeit unangekündigt einstellen zu können.

2.10 Datenleichen und Datenzombies

Nutzerkonten geraten in Vergessenheit oder lassen sich nicht endgültig löschen:

- Keine oder nur komplizierte Möglichkeit zum (vollständigen) Löschen
- Account wird von anderem Dienst gekauft/ übernommen
- Accounts und Zugangsdaten werden vergessen, Mitarbeiterfluktuation
- Die Nutzung läuft aus, ohne dass eine Abmeldung erfolgt
- Eine Nutzung durch Dritte findet noch statt (etwa Kommentierung von Beiträgen)

Das erläuterte Einräumen von Nutzungsrechten an einen Webdienst kann dazu führen, dass derjenige, der Dateien und Informationen an einen Webdienst übermittelt, sein Recht verliert, eingestellte Dateien zu entfernen. Dies gilt v.a. bezüglich Medieninhalten oder textuellen Threads in Blogsystemen. Diese bleiben bestehen, auch wenn sich ein Nutzer vom Dienst abmeldet und seinen Account löscht. Insofern ist bereits keine vollständige Möglichkeit mehr zum Löschen vorgesehen.

Weiterhin können Webdienste von anderen Diensten gekauft werden. Bspw. wurden in der Vergangenheit bestimmte Jobportale von Konkurrenten übernommen, welche die Nutzer zwar informierten, im Übrigen aber alle Accounts erst einmal übernahmen. Größere Webdienste sehen in ihren AGB sogar regelmäßig explizit vor, dass der Nutzer das Recht einräumt, dass sein Account im Falle eines Kaufs des Webdienstes vom Käufer übernommen werden darf. Andernfalls wären diese Daten für den Webdienst gegenüber Investoren nicht mehr werthaltig.

Darüber hinaus können Accounts auch einfach auslaufen, bspw. wenn ein Webdienst an Renommee verliert und mit der Zeit einfach nicht weiter genutzt wird oder aber, wenn Mitarbeiter ausscheiden und Nachfolger andere Dienste oder eigene Accounts verwenden. Da das Löschen oft umständlich ist, gerät der Account in Vergessenheit und entfaltet ggf. ein Eigenleben, bspw. wenn ein untergehender Dienst von einem Konkurrenten übernommen wird.

Letztlich bleiben trotz einer Löschung ganze Accounts häufig jahrelang in Backup-System der Betreiber und deren Subunternehmer.

2.11 Probleme bei der Rechtsdurchsetzung

Gegenüber einem Webdienst sind üblicherweise bestehende Rechte kaum durchsetzbar:

- Keine nachvollziehbaren Vereinbarungen
- Dienste und dahinter stehende Eigentümer sind unbekannt
- Betreiber und andere kooperierende Dienstleister sind unbekannt
- Kein Impressum, daher keine ladungsfähige Anschrift (Klage nicht einmal zustellbar)
- Die finanzielle Ausstattung des Anbieters ist unbekannt
- Hoher und unkalkulierbarer Aufwand der Rechtsverfolgung im Ausland
- Unklare Rechtslage bei internationalen Anbietern, viele betroffene Rechtsordnungen

2.11.1 Keine nachvollziehbaren Vereinbarungen mit dem Webdienst

Die Nutzung von Webdiensten erfolgt in aller Regel dadurch, dass sich der Benutzer beim Dienst registriert und im Rahmen des Registrierungsprozesses den vorgegebenen Nutzungsbedingungen (AGB) und Datenschutzhinweisen zustimmt bzw. deren Kenntnisnahme bestätigt. Zwar sieht das Europäische Telemedienrecht vor, dass die Nutzungsbedingungen und Datenschutzhinweise in abspeicherbarer Form zur Verfügung gestellt werden müssen, jedoch gilt dies nicht automatisch auch für außereuropäische Dienste. Zudem wird die Speichermöglichkeit oftmals nicht wahrgenom-

men und wenn, fehlen Signaturen und Zeitstempel für einen später sicheren Nachweis der Integrität. Da sich Webdienste in der Regel auch vorbehalten, die Nutzungsbedingungen und Datenschutzhinweise anzupassen, kann es im Streitfall zu der Situation kommen, dass nicht nachvollziehbar ist, auf welcher Grundlage die Nutzung eines Dienstes vereinbart wurde. Darüber hinaus ist es für einen Anspruchsteller schwer nachzuweisen, welche Version eines Regelwerks zu welchem Zeitpunkt gegolten hat und wie diese vereinbart wurde. Insofern besteht die Gefahr, dass Regelungen wie Nutzungsbedingungen und Datenschutzhinweise faktisch leer laufen. Dies gilt zwar auch soweit, als den Nutzer benachteiligende Regelungen entfallen (z.B. das Einräumen bestimmter Nutzungsrechte, wobei dann aber aufgrund einer gesetzlichen Auffangregelung jedenfalls soweit Nutzungsrechte eingeräumt werden, wie der Dienst zur Erbringung seiner Services unbedingt braucht), jedoch führt die daraus resultierende Rechtsunsicherheit dazu, dass Ansprüche gegen einen Webdienst praktisch nur sehr schwer und mit unvorhersehbarem Ergebnis verfolgt werden können.

2.11.2 Beeinträchtigungen durch Regelungen fremder Rechtsordnungen

Soweit Webdienste ihren Sitz nicht in Deutschland haben ist weiterhin zu beachten, dass diese aufgrund der gesetzlichen Regelungen in ihren Ländern zu Datenweitergaben verpflichtet sein können, die von der bekannten Rechtslage in Deutschland abweichen. Beispielsweise können umfangreiche Zugriffsmöglichkeiten für Konkurrenten nach ausländischem Recht bestehen. Weiterhin stehen behördlichen Institutionen in den USA, Russland oder in bestimmten asiatischen Staaten weitgehende Zugriffsrechte auf Daten eines Webdienstes zu, auf die die Webdienste nicht gerne hinweisen. Kommt es zu einem Zugriff, werden die Betroffenen nicht informiert, d.h. oftmals besteht nur ein nicht verifizierbarer Verdacht, dass Daten abgegriffen wurden.

2.11.3 Probleme bei der Durchsetzung von Ansprüchen

Über die Problematik hinaus, ob Regelungen mit einem Webdienst wirksam vereinbarten wurden und welche Version eines Regelwerkes gilt, sind die enthaltenen Ansprüche selbst bei klarer Sachlage gegenüber vielen Webdiensten nur schwer durchsetzbar. Die Gründe dafür sind

- eine Intransparenz, wer als Eigentümer hinter einem Dienst steht,
- eine oftmals nur geringe finanzielle Ausstattung des Anbieters,
- ein Firmensitz im (außereuropäischen) Ausland,
- Unklarheiten bezüglich der anzuwendenden Rechtsordnung.

Sofern nicht bekannt ist, wer hinter einem Dienst steht, fällt es schwer, gerichtliche Hilfe in Anspruch zu nehmen. Nach deutschem Recht ist bspw. eine „ladungsfähige Anschrift" Voraussetzung für die Zustellung einer Klage. Eine öffentliche Zustellung kommt nur selten in Betracht.

Weiterhin belegen bspw. die Streitigkeiten zwischen Google und bestimmten Aufsichtsbehörden, dass selbst staatliche Institutionen kaum eine Möglichkeit haben, geltendes gesetzliches Recht gegenüber einem außereuropäischen Webdienst durchzusetzen. Praktisch besteht somit die Situation, dass Ansprüche gegenüber vielen Webdiensten nicht durchsetzbar sind.

Vor Nutzung eines Webdienstes ist daher kritisch zu hinterfragen, ob beispielsweise im Falle von Datenverlusten, -beschädigungen oder Vertraulichkeitsverletzungen auf Haftungs- oder Richtigstellungsansprüche vollständig verzichtet werden kann. Zudem ist zu recherchieren, wo ein Webdienst seinen Firmensitz hat und wer finanziell hinter dem Webdienst steht.

3 Maßnahmen

Zur Vermeidung bzw. Begrenzung der genannten Risiken eines Webdienstes können insbesondere folgende Maßnahmen ergriffen werden.

3.1 Prüfung der Zulässigkeit - Einverständnis

Eine unzulässige Nutzung kann vermieden werden, wenn alle Verträge und AGB gelesen und geprüft werden. Bei Unzulässigkeit und im Zweifelsfall gilt:

- **1) Alle Unternehmen sollten ihre Zustimmung erteilen:**
  - Ist die Webdienstenutzung unzulässig, bedarf es einer Vertragsänderung
  - Daher Zustimmung durch alle Vertragspartner-Unternehmen (Projektpartner, Auftraggeber)
  - Im Voraus und nachvollziehbar (mindestens Textform, d.h. E-Mail)
  - Durch nachweislich bevollmächtigte Mitarbeiter der Unternehmen
  - Ggf. konkludente Zustimmung durch aktive Nutzung bevollmächtigter Mitarbeiter

  und ggf. zusätzlich

- **2) bei Übermittlung/Verarbeitung personenbezogener Daten (Regelfall):**
  - Zusätzlich Datenschutz-Einwilligung aller betroffenen Mitarbeiter
  - Im Voraus und grds. handschriftlich (ausnahmsweise in Textform wenn Authentizität sichergestellt ist, d.h. per E-Mail und bei Unbekannten mit Double-Opt-In)
  - Durch betroffene Mitarbeiter individuell und für sich persönlich
  - Ausdrückliche Einwilligung ist vorgeschrieben, ausnahmsweise konkludent bei Anhaltspunkten für schlüssiges Einwilligen
  - Alternativ: Datenschutzrelevante Betriebsvereinbarung

Zur Vermeidung von Vertragsverstößen sind Verträge mit Projektpartnern/Auftraggebern (Auftrag, Konsortialvertrag etc.) und die AGB des Webdienstes durchzusehen, ob die Dienstenutzung im vorliegenden Fall eventuell unzulässig ist (s. Ziffer 2.1). Dabei sollte man sich des Risikos bewusst sein, dass eine unzulässige Nutzung eines Webdienstes einen Vertragsverstoß darstellen kann, weswegen derjenige, der einen Webdienst einsetzt, für alle daraus resultierenden Schäden im Rahmen seiner vertraglichen Haftungsgrenzen einstehen muss (sofern überhaupt Haftungshöchstgrenzen vorhanden sind, das Gesetz sieht solche per se nicht vor). Dies gilt grundsätzlich auch für Schäden, die bspw. aus einer unsicheren Dienstegestaltung oder aus Angriffen Dritter resultieren, also laienhaft als „unverschuldet" empfunden werden. Denn hätte sich die betreffende Partei an den Vertrag gehalten und keinen Webdienst eingesetzt, wäre es nicht zum Schaden gekommen.

Kommt die Prüfung zu dem Ergebnis, dass eine Webdienste-Nutzung unzulässig ist oder bestehen darüber Zweifel, so muss vor der Verwendung eine Zustimmung von den beteiligten Unternehmen eingeholt werden.

Daneben sollte zur Vermeidung von Datenschutzverstößen eine datenschutzrechtliche Einwilligung der betroffenen Mitarbeiter eingeholt werden, sofern personenbezogene Daten an den Webdienst übermittelt werden. Die Einholung sollte zumindest bei wichtigen Daten (insbesondere Inhalte interner, nicht zur Veröffentlichung bestimmter Dokumente) in schriftlicher Form – wenigstens per E-Mail – erfolgen und dokumentiert werden.

3.1.1 Zustimmung der Vertragspartner

Durch eine Zustimmung zur Nutzung von Webdiensten wird z.B. sichergestellt, dass nicht gegen vertragliche Vereinbarungen wie bspw. Vertraulichkeitsregelungen verstoßen wird.

Da eine Zustimmung in diesen Fällen eine Vertragsänderung ist, sind mögliche Formerfordernisse für Vertragsänderungen zu berücksichtigen, die sich aus dem Vertrag ergeben. Häufig fordert ein Vertrag für alle Änderungen die Schriftform.

Die Zustimmung ist vor Beginn der Nutzung durch einen bevollmächtigten Vertreter mit Wirkung für das repräsentierte Unternehmen einzuholen. Wer bevollmächtigt ist, ist häufig im Projektvertrag geregelt („Der Ansprechpartner XY darf im Rahmen der Kooperation verbindliche Erklärungen abgeben…"). Bei kleineren Unternehmen, bei denen vertretungsberechtigte Geschäftsführer im Projekt sind, kann teilweise über www.handelsregister.de abgefragt werden, wer wie bevollmächtigt ist. Die Zustimmung sollte zur Ermöglichung eines späteren Nachweises nachvollziehbar abgegeben werden, d.h. schriftlich, wenigstens per E-Mail.

Die Zustimmung eines Unternehmens kann grds. auch konkludent (d.h. schlüssig) in der aktiven Nutzung eines Dienstes durch bevollmächtige Mitarbeiter liegen. Da die Bevollmächtigung aber häufig unklar oder nicht vorhanden sein wird, sollte eine förmliche und ausdrückliche Zustimmung eines Bevollmächtigten eingeholt werden.

3.1.2 Datenschutzrechtliche Einwilligung der betroffenen Mitarbeiter

Da bei der Webdienste-Nutzung in der Regel personenbezogene Daten der eigenen Mitarbeiter oder Mitarbeiter der Vertragspartner übermittelt werden (z.B. E-Mail-Adressen, Namen in Dokumenten, Präsentationen etc.) bedarf es neben der Zustimmung des Unternehmens auch einer datenschutzrechtlichen Rechtsgrundlage für die betroffenen Mitarbeiter. Diese kann v.a. in einer individuellen Einwilligung der Mitarbeiter oder einer Betriebsvereinbarung liegen, welche auf die Webdienste-Nutzung anwendbar ist. Sofern dagegen ausnahmsweise keine personenbezogenen Daten an den Webdienst übermittelt werden, bedarf es auch keiner datenschutzrechtlichen Rechtsgrundlage. Dies kann bspw. der Fall sein, wenn an einen Terminfindungsdienst nur die Initialen eines Adressaten gegeben werden und der Link zur Abstimmung vom Initiator selbst über seinen Mail-Client versendet wird (s. das Bsp. bei den Risiken unter Ziff. 2.1.3 - Datenschutz)

Durch eine vorherige Einwilligung der Mitarbeiter wird sichergestellt, dass nicht gegen deren Recht auf informationelle Selbstbestimmung verstoßen wird.

Anders als bei normalen vertraglichen Erklärungen, wie etwa der Zustimmung des Unternehmens, muss eine datenschutzrechtliche Einwilligung zum Schutz der Betroffenen **grds. schriftlich** und ausdrücklich abgegeben werden (absichtliche Hürde, sog. „Warnfunktion").

Ausnahmsweise kann eine **konkludente Einwilligung** genügen. Besonders einfach ist der Fall, wenn z.B. vorab über eine geplante Webdienste-Nutzung informiert wurde und in Kenntnis dieser Information eine bewusste Nutzung erfolgt, bspw. wenn ein Betroffener seine Daten selbst bei einem Webdienst einstellt. Überträgt ein Betroffener seine Daten nicht selbst an einen Webdienst, sondern geschieht dies durch einen anderen, der sich auf die konkludente Einwilligung des Betroffenen berufen muss, so kann es später zu Schwierigkeiten beim Nachweis der konkludenten Einwilligung kommen.

In keinem Fall genügt schlichtes Nichtstun, d.h. eine nur unterstellte Einwilligung. D.h. es ist nicht ausreichend, wenn ein Betroffener über eine beabsichtigte Publikation informiert wird und dazu nur schweigt. Wenigstens müsste er sich am Dienst beteiligen, dass ein Anknüpfungspunkt für eine konkludente Zustimmung besteht.

Alternativ zu individuellen Einwilligungen kann eine Betriebsvereinbarung, die sich auf die Übermittlung personenbezogener Daten an Webdienste bezieht, eine legitimierende Rechtsgrundlage darstellen. Nach derzeitiger Situation in vielen Unternehmen, welche erst langsam Betriebsvereinba-

rungen für die Webdienstenutzung abschließen, bestehen wohl nur selten Betriebsvereinbarungen, die individuelle Einwilligungen ersetzen.

3.2 Bewertung und Begrenzung von Schadensrisiken

Schadensrisiken müssen erkannt, Risiken und Folgen begrenzt werden:

- Die Eintrittswahrscheinlichkeit eines Risikos ist zu prüfen bzw. schätzen
- Sicherheitsvorfälle in der Vergangenheit sollten recherchiert werden
- Bspw. über Suchmaschinen und in den Foren eines Webdienstes
- Die mögliche Schadenshöhe ist kritisch zu prüfen („was, wenn Daten öfftl. werden?“)
- Missbrauchsmöglichkeiten sollten begrenzt werden (s. alle Maßnahmen der Ziffer 3)
- Die Schadenshöhe sollte begrenzt werden
- Grds.: es sollten keine sensiblen Daten an einen Webdienst übermittelt werden

3.2.1 Bewertung von Schadensrisiken

Vor der Verwendung von Webdiensten sollte im jeweiligen Projektkontext bewertet werden, welche Ausmaße eine Offenbarung, Manipulation oder der Verlust von Daten verursachen würde, insbesondere von Forschungsinhalten. Hierbei sollten Faktoren wie Geheimhaltung, Verschlüsselung, Sitz des Anbieters und Betreibers, bestehende Verträge, Ruf des Anbieters etc. mit einbezogen werden. Sicherheitsvorfälle beim Dienst sollten recherchiert werden, bspw. über Suchmaschinen oder eine Durchsicht (Dienste-eigener) Support-Foren.

3.2.2 Begrenzung: grundsätzlich keine Übermittlung sensibler Informationen

Besonders vertrauliche Daten sollten auch bei vorhandener Verschlüsselung grundsätzlich nicht in die Systeme von Webdiensten eingebracht werden, da die angewendeten Verfahren oft nur einige Jahre sicher vor Versuchen zum Brechen der Schlüssel sind und weil bei ihrer Anwendung Fehler vorkommen. Bei Unklarheiten sollte mit dem Projektleiter oder Vorgesetzten Rücksprache gehalten werden.

Inhalte, die eventuell einer späteren Patentanmeldung dienen sollen, sollten ebenfalls generell von einer Übermittlung an Webdienste ausgenommen werden. Allenfalls könnten Inhalte, die über bestimmte Tools Ende-zu-Ende verschlüsselt wurden (z.B. mittels Truecrypt bei ausreichender Schlüssellänge), mit vertretbarem Risiko sicher übermittelt werden.

3.3 Bewertung des Anbieter und Angebot

Risiken eines Webdienstes sind erkennbar, wenn Anbieter und Betreiber geprüft werden:

- Recherchen in Suchmaschinen, Support-Foren, Newslettern
- In Betracht kommen auch Bonitätsauskünfte oder Einsicht in das Handelsregister
- Optional können spezifische Tests in einem IT-Sicherheitslabor durchgeführt werden

3.3.1 Bewertung von Anbieter und Betreiber

Anbieter eines Webdienstes ist derjenige, in dessen Verantwortung ein Webdienst betrieben wird und der grds. Zugriff auf alle übermittelten Daten hat. Typischerweise wird der Anbieter im Impressum einer Webseite genannt.

Der Anbieter ist aber meist nicht identisch mit dem Betreiber. Als Betreiber ist in diesem Zusammenhang derjenige zu sehen, auf dessen Servern und Infrastruktur ein Dienst gehostet wird, z.B. Amazon, aber auch kleinere Hosting-Provider. Teilweise verlagern Betreiber bestimmte Services

wiederum weiter an andere Unterauftragnehmer. Ohne besondere Verschlüsselung hat auch der Betreiber Zugriff auf die Daten des Webdienstes.

Sowohl Anbieter als auch Betreiber sind damit für die Sicherheit eines Webdienstes entscheidend. Sofern der bzw. die Betreiber recherchiert werden können, sind auch sie zu überprüfen.

Eine einfache Prüfung kann dadurch erfolgen, dass über Suchmaschinen und entsprechende Suchbegriffe, bspw. „Anbieter XY" „Sicherheit" „Datenschutz" o.ä. recherchiert wird. Weiterhin können IP-Adressen der Dienste-Seiten aufgelöst werden. Auch Support-Foren können Hinweise auf Sicherheitsmängel und ggf. Patches enthalten. Zudem empfiehlt sich das regelmäßige Studium IT-relevanter Newsletter, bspw. des Heise.de-Verlags.

Neben diesen einfachen Recherche-Möglichkeiten bieten sich in wichtigen Fällen auch Recherchen zu den Eigentümern oder der Bonität der Anbieter und Betreiber an. So können Auskünfte bei bspw. der Creditreform oder Handelsregistereintragungen bei deutschen Unternehmen unter www.handelregister.de abgefragt werden.

3.3.2 Bevorzugung von Anbietern und Betreibern mit Sitz in Deutschland, EU/EWG

Zur leichteren Rechtsdurchsetzung sind Anbieter und Betreiber mit Sitz in Deutschland, mindestens aber der EU/EWG zu bevorzugen. In der Regel bestehen eine weitgehende Harmonisierung des Rechts in der EU/EWG oder wenigstens ein einheitliches Mindestniveau.

3.3.3 Bevorzugung renommierter Anbieter und Betreiber

Zur Vermeidung von Image-Schäden sollten in einem professionellen Umfeld ebenso professionelle und renommierte Anbieter genutzt werden. Bei diesen steht aufgrund des finanziellen Engagements ihrer Eigentümer/Investoren zu erwarten, dass zumindest keine offensichtlichen/öffentlich bekannten oder besonders krassen Sicherheitsmängel bestehen und bestehen bleiben, deren Bekanntwerden ihr Geschäft negativ beeinflussen würden. Tendenziell werden erkannte Mängel in einem solchen Umfeld - wenngleich teils intransparent - beseitigt. Kleinere und am Markt neue Anbieter sind dagegen eher innovativ und v.a. mit der Realisierung und Herstellung der Funktionsfähigkeit sowie der Finanzierung ihrer Innovation betraut als mit der (kostenintensiven) Umsetzung oder Zertifizierung von Sicherheits-Standards. Zudem fehlt es oftmals an grundlegenden betriebswirtschaftlichen und rechtlichen Kenntnissen. Dies ist anders bei zertifizierten Anbietern oder Betreibern, z.B. nach ISO/IEC 27001; einem ULD-Datenschutz-Gütesiegel oder ggf. einem (künftigen) Cloud-Zertifikat gem. BSI). Ganz allgemein sollten letztlich Dienste bevorzugt werden, die in ihrem Erscheinungsbild seriös und möglichst nachvollziehbar Wert auf IT-Sicherheit und Vertraulichkeit legen.

3.3.4 Optional: Vertiefende technische Prüfung in einem Sicherheitslabor

Soll ein Webdienst in größerem Umfang genutzt werden, bei wirtschaftlich sehr bedeutenden Auslagerungen oder erheblichen Risiken, sollte der Dienst bzw. dessen Software gegebenenfalls genauer getestet werden. Dazu können technische Sicherheitstests in einem Labor durchgeführt werden.

3.4 Bewertung von Nutzungsbedingungen und Datenschutzerklärung

Risiken eines Webdienstes sind erkennbar, wenn AGB und Datenschutzhinweise gelesen werden. Insbesondere sollten folgende Regelungen nicht enthalten sein:

- Jederzeitige, unangekündigte Einstellungs- bzw. Kündigungsmöglichkeit
- Ausschluss jeglicher Haftung und Gewährleistung
- Keine definierte Verfügbarkeit, keine Backups
- Nutzungsrechtseinräumung zu unbekannten/vagen Zwecken und für Dritte
- Mögliche Weitergabe von Daten an Dritte
- Fingierte Erklärungen des Nutzers, Verzicht auf bestimmte Rechte

Die Nutzungsbedingungen eines Dienstes sind auf bestimmte, nachteilige Regelungen zu prüfen. In Betracht kommt bspw., ob sich der Dienst ein jederzeitiges, grundloses Kündigungsrecht vorbehält und ob er vor einer Kündigung oder Einstellung des Angebots informieren muss. Ebenso werden häufig umfangreiche Nutzungsrechte an den Dienst übertragen, welche z.T. auch nach einer Beendigung der Nutzung oder Löschung des Accounts fortbestehen. Faktisch ist damit eine vollständige Löschung nicht mehr möglich. Typischerweise schließt ein Webdienst auch jegliche Gewährleistung und Haftung aus, d.h. es besteht auch keine verlässliche Verfügbarkeit. Es ist schon öfters vorgekommen, dass auch bei größeren Webdiensten nach Verfügbarkeitsbeschränkungen mangels Backup unwiderrufliche Datenverluste eingetreten sind. Letztlich werden häufig Erklärungen der Nutzer fingiert (bspw. „Der Nutzer stimmt zu, dass …" oder „Durch die Nutzung erkennt der Nutzer an, dass…").

Um die Funktion eines Webdienstes und die Rechtslage zu verstehen, ist die Durchsicht der vollständigen AGB und Datenschutzerklärung unabdingbar. Sie ist in der Regel in wenigen Minuten möglich. Bei größeren Webdiensten, die im Fokus der Öffentlichkeit stehen, ist wegen des sie betreffenden und auch im Ausland bestehenden Abmahnrisikos zudem davon auszugehen, dass die AGB und Datenschutzerklärung im Großen und Ganzen die tatsächliche Datenverwendung zutreffend wiedergeben. Bei unklaren Regelungen sind zudem Nachfragen beim Dienst angebracht. Seriöse Dienste antworten.

3.5 Suche nach Alternativen, eigene Dienste

Bei nicht tragbaren Risiken sind alternative Dienste zu suchen:

- Bevorzugt eigene Dienste
- Andere externe Webdienste, am besten renommierte und vorab geprüfte

3.5.1 Eigene Angebote bevorzugt nutzen und ausbauen

Vor der Verwendung eines Webdienstes sollte immer überprüft werden, ob nicht ein unternehmenseigener Dienst die gewünschte Funktionalität ausreichend zur Verfügung stellt. Dass solche eigenen Dienste möglicherweise etwas umständlicher zu nutzen sind, rechtfertigt nicht das Eingehen unbekannter Risiken und von Vertrags- oder Rechtsbrüchen durch irgendwelche Webdienste.

3.5.2 Angebote von Partnern nutzen

Stehen eigene Angebote nicht zur Verfügung, so hat doch mitunter der Projektpartner eine Alternative zu dem Webdienst. Ein vom Partner betriebener Sharepoint-Service kann bspw. eine Alternative zur Speicherung im Netz sein.

Eine weitere Alternative sind Angebote von wissenschaftlichen Einrichtungen. So bietet der DFN-Verein einen Terminplaner und im Verbund mit Universitäten einen Dienst zum Austausch großer Dateien.

3.5.3 Angebotsbewertung und Auswahlhilfen

Sofern keine eigenen Dienste oder Partnerangebote bestehen, sollten solche bevorzugt werden, die bereits geprüft bzw. grob vorab bewertet wurden.

Kriterien für eine solche zentrale Bewertung sind u.a. auch der Standort Deutschland bzw. die EU/EWG, Anbieterseriosität und Dauerhaftigkeit des Angebots und vorliegende nachgewiesene Sicherheitsbewertungen oder Datenschutzaudits (z.B. ISO 27001, ULD Datenschutz-Gütesiegel; ggf. auch künftig durch ein geplantes BSI „Cloud-Zertifikat", das in weiten Teilen auch für Webdienste relevant sein kann).

3.5.4 Handlungshilfe und Differenzierung falls keine Alternativen bestehen

Sofern weder eigene Dienste noch Partnerangebote bestehen (3.5.1 und 3.5.2) und auch keine Prüfung und Bewertung stattgefunden hat (3.5.3), kann für die Zulässigkeit der Nutzung eines Webdienstes grob nach folgendem Schema bewertet werden (Hinweis: diese nur grobe Differenzierung ersetzt nicht die übrigen Prüfungspunkte und Maßnahmen des gesamten Kapitels 3).

Auslagerung grundlegender Geschäftsprozesse und Datensammlungen

Daten aus grundlegenden internen Geschäftsprozessen wie bspw. HR-Daten, Buchhaltungsdaten oder große, unstrukturierte Datensammlungen wie Archive oder Backups, in denen alle möglichen unkritischen aber auch sensiblen Daten enthalten sein können, dürfen nur auf eigenen Servern bzw. in einer (künftigen) eigenen und privaten Cloud-Umgebung gespeichert werden. Denn eine Übermittlung und/oder Speicherung solcher Daten bei einem externen Webdienst kann in unvorhersehbarer Weise gegen alle möglichen vertraglichen Vorschriften mit Auftraggebern (z.B. NDA) oder gegen Gesetze (z.B. Exportkontrolle, Datenschutz, Mitbestimmung etc.) verstoßen und ebenso unvorhersehbare Folgen verursachen (z.B. Vertragsstrafen, Bußgelder, Unterlassungs- und Löschungsanordnungen, Ausschluss bei öffentlichen Ausschreibungen etc.). Der Begriff eigener Server meint dabei nicht unbedingt im Eigentum stehend, sondern ggf. auch eine Speicherung auf gemieteten/geleasten Servern bei einem sicheren, zertifizierten Rechenzentrum, in dem der Server hardwareseitig ausschließlich unter eigener Kontrolle steht, d.h. nicht nur virtuell zugeordnet wird (z.B. eigener, gesicherter Bereich in einem ISO 27001 RZ, Zugangsschutz).

Auslagerung von Inhaltsdaten und Arbeitsergebnissen

Arbeitsdokumente wie bspw. Projektberichte oder wissenschaftliche Ergebnisse können in der Regel dann ohne Weiteres an einen externen Webdienst übermittelt und dort bspw. zur Bearbeitung oder Freigabe an andere Nutzer zwischengespeichert werden, wenn (i) die „eigentliche Speicherung" nach wie vor beim Nutzer erfolgt und dort den üblichen Sicherungsmaßnahmen wie Backup etc. unterliegt und (ii) mit dem Webdienst eine schriftliche Auftragsdatenverarbeitungs-Vereinbarung in Papierform abgeschlossen ist (absichtliche Hürde der Warnfunktion) oder alle Beteiligten in die Nutzung nachvollziehbar eingewilligt haben. Immer mehr renommierte Webdienste gehen dazu über, solch schriftlichen Vereinbarungen anzubieten, welche dem Nutzer Aufschluss über die Datenverarbeitung geben und ihm bestimmte Kontrollrechte einräumen bzw. umgekehrt den Anbieter zur Vorlage regelmäßiger externer Prüfberichte verpflichten (z.B. Google bei manchen Diensten, MS bei MS365, Wired Minds etc.).

Sind diese beiden vorstehenden grundsätzlichen Kriterium erfüllt, ist lediglich zu prüfen, ob ausnahmsweise Gründe vorliegen, die einer Nutzung des externen Webdienstes dennoch widersprechen. Beispielsweise könnte es sich im Einzelfall um besonders sensible Daten handeln, um Informationen im Zusammenhang mit einer künftigen Patentanmeldung, um Informationen oder verschlüsselte Daten, deren Zugänglichmachung in bestimmten Ländern oder gegenüber Nutzern mitbe-

stimmten Staatsangehörigkeiten der Exportkontrolle unterliegen, bspw. im Bereich der Kernenergie (auch nicht überall dürfen Daten sicher verschlüsselt werden) oder es könnten vertragliche Verbote mit Auftraggebern oder Kooperationspartnern bestehen, welche den Einsatz eines externen Webdienstes untersagen (zu möglichen Verboten s. Kapitel 2.1).

Dienste mit geringem Schadenspotential

Sofern im Grunde genommen gar keine sensiblen oder besonders datenschutzrelevanten Daten an einen Webdienst übermittelt werden sollen und dieser keine technischen Schwachstellen aufweist, keine Installation kritischer Software erfordert und keine niedrigen Browser-Sicherheitseinstellungen erzwingt, d.h. insgesamt ein nur sehr geringes Schadenspotential vorliegt, können bekannte Webdienste relativ problemlos genutzt werden. Dies gilt auch, wenn Anbieter und/oder Betreiber im Ausland sitzen, dort den Zugriffsrechten bestimmter Behörden und Einrichtungen unterliegen und ggf., bei Diensten aus den USA, nur dem Safe-Harbor Abkommen beigetreten sind, ohne dass aber darüber hinaus explizite schriftliche Vereinbarungen bestehen oder den Nutzern irgendwelche Gewährleistungsrechte/Verfügbarkeiten zugestanden werden.

In einem solchen Fall sollte insbesondere darauf geachtet werden, dass die Nutzung sicher gestaltet wird. Bspw. sollte die Nutzung möglichst anonym/pseudonym erfolgen (z.B. kann es genügen, bei einem Terminfindungsdienst lediglich die Initialen anzugeben), es sollten Daten Ende-zu-Ende verschlüsselt werden (z.B. über Truecrypt), es sollte eine gesicherte SSL-Datenübertragung aktiviert werden und es sollten alle Beteiligten der Nutzung wenigstens schlüssig zustimmen.

3.6 Verbot oder Reglementierung der Dienstenutzung

Riskante Webdienste, die nicht benötigt werden, sollten verboten und die Nutzung möglichst technisch unterbunden werden.

- Erstellung einer Liste riskanter Webdienste
- Regeln vorgeben, welche Webdienste in einem Projekt verwendet werden dürfen
- In Projekten nicht benötigte, riskante Webdienste an Proxy oder Firewall generell sperren

Webdienste, die unsicher sind sollten im jeweiligen Projekt nicht genutzt werden. Dienste, die in Projekten eines Instituts nicht genutzt werden, sollten institutsweit verboten werden. Bei institutsweiten Verboten kann die Nutzung solcher Dienste dann durch Firewallregeln (IP-basiert) oder Webproxies (URL-basiert) unterbunden werden.

Im wissenschaftlichen Umfeld ist es allerdings schwierig, die Nutzung des Internet und von Webdiensten zu beschränken. Reglementierungen werden kaum akzeptiert und häufig gibt es im Einzelfall doch berechtigte Nutzungen. Deshalb werden sich nur einzelne Dienste verbieten lassen, wenn das Gefahrenpotential hoch ist oder Phishing vermutet werden kann. Ein solcher Dienst ist beispielsweise Skymem, mit dem E-Mail-Adressen aus übermittelten Texten extrahiert werden und dann veröffentlicht werden.

Statt eines Komplettverbotes kommt ein Verbot bestimmter kritischer Features in Frage. Verboten werden könnte beispielsweise der Dateiupload in den Terminfindungsdienst Doodle. Solche Verbote lassen sich mit intelligenten Webproxies oder Next Generation Firewalls durchsetzen.

Ist ein Verbot wegen eventueller Ausnahmen schwer umsetzbar, können Warnhinweise durch Webproxies generiert werden.

3.7 Individueller Vertragsschluss und Anbieter-Kontrolle

Wenn möglich, kann bei einer geplanten umfangreichen Nutzung ein individueller Vertrag geschlossen werden:

- Insbesondere bei kostenpflichtigen Angeboten Individualvertrag mit üblichen Rechten
- Audits/ Prüfpflichten entsprechend einem „echtem Outsourcing“

Bei kostenpflichtigen Diensten sind aufgrund der „Einkaufsmacht“ größerer Unternehmen auch normale individualvertragliche Regelungen mit dem Anbieter denkbar. Es ist kommt durchaus vor, dass Anbieter für große Kunden individuelle Verträge abschließen. Dadurch kann bspw. eine bestimmte Gewährleistung und Verfügbarkeit vereinbart werden. Auch State of the Art Regelungen wie bei „normalen“ Outsourcing-Dienstleistern inkl. technischer Leistungs-Spezifi-kationen können getroffen werden. Darin können auch Vereinbarungen über vertragliche Zusicherungen und Schadensersatzansprüche geschlossen werden. Zusätzlich können finanzielle Absicherungen durch Versicherungen vereinbart werden. In solchen Verträge können ferner - wie bei datenschutzrechtlichen Auftragsverarbeitungen ohnehin Standard - Audits oder Kontrollrechte vereinbart werden. In bestimmtem Umfang können diese Kontrollen durch vom Webdienst selbst vorzulegende Prüfberichte oder Zertifikate unabhängiger Dritter ersetzt werden (so bspw. bei bestimmten Webanalyse-Tools).

3.8 Verschlüsselung

Daten, die an einen Webdienst übermittelt werden, sollten verschlüsselt werden:

- Leitungsverschlüsselung und Authentisierung des Dienstes via SSL und HTTPS
- Eigene Ende-zu-Ende Verschlüsselung von Dateien mit sicherem Verfahren

Die Datenkommunikation mit einem Webdienst sollte grundsätzlich mit SSL bzw. HTTPS verschlüsselt erfolgen, damit Lauscher im Internet den Klartext von übertragenen Daten nicht mitlesen können. Zudem sollte es durch den Einsatz von Serverzertifikaten für den Dienstnutzer möglich sein, festzustellen, dass er tatsächlich mit dem Webdienst und nicht etwa mit einem gefakten Server bzw. Phishingserver kommuniziert.

Werden Daten an den Webdienst übermittelt, die unternehmensintern oder gar vertraulich sind, sollten diese vor der Übermittlung an den Webdienst lokal beim Dienstnutzer Ende-zu-Ende verschlüsselt werden. Denn nur so kann verhindert werden, dass der Dienstanbieter oder Hacker die Daten im Klartext lesen können.

Zur Verschlüsselung sollten unbedingt Algorithmen, Schlüssellängen, Betriebsmodi, sowie Programme und Passworte eingesetzt werden, die für den Zeitraum, in dem die Daten vertraulich bleiben müssen, nach dem Stand der Erkenntnisse als sicher betrachtet werden können. Die Verfahren sollten zudem interoperabel, d.h. möglichst auf verschiedenen Betriebssystemen und Hardwareplattformen anwendbar sein, so dass unterschiedliche Anwender sie auch ver- und entschlüsseln können. Zudem müssen verwendete Kennwörter geheim gehalten bzw. über sichere Kanäle ausgetauscht werden.

Leider sind anders als im Bereich qualifizierter Signaturen keine „offiziellen“ Bewertungen von Algorithmen und Parametern sowie Programmen bekannt und auch die Interoperabilität ist fraglich. Daher bleibt den Anwendern bzw. den Unternehmen derzeit nichts anderes übrig, als sich anhand von Veröffentlichungen und Tests ein eigenes Bild zu machen.

Für die Bewertung von Algorithmen kann auf die Erkenntnisse anerkannter Organisationen und Wissenschaftler zurückgegriffen werden, wie:[2]

- Agence nationale de la sécurité des systèmes d'information (ANSSI, englisch: French Network and Information Security Agency, FNISA)
- National Institute of Standards and Technology (NIST)
- European Network of Excellence in Cryptology II (ECRYPT II)
- Empfehlungen von Professor Arjen K. Lenstra.

Demnach sind sichere Verfahren u.a. AES, Blowfish, Twofish, serpent, CAST und RC4. Für gelten nach dem Empfehlungen für 6 Jahre 112 Bit als sicher. Als Betriebsmodus zur Verarbeitung und Verkettung von Blöcken ist dabei CTR zu wählen bzw. eine CBC-Anwendung.

Eine AES-CTR-Implementierung mit 128 Bit wäre demnach nach dem Stand von Wissenschaft und Technik geeignet, Daten für über 6 Jahre sicher zu verschlüsseln.

Neben der Eignung von Algorithmen und Parametern müssen die Verfahren auch sicher implementiert sein. Unabhängige Bewertungen oder gar Zertifizierungen fehlen allerdings für gängige Programme. So bleiben nur aktuelle Recherchen nach Schwachstellen. Aktuell geeignet für Dateiverschlüsselung erscheinen u.a.

- MS Office 2007 sowie 2010
- WINZIP ab Version 9
- 7.Zip ab Version 4.5.7
- OpenPGP-Dateiverschlüsselung mit GPG in der Version 1.4.9 bzw. 2.0.17

Jedes Dateiverschlüsselungsverfahren ist schließlich nur so sicher, wie das zur Verschlüsselung verwendete Geheimnis. Ein schlecht gewähltes Kennwort oder dessen Übermittlung über einen abgehörten Kommunikationsweg hebelt jedes sichere Verfahren aus. Ein sicheres Kennwort für Dateiverschlüsselung sollte mindestens 12 Zeichen, Groß und Kleinbuchstaben, sowie möglichst auch Nummern und Sonderzeichen beinhalten.

3.9 Ergänzende eigene Sicherungsmaßnahmen

Desweiteren sind übliche Maßnahmen der Informationssicherheit zu beachten:

- Aktuelle Updates von Betriebssystem, Browser, BrowserplugIns
- Aktueller Virenschutz, Kein Surfen im Internet mit Administrator-Rechten
- Lokale Backups
- Zugangsdaten bei einem Vertreter hinterlegen
- Restriktive Konfiguration des Webdienstes
- Installationen nur nach Abstimmung mit der IT-Administration

3.9.1 Allgemeine Maßnahmen der Informationssicherheit

Zunächst sind immer übliche eigene Sicherungsmaßnahmen zum Schutz der lokalen Infrastruktur vorzunehmen.

So sind zunächst Betriebssysteme, Webbrowser und seine Plug-Ins aktuell zu halten. Selbstverständlich ist ein üblicher Virenscanner in aktueller Version zu verwenden. Um die Folgen einer Infektion mit Schadcode zu begrenzen, sollte man ferner nicht mit Administrator-Berechtigung im Inter-

[2] Für Auswertungen und Hinweise zu den folgenden Bewertungen danken die Autoren Herrn Dr. Safuat Hamdy (Secorvo). Eine interaktive Übersicht der Empfehlungen für Schlüssellängen findet sich auch auf http://www.keylength.com/

net surfen. Sofern Daten an Webdienste übermittelt werden, ist vorab sicherzustellen, dass besonders schützenswerte Daten davon ausgeschlossen sind.

3.9.2 Korrekte Konfiguration des Dienstes

Auch wenn es im Einzelfall lästig sein mag, die Konfigurationseinstellungen eines Webdienstes zu finden und anzupassen, sollte dies gleich nach der Registrierung erfolgen. Die meisten Webdienste sind zunächst relativ weit konfiguriert, um neuen und nicht sachkundigen Nutzern das Kennenlernen aller Funktionen zu ermöglichen. Es gilt der Grundsatz „Funktionalität vor Sicherheit". Soll ein Dienst professionell genutzt werden und ist er nicht völlig neu, kommt dagegen der Sicherheit bei der Nutzung mehr Bedeutung zu. Daher sollte darauf geachtet werden, dass keine übermäßige Freigabe von Ressourcen des eigenen Endgeräts erfolgt (bspw. Freigabe von Ordnern). Besonderes Augenmerk ist auf die Netzwerk-Sicherheit, offene Ports und die Installation von Plug-Ins zu legen. Bei Sozialen Netzwerken sollten differenzierte Zugriffsrechte für Nutzer und Nutzergruppen eingestellt werden.

3.9.3 Datensicherung

Es empfiehlt sich, sich nicht völlig vom dauerhaften Vorhandensein und Funktionieren eines Webdienstes unter fremder Kontrolle abhängig zu machen. Insofern sollten Daten, die im Webdienst (rechtmäßig) gespeichert sind, regelmäßig auch lokal zu sichern.

3.9.4 Installation von Software und Nutzung nur nach Absprache mit der IT

Applikationen, Browser Add-Ons, Plug-Ins und sonstige Software dürfen nur installiert werden, wenn eine dienstliche Nutzung erfolgt und diese ausdrücklich gestattet wurde.

Eine dienstliche Nutzung wird nur gestattet, wenn die Verwendung der Dienste durch den Projektleiter oder Vorgesetzten erlaubt wurde. Dies ist v.a. der Fall, wenn die Verwendung durch den Projektpartner gewünscht wurde oder kein eigenes Angebot vorhanden ist. Zudem dürfen keine Dokumente mit personenbezogenen oder sensiblen Daten verwendet werden oder es muss dann eine Einwilligung der Betroffenen vorliegen.

Bevor die Software installiert wird, ist die lokale IT-Administration zu konsultieren, die die Installation betreut. Die verwendeten Dienste müssen dabei so installiert und konfiguriert werden, dass keine Risiken für die IT-Infrastruktur entstehen.

3.10 Awareness und Hilfestellung

Zur Vermeidung von Risiken sollte ein Problembewusstsein bei den Nutzern geschaffen werden. Nutzer sollten fachkundige Hilfe bekommen. Kritische Nutzungen sollten kontrolliert werden:

- Awareness-Maßnahmen (Vorabbewertungen, Flyer, Road-Shows, Handlungshilfen)
- Hilfestellung für eine sichere Nutzung von Webdiensten durch IT-Mitarbeiter
- Kontrolle der Nutzer bei sensiblen Nutzungen durch Projektleiter/Vorgesetzte
- Gängige Dienste sollten einzelfallunabhängig vorab geprüft werden

Viele Risiken sind vermeidbar, wenn bei den Nutzern überhaupt ein Bewusstsein für Sicherheitsmängel besteht. Insofern sind Awareness-Maßnahmen wichtig, bspw. kurze und informative Flyer, aber auch ausführlichere Handlungshilfen oder Road-Shows.

Bei der Installation von Software und der späteren Nutzung eines Webdienstes sind die Nutzer durch fachkundige IT-Mitarbeiter zu unterstützen. Diese sind zudem als Ansprechpartner wichtig, falls während der Nutzung Fragen aufkommen.

Weiterhin sind Erkenntnisse über bereits geprüfte Dienste verfügbar zu machen (etwa Bewertungspapiere) und ein Austausch von Erkenntnissen der Mitarbeiter untereinander ist zu ermöglichen.

4 Vorgehen bei geplanter Nutzung

4.1 Gestuftes Prüfungsverfahren, Vorabprüfung, Whitelist/Blacklist

Sofern ein Webdienst eingesetzt werden soll, ist zunächst zu prüfen, ob dieser bereits bzgl. der Informationssicherheit bewertet wurde. In größeren Unternehmen empfiehlt es sich, gängige Webdienste vorab technisch und rechtlich zu bewerten und über eine Whitelist freizugeben, ggf. unter einschränkenden Bedingungen, oder zu verbieten.

Ist ein Webdienst noch nicht bewertet worden oder die Bewertung nicht aktuell, empfiehlt sich ein gestuftes Prüfungsverfahren.

Häufig kann ein Mitarbeiter bereits nach einem einfachen Check (siehe Quickcheck, Kap. 4.2) erkennen, ob eine Nutzung im konkreten Kontext aus Sicht der Informationssicherheit möglich ist oder nicht.

Um Mehrfachprüfungen zu vermeiden und auch das Wissen der Mitarbeiter einzubeziehen, könnte der Aufbau einer Intranetpräsenz oder eines Wikis sinnvoll sein.

In jedem Fall ist vor einer Installation von Software bzw. Plug-Ins und vor der Nutzung des Dienstes die IT-Administration zu konsultieren.

4.2 Quickcheck für Webdienste

Die Autoren haben exemplarisch einen Quickcheck entwickelt, der es einem Mitarbeiter ohne größeren Aufwand erlauben soll, wichtige Prüfungspunkte abzufragen und der auch der Sensibilisierung dient.

Können alle Fragen mit einem „Ja" beantwortet werden, ist die Nutzung zulässig. In diesem Fall bedarf es nur noch einer Information an einen Verantwortlichen für die Informationssicherheit, damit diese sich ein Bild über die Häufigkeit der Nutzung im Unternehmen machen oder im Einzelfall eingreifen sowie neue Erkenntnisse an die Nutzer kommunizieren kann.

Kommt der Quickcheck nicht zu einem eindeutigen und positiven Ergebnis, sind weitere Prüfungen erforderlich. Dazu ist eine Abstimmung mit dem für die Informationssicherheit Zuständigen herbeizuführen.

Er passt auf ein einseitiges Formular nebst erläuternden Hinweisen auf der Rückseite:

Quickcheck für den Webdienst _____

URL	
Was kann der Dienst?[i]	
Welche Daten werden verarbeitet?[ii]	
Welche Daten sind personenbezogen?	
Wer will den Dienst nutzen?[iii]	
Für welchen Zweck?[iv]	

	Prüffragen	**Ja?**	**Bemerkung/Begründung°**
1.	Es besteht ein konkreter, betrieblicher Nutzen?[1]		
2.	Ein gleichwertiger eigener oder positiv bewerteter externer Dienst steht nicht Verfügung?[2]		
3.	Falls personenbezogene Daten von Mitarbeitern verarbeitet werden: Liegt Einwilligung oder Betriebsvereinbarung vor?[3]		
4.	Wenn Daten unerwartet weitergegeben oder verändert würden, entstünde dem Unternehmen und Dritten kein Schaden?[4]		
5.	Es bestehen keine Bedenken, wenn das Angebot unangekündigt eingestellt oder Daten gelöscht werden?[5]		
6.	Wenn personenbezogene oder vertrauliche Daten verarbeitet werden: Der Anbieter sitzt in der Europäischen Union?[6]		
7.	Es bestehen keine aktuellen Erkenntnisse über Sicherheitsschwachstellen?[7]		
8.	Es bedarf keiner Installation von Programmen/ Code-Teilen (z.B. ActiveX) und keine niedrige Browser-Sicherheitseinstellung?[8]		
9.	Anbieter und Dienst sind bekannt, werden als seriös angesehen und animieren nicht zu problematischen Nutzungen?[9]		
10.	Falls Daten anderer verarbeitet werden: Besteht eine ausdrückliche Zustimmung oder legitimierende Vertragsregel?[10]		
11.	Bestehen keine kritischen Datenschutzregelungen, insbes. keine Sammlung / Weitergabe personenbezogener Daten?[11]		
12.	Bestehen keine kritischen Nutzungsbedingungen, v.a. keine weit gehende Übertragung von Nutzungsrechten?[12]		
13.	Ist die kostenfreie und geschäftliche Nutzung zulässig?[13]		

Freigabe:#		Auflagen:	

Erläuterungen zum Quickcheck

Der Quickcheck ermöglicht einem IT-Sicherheitsbeauftragten in Rücksprache mit Anwendern eine kurze Prüfung, ob die Nutzung eines Webdienstes ohne tiefere Untersuchung gestattet werden kann. Er bezieht sich auf Webdienste, die noch nicht systematisch bewertet wurden. Hinweise zu den Feldern:

i Bsp.: Dokumentenmanagement, Terminmanagement, Blogging, Dokumentenerstellung.
ii Bsp.: Dokumente, Passwörter, Namen, Mailadressen, Interessendaten, Termindaten.
iii Abteilungen, Mitarbeiter (funktional nicht namentlich), externe Firmen und Mitarbeiter.
iv Beschreibung des geplanten betrieblichen Nutzungszwecks, etwa Arbeit im Projekt X mit Kunde Z.
0 Ggf. kann eine Prüffrage nur dann mit „ja" beantwortet werden, wenn an die Dienstenutzung eine Bedingung geknüpft wird. Zu denken ist z.B. an eine Nutzung nur bzgl. bestimmter Dokumentenarten.
1 Nur privater Nutzen genügt nicht. Ein betrieblicher Nutzen kann auch betrieblich veranlasstes Testen sein.
2 Ausnahme: Es sollen absichtlich mehrere Webdienste genutzt werden, z.B. Suchmaschinen.
3 Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmbaren natürlichen Person (d.h. Wahrscheinlichkeit der Bestimmbarkeit genügt, auch mit Hilfe Dritter). Betriebsvereinbarungen finden sich im Intraweb. Ob Einwilligungen schriftlich oder mündlich erfolgen sollen ist nicht generell bestimmbar, hier für den Quickcheck ist zumindest eine mündliche Einwilligung erforderlich.
4 V.a. dürfen keine Betriebsgeheimnisse offenbart werden. Daneben dürfen auch keine personenbezogenen Daten weitergegeben werden (dazu Fragen 3, 10 und 11). Betriebsgeheimnisse: Zu berücksichtigen sind eigene Geheimnisse und solche Dritter. Sensible Projekte: Hier bestehen besonders hohe Anforderungen an die Sicherung der Daten vor unbefugter Weitergabe.
5 Oft behalten sich kostenlose Dienste vor, ihr Angebot jederzeit und ohne Angabe von Gründen einzustellen.
6 Nutzungsbedingungen (EULA) sehen oft vor, dass Daten auch zu eigenen Zwecken des Dienstes verwendet werden dürfen, oder an dessen „Partner" übermittelt werden dürfen, d.h. an jeden beliebigen Dritten.
Außerhalb der EU besteht weder ein vergleichbares Datenschutzniveau noch eine Möglichkeit, Rechtsansprüche entsprechend durchzusetzen. Daher fordert das Gesetz spezielle Vereinbarungen für eine Datenübermittlung außerhalb der EU. Der Sitz des Webdienstes kann i.d.R. dem Impressum entnommen werden.
7 Kurze (Internet-)Recherche.
8 Niedrigere Sicherheitseinstellungen des Browsers sind u.a. die Installation von ActiveX-Controls.
9 Ein Impressum mit Anschrift und elektr. Kontakt sollte vorhanden sein. Dann kurze (Internet-)Recherche über z.B. Suchmaschinen, Whois-Abfrage. Bei der eigenveranlassten Nutzung, die man anderen Partnern vorgeben möchte, wird ein höherer Maßstab verlangt. Bestehen bspw. Anhaltspunkte, dass der Dienst bevorzugt für illegale Handlungen verwendet wird, wie oftmals bei Online-Tauschbörsen, soll er nicht genutzt werden. Zu berücksichtigen ist das Image der Gesellschaft als seriösem Betrieb. Darüber hinaus kann sich auch eine weitreichende Nutzung vieler als seriös angesehener Webdienste negativ auf die Wahrnehmung der Gesellschaft auswirken, wenn der Eindruck entsteht, dass üblicherweise in einem Unternehmen vorhandene eigene Dienste und Tools nicht bestehen oder deren Nutzung nicht getraut wird.
10 Betroffene können sowohl eigene Mitarbeiter als auch Externe sein. Soweit externe Projektpartner beteiligt sind, bedarf es einer ausdrücklichen Zustimmung des externen Projektpartners. Ist der externe Projektpartner wie üblich ein Unternehmen, so ist das Unternehmen betroffen, nicht nur der handelnde Mitarbeiter. Es bedarf daher der Zustimmung eines bevollmächtigten Mitarbeiters für das Unternehmen. Erteilt ein nicht bevollmächtigter Mitarbeiter seine Zustimmung, so wirkt diese i.d.R. nicht gegenüber seinem Unternehmen. Grund: Mitarbeiter können und dürfen rechtlich nicht ohne Weiteres Verpflichtungen für Ihr Unternehmen eingehen oder neue Arbeitsabläufe vereinbaren, bspw. eigenmächtig betriebliche Dateien verschlüsseln oder eine Datenspeicherung auf einen Webdienst auslagern. Grds. ist es Sache des Empfängers einer Erklärung wie einer Zustimmung, sich von der Vollmacht des Erklärenden zu überzeugen. Weiterhin genügt eine nur unterstellte Zustimmung nicht (z.B. durch die Annahme, eine solche Nutzung sei „üblich"). Eine nur mündliche Zustimmung genügt ebenfalls nicht. Die Zustimmung muss später belegt werden können, z.B. durch eine E-Mail oder einen Brief.
11 Die Datenschutzhinweise sind unbedingt zu prüfen. Sie sind zu speichern bzw. auszudrucken. Auftragsdatenverarbeitungen, bei denen der Betroffene aus Datenschutzsicht nicht einwilligen muss (unabhängig von Fragen 3 und 10), bedürfen nach dem Gesetz zwingend einer schriftlichen Vereinbarung unter Berücksichtigung aller Anforderungen nach § 11 BDSG, v.a. eine Kontroll- und Weisungsbefugnis geg. dem Dienst.
12 Bspw. können Nutzungsbedingungen (EULA) vorsehen, dass einem Dienst gewisse Nutzungsrechte an den übermittelten Daten eingeräumt werden. In diesem Fall kann der Nutzer sein ausschließliches Nutzungsrecht verlieren, was später einer kommerziellen Verwertung im Weg stehen kann. Die Nutzungsbedingungen sind daher unbedingt zu prüfen. Sie sind zu speichern bzw. auszudrucken.
13 Auch die Nutzung zu wissenschaftlichen nicht kommerziellen Zwecken kann in Frage kommen, wenn Projekte wissenschaftlich und öffentlich gefördert sind (nicht Auftragsforschung für die Industrie). Nutzungsbedingungen enthalten oftmals versteckte Zahlungsverpflichtungen. Insbesondere erlauben viele Webdienste eine kostenlose Nutzung nur für den privaten Gebrauch, nicht aber zu betrieblichen Zwecken. In diesem Fall darf ein Dienst nicht genutzt werden, da Lizenzverstöße erhebliche Schäden nach sich ziehen können.

Wenn alle Fragen mit „ja" beantwortet wurden, kann die Nutzung sofort gestattet werden. Bei Zweifeln oder einem „nein" ist eine Abstimmung mit dem IT-Sicherheitsbeauftragten nötig, der ggf. weitere Prüfungen veranlasst oder eine Ausnahmegenehmigung erteilt.

5 Aufbau eigener Angebote

In größeren Unternehmen kann es sinnvoll sein, häufig genutzte Webdienste selbst anzubieten. Dabei bieten sich freilich nicht Dienste an, die stark auf eine Social-Media-Komponente setzen, da eigene Angebote diese nicht ersetzen können (z.B. Facebook), jedoch solche, die lediglich mangels einer einfachen und schnell verfügbaren Alternative im Unternehmen extern beigezogen werden. In Betracht kommen etwa Dienste zum sicheren Austausch von größeren Dateien, zur Online-Speicherung in der Cloud oder zur Terminkoordination.

5.1 Wichtige Dienste für eigene Angebote

Für wichtige und vielfach genutzte Webservices sollte es eigene Angebote geben:

- *Terminfindungsdienste:* werden häufig eingesetzt.
- *URL-Shortener:* Die Abkürzung langer Links ist vielen Mitarbeitern ein Anliegen. Interne Links können interne Informationen enthalten.
- *Dienste zum vertraulichen Datenversand:* Vielfach besteht in Projekten der Wunsch, große Datenvolumina vertraulich zu versenden. Unbedarfte Nutzer verwenden YouSendIt oder ähnliche Internetangebote. Einzelne verwenden eigene Cryptshare-Installationen.
- *Kollaborationsplattformen*: Projekte benötigen Plattformen zum Dokumentenaustausch und zur Dokumentenverwaltung. Vielfach werden Dropbox und andere Webdienste verwendet.
- *Dienste zur Datensynchronisierung*: Für den Datenaustausch zwischen verschiedenen Geräten eines Nutzers verwenden unbedarfte Mitarbeiter ebenfalls Dropbox und ähnliche Webdienste.

5.2 Anforderungsübersicht für eigene Angebote

Bei eigenen Dienste-Angeboten ist nach vorläufiger Einschätzung insbesondere zu beachten

- Die Angebote sollten bei öffentlich geförderten Unternehmen nur von eigenen Mitarbeitern und Kooperationspartnern genutzt werden können. In diesen Fällen dürfen Angebote nicht in Konkurrenz zu Diensten der freien Wirtschaft stehen.
- Im Übrigen sollte eine Risikobegrenzung durch eine beschränkte Nutzerzahl erreicht werden.
- Die Schadenspotentiale sind zu bewerten. Abhängig davon sind Sicherheitsprüfungen und -konzepte festzulegen.
- Es sind sichere Programmierstandards vorzugeben.
- Der Login und die Datenübertragung sollten verschlüsselt erfolgen. Die verschlüsselte Speicherung von Daten mit Schlüsselverwaltung in Nutzerhand sollte ermöglicht werden (Ende-zu-Ende).
- Der Betrieb sollte auf eigenen, sicheren Servern an den Instituten erfolgen (nicht bspw. Amazon oder „China-Cloud").
- Impressum und Datenschutzhinweise sowie Nutzungsbedingungen sind zu erstellen. SLA sind in den Nutzungsbedingungen festzulegen.
- Gegenüber Externen sind Gewährleistung und Haftung auszuschließen. Externe sind auf die Einhaltung der übrigen Bestimmungen für die eigene IT-Infrastruktur zu verpflichten.
- Mitbestimmungs- und Informationsrechte des Betriebs-/Personalrats sind zu beachten.

6 Literaturverzeichnis

Zur Vertiefung der Themen in diesem Beitrag empfehlen die Autoren folgende Literatur, sortiert in historischer Reihenfolge:

- Im Netz von Google - Web-Tracking und Datenschutz, Roland Steidle, Ulrich Pordesch, DuD 2008, 324 ff.
- Privatsphärenschutz in Soziale-Netzwerke-Plattformen, Fraunhofer-Institut für Sichere Informationstechnologie, 23.9.2008.
- Towards an Analytic Approach to Evaluate Enterprises' Risk Exposure to Social Networks, Hewlett-Packard Development Company, 2009.
- Chrome mit Kratzern - Googles Webbrowser und der Datenschutz, Roland Steidle, Ulrich Pordesch, Katja Seitz, Jan Steffan, DuD 2009, 47 ff.
- Datenschutz bei Nutzung von Location Based Services im Unternehmen, Roland Steidle, MMR 2009, 167 ff.
- Cloud Computing - Evolution in der Technik, Revolution im Business, Bitkom Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V., 2009.
- Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) am 26./27. November 2009 in Stralsund.
- Informationelle Selbstbestimmung im Web 2.0, von der Deutschen Forschungsgesellschaft DFG 2009-2012 gefördertes Projekt an der Universität Kassel/Projektgruppe verfassungsverträgliche Technikgestaltung (provet).
- Twitter und Recht, Henning Krieg, K&R 2/2010, 73 ff.
- Leitfaden Social Media, Bitkom, 2010.
- Mehr Rechtssicherheit mit Social Media-Policies, Roland Steidle, E-Commerce Magazin, 3/2011, 42 ff.
- Datenschutz bei Sozialen Netzwerken jetzt verwirklichen! Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München.
- Orientierungshilfe – Cloud Computing, der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 26.09.2011.
- Datenschutz in Sozialen Netzwerken Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 08. Dezember 2011).
- Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG, Becker Philipp , Nikolaeva Julia, CR 2012, 170 ff.
- Wirksamkeit der Nutzungsbedingungen Sozialer Netzwerke - Rechtskonforme Lösung nach dem AGB- und dem Urheberrecht, Christian Solmecke, Annika Dam, MMR 2/2012, 71 ff.
- On the Security of Cloud Storage Services, Fraunhofer Institute for Secure Information Technology, SIT Technical Reports, 3/2012.
- Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter, Marit Hansen, DuD 6/2012, 407 ff.
- Value4Cloud: Marktunterstützende Mehrwertdienste zur Förderung von Vertrauen, Rechtsverträglichkeit, Qualität und Nutzung von Cloud Services für den Mittelstand, vom BMWi und Trusted Cloud 2012-2014 gefördertes Projekt an der Universität Kassel/provet, Institut für Wirtschaftsrecht.
- Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - International Working Group on Data Protection in Telecommunications, 51st meeting, 24. April 2012, Sopot (Poland).