Seminar „Governance, Risk & Compliance“

Neue Herausforderungen für die GRC-Organisation durch offenere Unternehmensgrenzen

Moritz Klammler[*]

27. Juni 2014

Betreuer:

Prof Dr Thomas Dreier[†] Dr Hans Röhm[‡] Dr Louisa Specht[§]

[*]Karlsruher Institut für Technologie (KIT), Fakultät für Informatik;
Studiengang: Informatik (Bachelor), Fachsemester: 6, Matrikel-Nummer: [verborgen].

[†]Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR).

[‡]Deloitte Touche Tohmatsu Limited (DTTL).

[§]Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR).

Copyright © 2014 Moritz Klammler

Dieses Werk ist lizenziert unter einer Creative Commons *Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International* Lizenz.

`https://creativecommons.org/licenses/by-sa/4.0/deed.de`

Dieses Dokument und die zugehörige Präsentation sind zusammen mit dem Quellcode über die Webseite des Autors verfügbar.

`http://klammler.eu/data/jura/kit/grc/`

Zusammenfassung

In diesem Aufsatz werden Fragen der GRC-Organisation diskutiert, die sich durch den fortschreitenden Einsatz neuer IT in allen Lebens- und Geschäftsbereichen und das zunehmende Verschwimmen der Grenzen zwischen Berufs- und Privatleben, ergeben. Dabei wird ein Schwerpunkt auf technologische Risiken, die für Unternehmen entstehen, und neue Herausforderungen an die Compliance für Datensicherheit und den Datenschutz gelegt. Im Appendix (S 11ff) sind einige Fallbeispiele mit realem Hintergrund aufgeführt.

Moritz Klammler, Karlsruhe am 27. Juni 2014

Inhaltsverzeichnis

I Fragestellungen **1**
A Datensicherheit und Datenschutz 1
1 Datensicherheit 1
2 Unbefugter Zugriff 1
3 Datenschutz 1
B Verlässlichkeit von IT-Systemen 2
C Verantwortung und Haftung 2

II Herausforderungen **2**
A Soziale Online-Netzwerke 2
B Ubiquitäres Rechnen 5
1 Persönliche mobile Endgeräte 5
2 Vernetzte intelligente Mess-, Steuer- und Regelungssysteme 7
C Externe IT-Dienstleistungen und verteiltes Rechnen 8

III Fazit **10**

Fallbeispiele **11**

Abkürzungen

AGB Allgemeine Geschäftsbedingungen

BDSG Bundesdatenschutzgesetz

BGB Bürgerliches Gesetzbuch

BYOD *bring your own device*

bzw beziehungsweise

etc *et cetera*

Fn Fußnote

GPS *global positioning system*

idR in der Regel

IP *internet protocol*

iSd im Sinne (der|des)

iSv im Sinne von

IT Informationstechnologie

PC *personal computer*

RSA Public-Key-Kryptographiesystem, benannt nach Ron Rivest, Adi Shamir und Leonard Adleman

Rz Randziffer

SaaS *software as a service*

sog sogenennt[s|e|r]

TKG Telekommunikationsgesetz

TMG Telemediengesetz

UrhG Urheberrechtsgesetz

zB zum Beispiel

Literatur

Andresen 2009
Andresen, „Compliance“. 2009. URL: https://www.admin-magazin.de/Online-Artikel/Technical-Review/Compliance/ (abgerufen am 13. 06. 2014).

BayLDA 2014
BayLDA, „Erneute App-Prüfung zeigt weiterhin erhebliche Mängel beim Datenschutz“. Pressemitteilung des Bayerischen Landesamtes für Datenschutzaufsicht. Mai 2014. URL: http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2014/pm008.html (abgerufen am 08. 06. 2014).

Bergmann, Moehrle und Herb 2013
Bergmann/Moehrle/Herb, Hrsg., Datenschutzrecht: Handkommentar zum Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, Bereichsspezifischer Datenschutz. Stuttgart: Boorberg, 2013. ISBN: 978-3-415-00616-4.

Brendel 2013
Brendel, „Mobile Mega-Flops“. Juli 2013. URL: https://www.admin-magazin.de/News/Mobile-Mega-Flops/ (abgerufen am 10. 06. 2014).

Bussche und Schelinski 2013
Bussche/Schelinski, Münchener Anwaltshandbuch IT-Recht. 3. Aufl. München: C H Beck, 2013. ISBN: 978-3-406-64845-8.

Eckersley 2010
Eckersley, „How Unique Is Your Web Browser?“ In: *Proceedings of the Privacy Enhancing Technologies Symposium*. Springer Lecture Notes in Computer Science, 2010. URL: https://panopticlick.eff.org/browser-uniqueness.pdf (abgerufen am 10. 06. 2014).

EFF 2010
EFF, „Panopticlick“. Electronic Frontier Foundation. 2010. URL: https://panopticlick.eff.org/ (abgerufen am 10. 06. 2014).

Ernst 2011
Ernst, „Social Networks und Arbeitnehmer-Datenschutz“. In: *NJOZ* 23 (2011), 953.

Ernst 2010
Ernst, „Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem“. In: *NJOZ* 36 (2010), 1917–1958.

Fahl 2013
Fahl, „Ergebnisse eines Android-Sicherheitschecks erschrecken“. In: *Admin* 11 (2013), 110–113. URL: https://www.admin-magazin.de/Das-Heft/2013/11/Ergebnisse-eines-Android-Sicherheitschecks-erschrecken/ (abgerufen am 10. 06. 2014).

FSF 2014
FSF, „Zu vermeidende Wörter“. Juni 2014. URL: https://www.gnu.org/philosophy/words-to-avoid.de.html (abgerufen am 10. 06. 2014).

Genkin, Shamir und Tromer 2013
Genkin/Shamir/Tromer, *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*. Dez. 2013. URL: https://www.cs.tau.ac.il/~tromer/acoustic/ (abgerufen am 10. 06. 2014).

gerloff 2013
gerloff, „Renault will remotely lock down electric cars“. Okt. 2013. URL: https://blogs.fsfe.org/gerloff/2013/10/31/renault-will-remotely-lock-down-electric-cars/ (abgerufen am 10. 06. 2014).

Greveler et al 2012
Greveler, „Multimedia Content Identification Through Smart Meter Power Usage Profiles“. Ruhr-Universität Bochum, 2012. URL: https://www.nds.rub.de/research/publications/SmartmeterContentIdent/ (abgerufen am 10. 06. 2014).

Hammersen und Weißgerber 2014
Hammersen/Weißgerber, „Bring Your Own Device – Patentlösung im Klinikbereich?“ In: *ZD-Aktuell* 10 (2014), 03195.

Heydn 2014
Heydn, „BGH: Handel mit Gebrauchtsoftware – UsedSoft II“. In: *MMR* 4 (2014), 209–280.

Hucko 2013
Hucko, „Akkuleasing für Elektroautos: Ausgeliehen und abgewürgt“. In: *Spiegel Online* (Okt. 2013). URL: https://www.spiegel.de/auto/aktuell/elektroauto-renault-kann-aufladen-der-batterie-stoppen-a-930066.html (abgerufen am 12. 06. 2014).

IBM 2012
IBM, „Mid-year Trend and Risk Report“. IBM X-Force, Sep. 2012. URL: https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=ov7304&lang=de_DE (abgerufen am 07. 06. 2014).

Kuppinger 2010
Kuppinger, „Sicherheitsrisiko Cloud Computing?“ 2010. URL: https://www.admin-magazin.de/Online-Artikel/Technical-Review/Sicherheitsrisiko-Cloud-Computing/ (abgerufen am 10. 06. 2014).

Roosendaal 2011
Roosendaal, „Facebook tracks and traces everyone: Like this!“ Tilburg Institute for Law, Technology, und Society, 2011. URL: http://ssrn.com/abstract=1717563 (abgerufen am 10. 06. 2014).

Schmidt 2011
Schmidt, „2 Klicks für mehr Datenschutz". Sep. 2011. URL: https://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html (abgerufen am 10. 06. 2014).

Stallman 2010
Stallman, „What Does That Server Really Serve?" In: *Boston Review* (März 2010). URL: http://www.bostonreview.net/richard-stallman-free-software-DRM/ (abgerufen am 10. 06. 2014).

Stone 2009
Stone, „Amazon Erases Orwell Books From Kindle". In: *The New York Times* (Juli 2009), B1. URL: http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html (abgerufen am 10. 06. 2014).

StudiVZ 2007
StudiVZ, „StudiVZ Allgemeine Geschäftsbedingungen (Version 2.0)". Dez. 2007. URL: http://www.studivz.net/l/terms/ (abgerufen am 10. 06. 2014).

Thüsing 2014
Thüsing, Beschäftigtendatenschutz und Compliance. 2. Aufl. München: C H Beck, 2014. ISBN: 978-3-406-62820-7.

Weßelmann und Wiele 2010
Weßelmann/Wiele, „Security Awareness: Der Mensch als Sicherheitsrisiko". In: *Admin* 3 (2010), 80–83. URL: https://www.admin-magazin.de/Das-Heft/2010/03/Security-Awareness-Der-Mensch-als-Sicherheitsrisiko/ (abgerufen am 10. 06. 2014).

Wikipedia 2014
Wikipedia, „SCO–Linux controversies — Wikipedia, The Free Encyclopedia". 2014. URL: http://en.wikipedia.org/w/index.php?title=SCO%E2%80%93Linux_controversies&oldid=609983592 (abgerufen am 10. 06. 2014).

ZD-Redaktion 2013
ZD-Redaktion, „HmbBfDI: Bußgeld gegen Google festgesetzt". In: *ZD-Aktuell* (2013).

I Fragestellungen

Für ein modernes Unternehmen stellen sich im Hinblick auf Risikomanagement und Compliance heute zahlreiche Fragen, die sich aus technologischen und gesellschaftlichen Veränderungen ergeben.

A Datensicherheit und Datenschutz

1 Datensicherheit

a Datenverlust Ein (auch nur vorübergehender) Verlust von Geschäftsdaten ist für viele Unternehmen heute ein existenzgefährdendes Risiko. In Kapitel II soll anhand von Beispielen diskutiert werden, welche Technologien und Produkte ein besonders hohes Risiko in diesem Bereich haben. Während die Gefährdung durch physische Zerstörung der Datenträger eher an Bedeutung verliert, stellt die wachsende Komplexität von (insbesondere von verteilten) IT-Systemen große Herausforderungen an die revisionssichere Archivierung.[1]

2 Unbefugter Zugriff

Mit wachsender Komplexität eines IT-Systems steigt auch die Gefahr, dass an einer Stelle Personen Zugriff auf Daten erlangen, die nicht sollten. Dies kann einerseits geschäftsrelevante Informationen in falsche Hände geraten lassen, andererseits gegen datenschutzrechtliche Auflagen verstoßen. Beim Angriff auf IT-Systeme und Industriespionage ist ein Trend zu „blended attacks“ zu beobachten, die insbesondere den Faktor Mensch ausnutzen.[2] Dieser Umstand gewinnt dadurch noch an Bedeutung, dass IT-Systeme heute längst nicht mehr nur von Spezialisten bedient werden.

3 Datenschutz

Mittels moderner Technologie ist es möglich, immense Datenmengen zu vernachlässigbaren Kosten zu erheben und auszuwerten. Datenschutz ist nicht nur ein gesetzliches, sondern auch ein ethisches Gebot für Unternehmen. Dabei geht es sowohl um die Daten von Dritten (Kunden, Geschäftspartner, etc), als auch um den Schutz der eigenen Mitarbeiter vor allzu viel Überwachung im eigenen Unternehmen (Mitarbeiterdatenschutz).

[1] Eine Diskussion der Konsequenzen für die Datenarchivierung, die sich für Unternehmen aus dem Sarbanes Oxley Act oder dem Basel-II-Standard ergeben, findet sich bei Andresen 2009. Ergebnis: nicht allzu viel Neues.

[2] Für eine recht gute Diskussion siehe Weßelmann und Wiele 2010.

B Verlässlichkeit von IT-Systemen

Ein unzuverlässiges oder ausfallendes IT-System ist für die meisten Unternehmen heute ein signifikantes Risiko. Hier stellt sich insbesondere die Frage, *was* die Systeme machen, wer sie kontrolliert, und ob dies auch in Zukunft gewährleistet sein wird. Bei proprietären Systemen können diese Fragen allgemein nur unzureichend beantwortet werden.

C Verantwortung und Haftung

Viele neue Technologien werfen Rechtsfragen auf, die von der Rechtsprechung noch nicht abschließend geklärt wurden. Für ein Unternehmen ist diese Unsicherheit einerseits ein zusätzliches Risiko, anderseits eine Herausforderung, jenseits klarer Rechtsnormen einen eigenen Compliance-Kodex zu finden.

II Herausforderungen

A Soziale Online-Netzwerke

Soziale Netzwerke sind längst nicht mehr bloße Freizeitbeschäftigung, sondern werden von vielen Unternehmen als wichtiges Medium genutzt, um sich der Öffentlichkeit zu präsentieren, neue Kunden zu werben, mit bestehenden Kunden im Kontakt zu bleiben und (potentielle) Mitarbeiter anzusprechen. Die heute populären Netzwerke[3] werden von zentralen Organisationen weltweit verwaltet, die die volle technische Kontrolle über die Aktivitäten der Benutzer haben.[4]

a Nutzung zur Mitarbeiterakquise Die systematisch strukturierten Daten in einem sozialen Netzwerk erlauben es einem Unternehmen, sehr effizient Informationen über potentielle neue Mitarbeiter zu gewinnen. Seitens der Betreiber des sozialen Netzwerks kann dies explizit gewünscht (etwa bei XING[5]), untersagt (etwa bei StudiVZ[6]) oder ungeklärt (etwa bei Facebook[7]) sein. Aus datenschutzrechtlicher Sicht dürfte die offizielle Zweckbestimmung des Anbieters jedoch nachrangig und jedes soziale Netzwerk als allgemein zugängliche Quelle iSd BDSG anzuse-

[3] Vor allem Twitter (`https://twitter.com/`), Facebook (`https://facebook.com/`) oder Google+ (`https://plus.google.com/`).

[4] Das ist keineswegs eine technische Notwendigkeit, sondern eine bewusste Entscheidung der Betreiber, deren Geschäftsmodell auf dieser Zentralisierung basiert. Es ist durchaus möglich, ein soziales Netzwerk dezentral zu organisieren. Das soziale Netzwerk Diaspora★ (`https://joindiaspora.com/`) ist ein Beispiel dafür.

[5] `https://www.xing.com/`

[6] `http://www.studivz.net/`, zu den AGB siehe StudiVZ 2007

[7] `https://www.facebook.com/`, siehe auch Ernst 2011

hen sein.[8] Rechtliche Grundlage für eine solche Recherche ist entweder § 28[9] oder § 32[10] BDSG. Ernst lässt diese Frage dahinstehen, und kommt unabhängig davon zum Ergebnis, dass die Erhebung grundsätzlich zulässig sei, wenn ihr kein berechtigtes Interesse des Arbeitnehmers entgegensteht, wovon „nicht auszugehen sei".[8]

b Nutzung zum Kundenkontakt Viele Firmen präsentieren sich aktiv in sozialen Netzwerken und wickeln einen erheblichen Teil ihrer Kundenkommunikation darüber ab.

aa Abhängigkeit vom Netzwerkbetreiber Da das soziale Netzwerk vollständig unter der Kontrolle des Betreibers ist, ist ein Unternehmen, das es zur Kommunikation mit Kunden nutzt, in hohem Maße von diesem Betreiber abhängig (siehe jedoch auch Fn 4). Er kann (zumindest technisch) jederzeit den Kontakt zu Kunden blockieren, Nachrichten zensieren oder den Account des Unternehmens als ganzes deaktivieren. Nachdem die Nutzung idR unentgeltlich erfolgt, sind die Nachteile für den Netzwerkbetreiber sehr gering. Zusätzlich dürften die Möglichkeiten des betroffenen Unternehmens, sich rechtlich zu wehren – nicht zuletzt aufgrund von AGB, die häufig den Betreibern sehr viele und den Benutzern sehr wenige Rechte einräumen (und die im Unternehmergeschäft keiner Inhaltskontrolle unterworfen werden) – schlecht sein.

bb Arbeitsrechtliche Fragen Denkbar ist, dass der Kundenkontakt über

(i) ein Nutzerprofil des Unternehmens, das von Mitarbeitern gepflegt wird,

(ii) individuelle Benutzerprofile, die sich Mitarbeiter zu diesem Zweck anlegen, oder

(iii) die privaten Benutzerprofile der Mitarbeiter

erfolgt. Der Fall (i) ist offensichtlich unproblematisch. Im Fall (ii) wird es von der Position des Arbeitnehmers abhängen, ob eine solche Repräsentation des Unternehmens zu seinen Dienstpflichten zählt, was – dort, wo sich diese Frage stellt – regelmäßig zu bejahen sein wird. Kritisch ist Fall (iii), der im Allgemeinen nicht von der Dienstpflicht umfasst sein wird, und explizit im Arbeitsvertrag erwähnt sein müsste.[11]

Im Fall (i) kann der Account beim Ausscheiden des Mitarbeiters, der ihn gepflegt hat, an den Arbeitgeber übertragen werden. Im Fall (iii) wird der Arbeitgeber einen Anspruch darauf haben,

[8] Siehe dazu ausführlich Ernst 2011.

[9] Datenerhebung und -speicherung für eigene Geschäftszwecke

[10] Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

[11] Siehe dazu ausführlich Thüsing 2014, Rz 51ff.

dass der Mitarbeiter Kunden- und sonstige Geschäftsdaten, die mit dem Account verbunden sind, an ihn herausgibt und sodann bei sich löscht, den Account selbst wird der Mitarbeiter weiter nutzen dürfen. Im Fall (ii) wird man den Account nach Herausgabe der Kunden- und sonstigen Geschäftsdaten wohl dauerhaft deaktivieren.[11]

c Private Nutzung durch Mitarbeiter Tätigkeiten, die einen Bezug zu Arbeit oder Arbeitsplatz haben, und das Arbeitsverhältnis konkret beeinträchtigen, hat der Arbeitnehmer (auch außerhalb sozialer Netzwerke) aufgrund der durch den Arbeitsvertrag begründeten Treuepflicht (§ 241 BGB) zu unterlassen. In besonderen Fällen kann es (zB aus Sicherheitsgründen) angemessen sein, dass ein Mitarbeiter seine Position im Unternehmen nicht auf seiner Profilseite preisgibt. Ein generelles Verbot, in sozialen Netzwerken aktiv zu sein, und dort auch über den Arbeitsplatz zu berichten, steht dem Arbeitgeber nicht zu.[11]

In der Literatur finden sich zahlreiche Hinweise dafür, dass manche Mitarbeiter mit der Nutzung sozialer Netzwerke überfordert sind, und ungewollt rechtswidrige Handlungen begehen oder Firmengeheimnisse verraten.[12] Relevant für den Arbeitgeber ist hier insbesondere, dass er für Urheberrechtsverletzungen der Mitarbeiter mithaftet (§ 99 UrhG).

Da diese Handlungen nicht vorsätzlich begangen werden (und ohnehin bereits per Gesetz verboten sind), ist ein Verbot wenig zielführend. Besser ist es, die Mitarbeiter im Umgang mit sozialen Netzwerken zu trainieren.[13] Teilweise wird auch noch diskutiert, den Gebrauch sozialer Netzwerke am Arbeitsplatz völlig zu untersagen,[14] was – sofern dazu ein Computer des Arbeitgebers verwendet wird – zwar rechtlich möglich, praktisch aber wohl nicht mehr realistisch ist.

d Einbindungen auf die eigene Webseite Die meisten sozialen Netzwerke beschränken sich nicht auf ihre eigene Internetpräsenz, sondern bieten auch Dritten die Möglichkeit, mittels einfach zu verwendender Plugins Inhalte und Funktionalitäten des Netzwerks auf ihrer Webseite zu integrieren. Das bekannteste Beispiel ist wahrscheinlich der „Like-Button“ von Facebook.[15]

Diese Plugins stellen an die einbindende Webseite so wenig Anforderungen wie möglich, und implementieren fast die gesamte (idR proprietäre) Funktionalität auf den Servern des sozialen Netzwerks. Das führt zumindest dazu, dass der Betreiber des sozialen Netzwerks für jeden Besucher der Firmenwebseite – auch solchen, die keinen Account besitzen und den Like-Button (oder was auch immer) nicht anklicken – in Kenntnis über die IP-Adresse, Zeitpunkt des Aufrufs und

[12] So etwa bei Thüsing 2014, Ernst 2011 oder Weßelmann und Wiele 2010.
[13] Ernst 2011
[14] Thüsing 2014
[15] `https://developers.facebook.com/docs/plugins/like-button/`

der Browser-Signatur kommt. Letztere genügt – mithilfe von etwas JavaScript-Code – um fast jeden Browser der Welt eindeutig zu identifizieren, sofern der Benutzer nicht besondere Gegenmaßnahmen getroffen hat.[16] Im Falle des Facebook-Like-Buttons wird zusätzlich ein Facebook-Cookie übertragen, wenn dieses zuvor durch ein anders Facebook-Plugin gesetzt wurde.[17] Verantwortlicher für diese Verarbeitung personenbezogener Daten iSd BDSG ist nicht etwa (alleine) Facebook, sondern das Unternehmen, dessen Webseite besucht wird – obgleich es keinerlei Kontrolle darüber hat, was mit den Daten geschieht. Die Rechtsgrundlage, auf der der Like-Button zu bewerten ist, ist strittig (TMG oder BDSG, wohl nicht TKG). Nicht zuletzt, weil Facebook nicht offenlegt, welche Daten erhoben werden und was mit ihnen geschieht. Ernst sieht derzeit „keine Möglichkeit einer gesetzeskonformen Nutzung dieser Technik."[18]

Die Webseite `www.heise.de` hat 2011 als erste begonnen, Benutzer nach einer Einwilligung zu fragen, bevor das Plugin für den Facebook-Like-Button geladen wird. Der Code dafür wurde als freie Software auch anderen Webseiten zur Verfügung gestellt.[19]

B Ubiquitäres Rechnen

Der technische Fortschritt der letzten Jahre hat es ermöglicht, selbst kleinste Geräte mit hoher Rechenkapazität auszustatten und es wirtschaftlich gemacht, mehr und mehr Geräte elektronisch zu vernetzen.

1 Persönliche mobile Endgeräte

Für die meisten Menschen ist es längst selbstverständlich geworden, kaum jemals ohne ein elektronisches Gerät unterwegs zu sein. Während die beschränkte Rechenkapazität von Handys diese lange Zeit für kaum mehr als zum Telefonieren und für einfache Organisationsaufgaben nützlich machte, verfügen moderne Smartphones und Tablets über eine Rechenleistung, die jene von auch nur wenige Jahre alten Laptop- und Desktop-PCs bei weitem übersteigt. Zusätzlich sind diese Geräte mit viel Spezialhardware wie Mobilfunk-Modems, Mikrofonen, Kameras, GPS-Empfängern oder Beschleunigungssensoren ausgestattet.

Im Unternehmensbereich war es lange Zeit selbstverständlich, dass Mitarbeiter ihre Arbeitsplatzrechner nicht selbst administieriren, sondern ein von der IT-Abteilung gewartetes und ver-

[16] Zur Möglichkeit der Browser-Identifikation, siehe EFF 2010 bzw darüber Eckersley 2010.

[17] Der Mechanismus ist bei Roosendaal 2011 gut beschrieben.

[18] Siehe Ernst 2010; mit einer leider sehr kurzen und nicht wirklich überzeugenden Begründung dafür, dass alleine das BDSG und nicht das TMG anzuwenden sei.

[19] Schmidt 2011

waltetes Gerät benutzen, auf dem sie selbst nur über beschränkte Rechte verfügen. Dies erlaubt es der IT-Abteilung, gewisse Sicherheitsstandards unternehmensweit durchzusetzen.

Mobile Endgeräte stellen dagegen häufig ein sehr persönliches Accessoire und Statussymbol des Besitzers dar, und werden für berufliche wie private Zwecke gleichermaßen genutzt. Viele Mitarbeiter (vor allem auch in der Führungsetage) wollen ihr eigenes Gerät auch am Arbeitsplatz nutzen. Die IT-Abteilungen der Unternehmen haben diesem Wunsch in den letzten Jahren größtenteils nachgegeben, was den Slogan „bring your own device" (BYOD) etablierte. Manche Unternehmen erhofften sich auch Einsparungen dadurch, dass die Mitarbeiter ihre Geräte selbst finanzieren. Diese Einschätzung dürfte sich in vielen Fällen als teurer Irrtum erwiesen haben.[20]

a Externe Angriffe Mit BYOD befinden sich in einem modernen Unternehmen permanent hunderte technisch hoch ausgestattete Endgeräte, über die die firmeneigene IT-Abteilung wenig bis keine Kontrolle hat. Die Besitzer der Geräte können nach eigenem Belieben Software installieren, die häufig von sehr schlechter Qualität ist und Sicherheitslücken aufweist.[21] Außerdem übermitteln die meisten der sogenannten Apps ((zu[22]) viele) Daten an Externe. Darunter können sich auch sensible Unternehmensdaten befinden. Darüber hinaus können Vorsätzlich eingebaute Hintertüren mit sehr wenig Aufwand jederzeit unbemerkt Kamera oder Mikrofon übernehmen und damit mühelos Mitschnitte von vermeintlich vertraulichen Gesprächen an Unbefugte weiterleiten. Genkin, Shamir und Tromer gelang sogar ein erfolgreicher Angriff auf eines der stärksten bekannten Krypto-Systeme (RSA), indem sie mit dem Mikrofon eines auf dem Tisch liegenden Smartphones die Mainboard-Geräusche eines Computers aufzeichneten und analysierten, der gerade kryptographische Berechnungen durchführte.[23] Schließlich haben mobile Geräte ein inhärent höheres Risiko, verloren oder gestohlen zu werden – und mit ihnen alle Daten, die der Besitzer darauf abgespeichert hat.

b Interner Missbrauch Auch im eigenen Unternehmen kann die Funktionalität mobiler Endgeräte missbraucht werden. Mithilfe einer unternehmenseigenen App, zu deren Installation Mitarbeiter aufgefordert werden, können Vorgesetzte mit minimalem Aufwand massenhaft Mitarbeiter überwachen. Bei Geräten, die gleichzeitig beruflich und privat genutzt werden, ist es dabei problemlos möglich, bis in den Kernbereich persönlicher Lebensgestaltung vorzudringen.

[20] Brendel 2013
[21] Dazu IBM 2012 und Fahl 2013.
[22] Wie kürzlich wieder von BayLDA 2014 kritisiert.
[23] Genkin, Shamir und Tromer 2013

c Best-Practices und offene Fragen BYOD schichtet Verantwortung von der IT-Abteilung auf die individuellen Mitarbeiter um. Eine zentrale Empfehlung für die erfolgreiche Implementierung eines BYOD-Programms ist daher, Mitarbeiter für das erhöhte Risikopotential zu sensibilisieren und klare Regeln für die Anforderungen an Geräte, Wartung und Gebrauch aufzustellen.[24] Diese Regeln sollten in schriftlich – am besten im Rahmen einer Betriebsvereinbarung – vereinbart werden.[25]

Eine solche Vereinbarung sollte zumindest folgende Fragen beinhalten:[26]

(i) Welche Geräte sind zugelassen?

(ii) Welche Software darf / muss auf dem Gerät installiert werden?

(iii) Welche Maßnahmen soll der Besitzer ergreifen, um das System sicher und aktuell zu halten?

(iv) Welche beruflichen Tätigkeiten dürfen auf dem Gerät verrichtet werden?

(v) Welche privaten Tätigkeiten sind zu unterlassen?

(vi) Welche Unternehmensdaten dürfen auf dem Gerät gespeichert werden?

(vii) Wie ist das Gerät gegen unbefugten Zugriff zu schützen?

(viii) Was soll der Besitzer beachten, wenn er das Gerät vorübergehend Dritten zur Verwendung überlässt oder sich seiner dauerhaft entledigen möchte?

(ix) Wie ist im Fall eines verlorenen oder gestohlenen Geräts zu verfahren?

(x) Welche Rechte werden der IT-Abteilung eingeräumt, auf das private Gerät zuzugreifen?

Sofern sensible Daten auf dem Gerät verarbeitet werden sollen, werden regelmäßig so hohe Anforderungen zu stellen sein, dass eine private Nutzung desselben Geräts erheblich beeinträchtigt sein wird.[27] Strittig ist, ob eine Verarbeitung personenbezogener Daten auf dem Gerät eines Mitarbeiters als Auftragsverarbeitung iSv § 11 BDSG anzusehen ist.[28]

2 Vernetzte intelligente Mess-, Steuer- und Regelungssysteme

Technische Abläufe werden heute in hohem Maße von IT unterstützt. Dabei kooperieren häufig zahlreiche Sensoren und Aktoren über in Echtzeit (häufig über das Internet) ausgetauschte Informationen. Es sind zwei grundsätzliche Anwendungsfälle zu unterscheiden: Technik, die ein

[24] IBM 2012

[25] Bussche und Schelinski 2013, Rz 468–740

[26] Extrahiert aus den Empfehlungen in IBM 2012 und bei Hammersen und Weißgerber 2014.

[27] Siehe etwa dazu resignativ Hammersen und Weißgerber 2014 zum Einsatz im Medizinbereich (Patientendaten).

[28] ebenda

Unternehmen vertreibt, und Technik, die ein Unternehmen selbst einsetzt. Die Problematik soll hier exemplarisch anhand sogenannter „Smart-Meter“ diskutiert werden.

Klassische Stromzähler summieren laufend den Gesamtverbrauch an elektrischer Energie und speichern lediglich diese Summe ab, die nur sehr selten (zB einmal pro Jahr) manuell abgelesen und protokolliert wird. Um den Strommarkt dynamischer zu gestalten und eine möglichst konstante Nachfrage zu erreichen, wird aktuell erprobt, den dynamischen Strompreis der Börse in Echtzeit an die Endabnehmer weiterzugeben. Dazu setzen diese sogenannte Smart-Meter ein, die den Stromverbrauch im Sub-Sekunden-Takt messen und an den Versorger übermitteln, woraus sich letztendlich der zu zahlende Strompreis errechnet.

Da das moderne Leben stark vom Gebrauch elektrischer Geräte geprägt ist, lassen sich über den Stromverbrauchsverlauf weitreichende Rückschlüsse über das Privatleben einer Person ziehen (Anwesenheit, Tätigkeit, zB Benutzung von Kaffee- oder Waschmaschine, etc), die problemlos bis in den Kernbereich persönlicher Lebensgestaltung vordringen können. Greveler et al konnten anhand einer im 0.5-Sekunden-Takt gesampelten Verbrauchskurve sogar zuverlässig rückschließen, welcher Film in einem Haushalt aktuell gesehen wurde.[29] In derselben Veröffentlichung stellten die Autoren auch fest, dass das untersuchte Gerät nicht einmal rudimentären Sicherheitsanforderungen genügte, und die Daten entgegen der Herstellerbehauptung unverschlüsselt und unsigniert über das Internet verschickte.

Ein Unternehmen, das solche Technologie vertreibt, sammelt (möglicherweise unbedacht) enorme Mengen an brisanten personenbezogenen Daten seiner Kunden, die prima facie nichts mit dem eigentlichen Vertragszweck zu tun haben.

C Externe IT-Dienstleistungen und verteiltes Rechnen

Kaum ein Buzzword wurde in der IT-Welt in den vergangenen Jahren so stark strapaziert wie die „Cloud“. Was sich dahinter verbirgt ist idR ein Marketing-Bluff, der von Anbieter zu Anbieter unterschiedliche Bedeutungen hat.[30] Manche Autoren gehen deshalb so weit, die „Cloud“ als politisch unkorrekten Begriff zu klassifizieren.[31] In jedem Fall ist (ermöglicht durch immer schnellere und zuverlässigere Internetverbindungen) ein klarer Trend in der Software-Welt zu beobachten, Rechenleistung in großen Rechenzentren zu konzentrieren, die von Anwendern über wohldefinierte Schnittstellen über das Internet genutzt wird. Auf den Rechnern der Anwender findet sich lediglich Software, die das aller Nötigste liefert (sog „Thin-Clients“), um zwischen Benutzer und

[29] Greveler et al 2012
[30] Kuppinger 2010
[31] Siehe Eintrag zu „Cloud-Computing“ in FSF 2014.

Rechenzentrum zu vermitteln. Gerade auf mobilen Endgeräten findet sich häufig nur noch sehr wenig Funktionalität und selbst einfache Aufgaben werden auf den Servern der Anbieter berechnet. Weil die Software auf dem Computer des Anwenders die eigentliche Aufgabe nicht berechnen kann, und von dem zentralen Server abhängig ist, werden solche Dienste auch als „software as a service" (SaaS) oder – von Kritikern[32] – als „service as a software substitute" (SaaSS) bezeichnet.

a Vorteile Für den Anbieter bietet SaaS den Vorteil, dass er lediglich die Software für den Thin-Client portieren muss, und das „Arbeitspferd" in seinem Rechenzentrum jederzeit ändern kann. Für den Benutzer hat dies gleichzeitig den Vorteil, dass seine Software einfacher zu installieren und zu warten ist, und weniger Rechenleistung fordert, als eine vollwertige Software. Einer der Hauptmotivationen für Anbieter, Services anzubieten, statt Software zu vertreiben, dürfte aber vertraglicher bzw urheberrechtlicher Natur sein. Während die Rechtsprechung inzwischen etabliert hat, dass auch Software weiterverkauft werden kann[33], ist ein SaaS-Vertrag jederzeit kündbar. Außerdem schließt der Anbieter dadurch, dass er das eigentliche Programm gar nie veröffentlicht, von vornherein aus, dass es illegal vervielfältigt wird.

b Nachteile SaaS birgt allerdings auch einige schwerwiegende Gefahren für den Nutzer:[34]

- Während ein Anwender von proprietärer Software zumindest noch die Möglichkeit hat, das Programm einer Laufzeitanalyse zu unterziehen, zu sandboxen, zu dekompilieren oder auch einfach nur im Notfall abzuschalten, hat ein SaaS-Kunde keinerlei Kontrolle über die Software – er *hat* nicht einmal „die" Software.
- Der Benutzer ist deshalb in hohem Maße vom Anbieter abhängig. Dieser Umstand wird besonders virolent, wenn die Schnittstellen und Datenformate einen Wechsel zu einem Konkurrenzanbieter schwer oder unmöglich machen.
- Der Anbieter erlangt Kenntnis von allen Daten. (Und auch davon, wann und wie die Daten entstanden sind und verarbeitet wurden.) Je nach Art der Daten und Person des Anbieters kann dies sogar rechtlich verboten sein.

[32] Siehe Eintrag zu „Software as a Service" in FSF 2014.

[33] Siehe etwa rückblickend auf einen langen Rechtsstreit Heydn 2014.

[34] Im Wesentlichen nach Stallman 2010; dort auch mit einer guten Abgrenzung von SaaS zu anderen Online-Angeboten.

c SaaS-Verträge Vertraglich zu regeln sind Anforderungen an Datensicherheit und Datenschutz, sowie gegebenenfalls an die geografische Region, in der die Daten gespeichert werden dürfen.[35]

III Fazit

Die fortschreitende Digitalisierung aller Arbeits- und Lebensabläufe hat dazu geführt, dass moderne Unternehmen über komplexe IT-Systeme verfügen, die nicht mehr nur von Spezialisten, sondern von allen Mitarbeitern intensiv genutzt werden. Durch falsche Technologie-Entscheidungen und unbeholfenen Umgang mit IT-Systemen können Mitarbeiter großen Schaden für das Unternehmen verursachen und schwerwiegende Compliance-Verstöße (vor allem bei Datensicherheit und Datenschutz) begehen.

Aktuelle Trends im IT-Sektor bringen für Unternehmen Chancen, bergen bei nicht hinterfragter Übernahme aber auch große Risiken. Der Gesetzgeber geht zu Recht davon aus, dass Unternehmer fundierte Entscheidungen treffen können als Verbraucher, weswegen ihnen die Rechtsordnung mehr Vertragsfreiheit und weniger Schutz vor unfairen Verträgen bietet. Gerade deshalb ist es wichtig, dass ein Unternehmen nicht voreilig jeden neuen Trend adaptiert. Die Vergangenheit hat gezeigt, dass gerade das Internet auch anfällig für Hypes, Blasen und Quacksalber ist.

Gleichzeitig findet ein gesellschaftlicher Wandel statt, der die Grenzen zwischen Berufs- und Privatleben immer weiter verschwimmen lässt. Das stellt zusätzlich neue Anforderungen an Unternehmen und ihre Mitarbeiter, sich in beiden Kontexten regelkonform zu verhalten. Viele Compliance-Verstöße mit IT-Bezug werden nicht bewusst, sondern aus Unbeholfenheit begangen. Hier ist es besonders wichtig, ein Risikobewusstsein bei den Mitarbeitern zu schaffen. Diesen Herausforderungen kann nicht alleine durch Dienstvorschriften und zusätzlichen Klauseln in Arbeitsverträgen begegnet werden. Entscheidend für ein gelungenes Konzept ist, dass alle Mitarbeiter für die Chancen und Risiken moderner Technologie sensibilisiert werden, und verstehen, welche Auswirkungen ihre Entscheidungen haben.

[35] Siehe eher technisch bei Kuppinger 2010 oder eher juristisch bei Bergmann, Moehrle und Herb 2013.

Fallbeispiele

Beispiel 1 (Backdoor[36]): Software-Entwickler *S* entwickelt Computerspiele für Smartphones und vertreibt sie recht erfolgreich für wenig Geld. Für den Multiplayer-Modus verbinden sich die Clients mit einem Server des *S*. Programmierer *P* – ein Mitarbeiter des *S* – stellt fest, dass – aufgrund eines Design-Fehlers – *S*' Mitarbeiter über diese Verbindung die Adressbücher der Kunden auslesen können. Um dies zu ändern müsste *S* die Spiel-Software grundlegend umschreiben lassen, was hohe Kosten verursachen würde. Er versucht *P* davon zu überzeugen, dass die Kunden dies ohnehin nicht merken würden.

Beispiel 2 (Google W-LAN-Mapping[37]): Unternehmen *G* kartographiert flächendeckend W-LAN-Funknetze. Gegen die Kartographierung an sich bestehen keine datenschutzrechtlichen Bedenken. Im Nachhinein stellt sich jedoch heraus, dass die verwendete Software auch Datenfragmente aus dem laufenden Funkbetrieb akkumuliert hat. Hat *G* unrechtmäßig gehandelt?

Beispiel 3 (angelehnt an einen Fall bei Amazon[38]): Chief-Compliance-Officer *C* ist begeistert von dem neuen Buch über regelkonformes Verhalten im Unternehmensbereich. Als Weiterbildungsmaßnahme ordnet er an, dass es für die Mitarbeiter in seinem Unternehmen beschafft wird. Die Einkaufsabteilung kauft daraufhin E-Book-Versionen von Buchhändler *B*. Kurze Zeit später beklagen die Mitarbeiter, dass sie die E-Books nicht mehr lesen können. Die IT-Abteilung kann sich das Problem nicht erklären. Später berichtet die Einkaufsabteilung, dass *B* mitgeteilt habe, er hätte die Bücher „aus rechtlichen Gründen" von den E-Book-Readern der Mitarbeiter löschen müssen. Er bedaure den Vorfall und würde den Kaufpreis umgehend zurückerstatten. Kann sich das Unternehmen des *C* gegen diese Maßnahme wehren?

Beispiel 4 (Renault-Ladehemmung[39]): Kalkulant *K* hat einen neuen Job bei der Firma *F* für innovative Umwelttechnologie angenommen. *F* lebt ein ausgeprägtes Unternehmensleitbild, weswegen alle Mitarbeiter mit öffentlichen Verkehrsmitteln zur Arbeit kommen und nur Elektrofahrzeuge als Dienstwagen angeschafft werden. Leider ist *F* in letzter Zeit finanziell angeschlagen und kann seinen Lieferantenverbindlichkeiten teilweise nicht mehr nachkommen. Glücklicherweise eröffnet sich die vielversprechende Möglichkeit, bei einer öffentlichen Ausschreibung mitzubieten. Aufgrund der angespannten Finanzlage der

[36]Angelehnt an eine Diskussion aus dem Jahr 2012 auf StackExchange:
`https://security.stackexchange.com/questions/15076/i-found-that-the-company-i-work-for-is-putting-a-backdoor-into-mobile-phones`

[37]Die strafrechtlichen Ermittlungen der Staatsanwaltschaft wurden ergebnislos eingestellt. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) verhängte dagegen ein Bußgeld iHv 145 000 € gegen Google. Vergleiche ZD-Redaktion 2013: „Offensichtlich [haben] die firmeninternen Kontrollmechanismen in erheblicher Weise versagt."

[38]2009 löschte Amazon „aus rechtlichen Gründen" Exemplare von George Orwells Büchern „1984" und „Animal Farm" remote von den Kindle-Geräten seiner Kunden, die die Bücher zuvor korrekt bei Amazon erworben hatten. Vergleiche dazu Stone 2009.

[39]Zur dieser Problematik beim Renault *Zoe* siehe gerloff 2013 oder Hucko 2013.

F und weil es sein erstes Projekt ist, vergewissert sich *K* am Vorabend der Angebotseröffnung besonders gründlich, dass sein Firmenwagen an die Ladesteckdose angeschlossen ist. Umso entsetzter ist er, als das Fahrzeug am nächsten Morgen eine leere Batterie anzeigt und sich nicht starten lässt. In seiner Not bittet er seinen Kollegen, ihm dessen Firmenwagen zu leihen, doch dieser hat dasselbe Problem. Da *K* auf die Schnelle kein Taxi für die weite Fahrt bekommt, schafft er es nicht mehr, das Angebot rechtzeitig abzugeben und *F* entgeht der Auftrag. Später erfährt *K*, dass der Autohändler die Ladefunktion der Firmenwagen remote deaktiviert hat, weil *F* die Leasingraten nicht beglichen hat.

Beispiel 5 (SCO gegen IBM, Novell, Red Hat et al[40]): Software-Unternehmen *S* ist der Meinung, dass einige seiner Mitbewerber sein Urheberrecht verletzt haben. Da *S* gegen die Mitbewerber direkt keinen schnellen gerichtlichen Erfolg erzielt, sendet es an die Kunden seiner Mitbewerber Warnungen, dass sie illegale Software benutzen. Zahlreiche Kunden sind dadurch irritiert und erwägen einen Produktwechsel. Da *S* im Laufe des weiteren Rechtsstreits insolvent wird, wird die Frage nie abschließend geklärt.

Beispiel 6 (Heartbleed und Android): Softwarekonzern *G* entwickelt und vertreibt ein mobiles Betriebssystem, dessen Bestandteile teilweise übernommen und teilweise selbst entwickelt sind. Eines davon ist die Kryptographie-Bibliothek *B*. *B* ist freie Software und kann von *G* unter geringen Auflagen gratis verwenden werden. Welche Mitverantwortung trägt *G* an der Qualität von *B*?

[40]Für eine – nicht allzu gute – Zusammenfassung zu diesem langen und verworrenen (Rechts-)streit, siehe Wikipedia 2014.