Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag Magdeburg

Dieser Artikel erscheint in der Serie „Informationstechnik und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?“ Herausgegeben von Jörg Sambleben und Stefan Schumacher

Datenschutz, IT-Sicherheit, Betriebsschutz: Unternehmensentscheidungen zwischen gesetzlichem Zwang und betrieblicher Notwendigkeit

Robert Kudrass

Dieser Artikel setzt sich mit dem Risiko des Datendiebstahls über Firmennetzwerke auseinander und wie Konzerne immer wieder Opfer von Hackerangriffen werden. Ein angemessenes Datensicherheitssystems kann über die Firmenexistenz entscheiden.

.

Zitationsvorschlag: Kudrass, Robert (2011). Datenschutz, IT-Sicherheit, Betriebsschutz: Unternehmensentscheidungen zwischen gesetzlichem Zwang und betrieblicher Notwendigkeit. Magdeburger Journal zur Sicherheitsforschung, Band 2, 2011, S. 84–101.
http://www.wissens-werk.de/index.php/mjs/article/view/106/76

I. Einleitung

Als Anfang April 2011 bekannt wurde, dass Sonys Playstation Netz sowie Video- und Musikdienst von Hackern geknackt wurde,[1] sollte das für den japanischen Konzern empfindliche Folgen haben. So verzeichnete Sony sowohl direkte Umsatzausfälle durch das zeitweise Aussetzen seines Dienstes und hatte zeitgleich mit einem Reputationsverlust zu kämpfen.[2] Ein Beispiel, das nicht nur verdeutlicht, wie schnell Ruf und Umsatz eines Unternehmens von seiner IT-Sicherheitsstruktur abhängen können, sondern auch wie verwundbar selbst gut aufgestellte Branchenriesen sein können. Der Diebstahl von Kundendaten durch einen externen Angreifer ist die in der Öffentlichkeit und von den Unternehmen selbst wohl am stärksten wahrgenommene Gefahr.[3] Der Angreifer verschafft sich in solchen Fällen technisch einen Zugriff auf die Datenbank des betroffenen Unternehmens, auf der personenbezogene Kundendaten lagern und bemächtigt sich der Kundendaten, die, je nach Datenbankaufbau, auch Zahlungsdaten oder besonders schützenswerte personenbezogene Daten enthalten. Damit kann das grundlegende Vertrauensverhältnis und Sicherheitsempfinden zwischen Kunde und Unternehmen gestört werden. Gleichzeitig stellt sich die Frage, wie sich Datenpannen auf das gesellschaftliche Sicherheitsgefühl auswirken. Unternehmen, die mehrere Millionen personenbezogener Daten halten, beeinflussen zudem das soziale Vertrauen in die Sicherheitsstrukturen einer Gesellschaft. Dies wiederum bewirkt Rückkopplungen auf die Gesetzgebung, die Unternehmen zur Einhaltung hoher Datenschutzstandards auffordert.

Auch wenn sich das obige Beispiel von Sony auf einen großen Internetentertainmentanbieter bezieht, sind heute beinah alle Unternehmen durch moderne IT-Infrastruktur so vernetzt, dass diese auch Opfer eines Angriffs werden können. Fast jedes Unternehmen muss sich den Herausforderungen des Datenschutzes, der Datensicherheit bzw. IT-Sicherheit[4] stellen – unabhängig davon, ob es einer Branche der so genannten „old economy" oder der IT-Branche angehört.[5] Die Höhe des Firmenwerts, ja sogar die Firmenexistenz hängen direkt oder indirekt vom praktizierten Datensicherheitssystem ab, da in einer immer spezialisierteren Wirtschaftsstruktur Daten und Informationen eine eigene zentrale wenn auch immaterielle Unternehmensressource sind. Neben den Kundendaten gehören auch die betriebssensiblen Daten zu eben diesen immateriellen Unternehmensressourcen. Auch diese können zum Angriffsziel werden.

1 Siehe dazu bspw.: Reißmann, O., Lischka, K., Breithut, J. (2011). Angriff auf Playstation-Netz. Weckruf für Sonys Spielerheer. http://www.spiegel.de/netzwelt/web/a-759220.html (27.04.2011).

2 Der Datendiebstahl hat Sony laut Spiegel 1,2 Mrd. EUR gekostet und zu einem Vertrauensverlust bei den Kunden der Playstation-Anwendungen geführt. Spiegel-Online (23.05.2011). Elektronikriese in Nöten. http://www.spiegel.de/wirtschaft/unternehmen/0,1518,764261,00.html (23.05.2011). Siehe auch: Sony Corporation (2011). Consolidated Financial Results for the First Quarter Ended June 30, 2011. http://www.sony.net/SonyInfo/IR/financial/fr/11q1_sony.pdf (04.08.2011), S.3.

3 Weiss, S., Fritzsche T. (2010). Forensic. e-Crime-Studie 2010. Computerkriminalität in der deutschen Wirtschaft. Risk & Compliance, S.9f. http://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf (14.08.2011).

4 Zur Definition siehe z. B.: Rieger, H., IT-Sicherheit – Risiken und Gefährdungspotenziale, in: Rieger, H., Schoolmann, J. (Hrsg.) (2005). Praxishandbuch IT-Sicherheit: Risiken, Prozesse, Standards, S.23. „IT-Sicherheit meint das Ausbleiben unbefugter Zugriffe oder Schädigungen der IT-Systeme und der auf ihnen gespeicherten Daten."

5 Die Begrifflichkeit „new economy" und „old economy" sind meines Erachtens hinfällig, da die Nutzung moderner datenverarbeitender Systeme in den klassischen Dienstleistungs- und Industriesektor integriert wurden bzw. werden.

In einer Wirtschaftsstruktur, in der das Endkundengeschäft (B2C) immer stärker die personalisierte Kundenansprache via E-Mail, Social Media Tools und mobilen webfähigen Endgeräten (z. B. Smartphones) hervortritt, tritt auch der Datenschutz ins Interessenzentrum der Kunden, Verbraucherschützer und der staatlichen Kontrollorganisationen. In einer Wirtschaftsstruktur, in der innerbetriebliche Prozesse immer mehr automatisiert werden, Unternehmenseinheiten mit einander umso enger vernetzt sind und Unternehmensressourcen immaterieller Art immer wichtiger, kommt der innerbetrieblichen Informations- und IT-Sicherheit eine zentrale Bedeutung zu. In einer Wirtschaftsstruktur, in der zwischen Unternehmen (B2B) Daten zur Bearbeitung oder Speicherung weitergereicht werden, rückt auch die Verifizierung der Datensicherheitsstrukturen des jeweiligen Partners ins Blicklicht des eigenen Unternehmens.

II. Sphären der unternehmensbezogenen Datenflüsse

Unabhängig davon, ob ein Wirtschaftsunternehmen im B2C oder B2B Bereich tätig ist, muss es in wechselseitiger Beziehung zu dessen Kunden treten. Diese Sphäre soll im Folgenden als „Kundenkontaktsphäre" bezeichnet werden. Um die Bedürfnisse seiner Kunden wiederum zu erfüllen und eingehende Aufträge zu bearbeiten, bedarf es innerbetrieblicher Prozesse, die durch technische Systeme und Mitarbeiter durchgeführt werden.[6] In dieser „innerbetrieblichen Sphäre" obliegt es dem Unternehmen selbst, Sorge für die IT-Sicherheit und der Durchsetzung des Datenschutzinteresses seiner Kunden (und Mitarbeiter[7]) zu sorgen. Für die Verarbeitung von Kundenprozessen bedienen sich Unternehmen dazu oft weiterer Dienstleister und lagern abgrenzbare Teilprozesse an andere Firmen aus (z. B. Fulfillment, Inkasso etc.). Das Unternehmen entscheidet hierbei selbst, inwieweit solche Beziehungen eingegangen werden. Diese Beziehungen bilden die intrabetriebliche Sphäre, die dadurch charakterisiert ist, dass die eigentliche Aufgabenerfüllung vom Unternehmen zwar definiert, aber in einem anderen Unternehmen umgesetzt wird. Da das Drittunternehmen (Dienstleister) i.d.R. keine direkte Vertragsbeziehung zum Kunden seines Auftraggebers unterhält, sind dessen Anreize für die Einhaltung des Kundendatenschutzes und die IT-Sicherheit des Auftraggebers stark durch die Anforderung eben des Auftraggebers bestimmt. Damit muss das auftraggebende Unternehmen neben den eigentlichen Aufgaben auch das Sicherheitsinteresse gegenüber dem Dienstleister definieren und durchsetzen.

Aus den Wechselbeziehungen zwischen Kunde und Unternehmen ergeben sich zudem rechtliche Erfordernisse sowie branchenspezifische Standards zur Daten- und IT-Sicherheit, die einzuhalten sind. Daraus resultieren letztendlich Berichts- oder Prüfpflichten gegenüber Kontrollorganisationen (Aufsichtsbehörden bzw. nichtöffentlichen Prüfstellen). Diese Sphäre soll hier als „Kontrollsphäre" bezeichnet werden. Wie bei der „intrabetrieblichen Sphäre" besitzt die externe Organisation keine Vertragsbeziehung zum eigentlichen Kunden. Die „intrabetriebliche Sphäre" und die Kontrollsphäre sollen hier unter dem

6 Von den klassischen drei Produktionsfaktoren sind für diese Betrachtung der Faktor Arbeit und der Faktor Kapital zu beachten.

7 Zu den aktuellen Entwicklungen im Bereich Personaldatenschutz, auf das hier nicht näher eingegangen werden soll, siehe: Beckschulze, M., Natzel, I. (2010). Das neue Beschäftigtendatenschutzgesetz. Eine Darstellung des aktuellen Gesetzentwurfs vom 25.8.2010. Betriebs Berater (39/2010), S. 2368–2375.

Begriff „Drittsphäre“ zusammengefasst werden.

a) Schutzaufgaben in der „Kundenkontaktsphäre“

Von den genannten Sphären ist die „Kundenkontaktsphäre“ die sensibelste, wenn Angebots- und/oder Kaufabwicklung über elektronische Medien durchgeführt werden (vor allem im E-Commerce-Geschäft). Ausschlaggebend sind sowohl die technischen und organisatorischen Maßnahmen zur korrekten Übermittlung von Angebotsdaten auf der einen als auch die personenbezogenen Käuferdaten auf der anderen Seite. Ebenso müssen die einschlägigen rechtlichen Bestimmungen, welche es bei der Datenübertragung durch den Anbieter einzuhalten gilt, beachtetet werden. Das Bundesdatenschutzgesetz (BDSG) gehört hierbei zu den wichtigsten und bekanntesten Rechtsnormen. Daneben sind das Telemedien- (TMG) und das Telekommunikationsgesetz für E-Commerce Anbieter maßgeblich[8] für den elektronischen Geschäftsverkehr.

Das BDSG zielt auf den Schutz der informationellen Selbstbestimmung des Kunden (als natürliche Person) gegenüber dem Anbieter.[9] Aus seiner Gestaltung heraus bewirkt das BDSG ein Schutzprogramm[10], welches durch den E-Commerce Anbieter gegenüber seinen Kunden einzuhalten ist. Es regelt die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung und bindet diese an einen konkreten Zweck.[11] Weiter regelt es die Informationspflichten bzw. Betroffenenbenachrichtigung[12] gegenüber dem Kunden und soll ihm die Transparenz bezüglich dem Zweck seiner überlassenen Daten sichern. Nicht zuletzt entfaltet das BDSG Korrektur-, Änderungs- und Löschrechte für den betroffenen Kunden[13]. Mit dem Telemediengesetz (TMG) wird der Rahmen für die kommerzielle Kommunikation mit audiovisuellen, elektronischen Informations- und Kommunikationsdiensten abgesteckt[14], welche nicht unter Telekommunikation oder Rundfunk fallen (z. B. E-Mail-Marketing).

Das Telekommunikationsgesetz (TKG) regelt letztlich den technischen Übermittlungsvorgang und beinhaltet ebenso einen Abschnitt zum Datenschutz.[15]

Auf Basis dieser Rechtslage[16] muss der Anbieter Kenntnis über seine IT-Struktur und seine Software haben, noch bevor er seinen potenziellen Kunden sein Angebot elektronisch darbietet. Nur wenn die verantwortlichen Personen eines Unternehmens die eingesetzte Technik zur Datenübermittlung zwischen Kunde und Unternehmen kennen, können sie den Informationspflichten nachkommen sowie die Daten, die für die Leistungserfüllung notwendig sind und für die der Kunde seine ausdrückliche Erlaubnis gegeben hat, erheben.

8 Auf einzelne Regelungen aus dem Gesetz gegen unlauteren Wettbewerb (UWG), dem Einführungsgesetz zum Bürgerlichen Gesetzbuch (EGBGB) und dem Bürgerlichen Gesetzbuch (BGB) soll hier der Einfachheit halber nicht näher eingegangen werden.

9 §1 Abs. 1 BDSG.

10 Vgl. Rossnagel, A. (2006). Datenschutz im 21. Jahrhundert. Aus Politik und Zeitgeschichte (APuZ), 5–6/2006, S. 10.

11 §§ 4, 4a BDSG.

12 §§ 6c, 33, 34, 42a BDSG.

13 § 35 BDSG.

14 §§ 1 Abs. 1, 2 Abs. 5 TMG.

15 §§ 91–107 TKG.

16 Eine tiefergehende, wenn auch durch die aktuelle Entwicklung in Teilen überholte, Betrachtung der rechtlichen Aspekte bietet Knupfer, J. (2005). Rechtliche Grundlagen der IT-Sicherheit, in: Rieger, H., Schoolmann, J. (Hrsg.) (2005). Praxishandbuch IT-Sicherheit: Risiken, Prozesse, Standards, S. 27–52.

b) Schutzaufgaben in der „innerbetrieblichen Sphäre“

Sind die Daten eines Kunden an die Server des Unternehmens einmal übermittelt worden, tritt die innerbetriebliche Sphäre in den Vordergrund. Das Unternehmen ist nun „Sachwalter“ der überlassenen personenbezogenen Daten. Es hat diese so zu speichern, zu verarbeiten und ggf. weiterzureichen, wie es das Kundeneinverständnis dazu bekommen hat. Zudem muss es die Möglichkeit vorhalten, diese Daten zu berichtigen oder auf Anforderung zu löschen bzw. für den weiteren innerbetrieblichen Zugriff zu sperren.[17] In der Theorie scheint dies einfach und nachvollziehbar. In der Praxis gestaltet sich der innerbetriebliche Ablauf aufgrund der vielfältigen technischen und organisatorischen Möglichkeiten als besondere Herausforderung. Immerhin müssen, wie weiter unten gezeigt werden wird, Mitarbeiter eingewiesen, die technischen Systeme angemessen aufgebaut sowie auf Stand gehalten und gewartet werden und zudem die Betriebsräume an die Erfordernisse des Datenschutzes angepasst sein.

Innerhalb des Unternehmens geht es jedoch um mehr als den Schutz der personenbezogenen Kundendaten. Gewiss sind Kundendaten vor allem für Unternehmen im Massengeschäft ein zentrales Asset. Doch wer mit geeigneten Mitteln und Methoden Kundendaten gut schützt, kann auch andere unternehmenssensiblen Daten, Systeme und Netze sicher behandeln. Dieser innerbetriebliche Bereich ist bestimmt durch die Informations- bzw. IT-Sicherheit. Während der Datenschutz auf den Schutz der informationellen Selbstbestimmung abzielt, agiert die IT-Sicherheit in einem breiteren Rahmen. Sie muss gewährleisten, dass IT-Systeme, die mit bestehenden Unternehmenswerten verknüpft sowie an laufende Geschäftsprozesse verbunden sind, auch ausreichend abgesichert sind. Je stärker die Integration von IT-Systemen in die Geschäftsprozesse ist, desto mehr muss die innerbetriebliche IT-Sicherheit Gefahrenpotenziale erkennen und wirksame Schutzmaßnahmen in den betroffenen Geschäftseinheiten entfalten. Neben dem Kundendatenschutz sollte somit in der „innerbetrieblichen Sphäre“ der IT-Sicherheit folgenden Feldern besondere Aufmerksamkeit zukommen:

- Erfüllung der zentralen produktiven Unternehmensaufgaben, die durch IT-Systeme gestützt werden
- Schutz der immateriellen Unternehmenswerte (z. B. Quellcodes, Lizenzen, Markenrechte etc.)
- Schutz der materiellen Unternehmenswerte (z. B. der Server, Router, Rechner oder weiterer angebundener Produktivsysteme)
- Schutz betriebssensibler Daten (Mitarbeiterdaten, buchhalterische Daten)
- Sicherstellung einer ausreichenden und aktuellen Dokumentation

Mit diesem Aufgabenbündel, das die IT-Sicherheit in einem Unternehmen bewältigen muss, obliegt es den jeweiligen Verantwortlichen die geeigneten Schutzmaßnahmen zu definieren, umzusetzen und dauerhaft auf aktuellem Stand zu halten.

c.) Schutzaufgaben in der „Drittsphäre“

Hat die eigene IT-Sicherheit in der „innerbetrieblichen Sphäre“ den Vorteil, zeitnah Zugriff und Zugang zu den eigenen vorhandenen Systemen und Netzen zu be-

17 Der Gesetzgeber sieht eine Sperrung u. a. dann vor, wenn der Löschung bestimmte Aufbewahrungsfristen entgegenstehen. Mit einer Sperrung haben die Mitarbeiter nur dann Zugriffsrecht auf die betroffenen personenbezogenen Daten, wenn dies im gesetzlichen Zweck nach §20 Abs. 3 BDSG begründet liegt.

kommen, so stellen sich die weiteren Herausforderungen in der „intrabetrieblichen Sphäre". Als Teil der „Drittsphäre" kann die „intrabetriebliche Sphäre" erhebliche Probleme für ein Unternehmen bereiten. Werden Kundendaten im Sinne der Auftragsdatenverarbeitung an ein Drittunternehmen weitergereicht, steht trotzdem die Firma in der Verantwortung für den Datenschutz, die den ursprünglichen Kundenauftrag entgegengenommen hat. Sie muss sich darüber vergewissern, ob das Unternehmen, an das es die Daten weitergibt, auch die organisatorischen und technischen Sicherheitsbestimmungen erfüllt, die es selbst einhalten muss oder will. Neben der Kundendatenverarbeitung durch externe Dienstleister kommen Drittfirmen, gewollt oder ungewollt, in verschiedenster Art Zugriff auf unternehmenssensible Daten – sei es im Zuge regulärer Wartungsarbeiten an IT-Systemen, sei es im Zuge der Auftragsdatenverarbeitung bei bestimmten Geschäftsprozessen oder schlicht durch Unachtsamkeit. Verträge zwischen zwei oder mehreren Firmen sind schnell unterzeichnet. Auch die Kostenkalkulation, die gegen die Ausführung eines bestimmten datenverarbeitenden Prozessschrittes im eigenen Unternehmen spricht, ist schnell berechnet. Doch ob das externe Unternehmen die geforderten Sicherheitsstandards einhält, ist nicht immer einfach nachzuvollziehen. Vor diesem Hintergrund wundert es nicht, dass Datenskandale großer, bekannter Firmen nicht selten eben von Partnerunternehmen und Dienstleistern hervorgerufen wurden. Eine immer wieder zu Tage tretende Folge ist die Markenschädigung des Auftraggebers, während der Auftragnehmer bzw. Dienstleister in den Medien kaum erwähnt wird oder schnell in das Dunkel des Vergessens gerät.[18]

Wie oben angedeutet, ist die „Kontrollsphäre" ebenfalls ein Teilbereich der „Drittsphäre". In den Bereich der „Kontrollsphäre" fallen alle Handlungen im Unternehmen, welche externen Organisationen zu Kontroll- und Nachweiszwecken dienlich sind. Der eigentliche Arbeitsauftrag, der in der Darlegung und Nachweisführung über anforderungskonforme Abläufe besteht, wird in der „Kontrollsphäre" von der kontrollierenden Organisation definiert und dem Unternehmen aufgezwungen. Klassisches Beispiel für die „Kontrollsphäre" ist die Betriebsprüfung durch das zuständige Finanzamt. Für die IT-Sicherheit und den Datenschutz relevante Kontrollen sind behördliche Datenschutzaudits, Wirtschaftsprüfungsaudits, Audits von Zertifizierern im Bereich Datenschutz bzw. -sicherheit[19], behördliche Einzelfallanfragen (z. B. im Fall einer Strafverfolgung) oder Reportingpflichten gegenüber bestimmten auftraggebenden Unternehmen, welche ihre Sicherheitsstandards auf den Auftragnehmer ausweiten müssen oder wollen. Folglich ergibt sich die Notwendigkeit der bewussten

18 Beispielhaft ist die Weitergabe von Kundendaten an externe Callcenter, die nur über mangelhafte Sicherheitsstrukturen verfügen. Immer wieder im Licht der Öffentlichkeit ist dabei die Deutsche Telekom: Thieme, M. (2011). Neue Datenpanne bei der Telekom. http://www.fr-online.de/politik/spezials/datenschutz/neue-datenpanne-bei-der-telekom/-/1472644/2722902/-/index.html (28.08.2011).

19 Einen Überblick über die IT-Sicherheitsstandards findet sich in: BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., DIN Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik und Anwendungen (NIA) (Hrsg.) (2009), Kompass der IT-Sicherheitsstandards. Leitfaden und Nachschlagewerk, 4. Auflage (2009).

Bereithaltung einer ordnungsgemäßen Dokumentation für diese Organisationen. Da in einem Unternehmen, in dem IT-Systeme sehr starken Anteil an den Geschäftsprozessen haben, Dokumentationen zu den verwendeten IT-Systemen auch im stärkeren Maße verschiedenen Unternehmenseinheiten zur Verfügung stehen müssen, muss auch der Zugriff auf diese effektiv gestaltet sein. Ist dies nämlich nicht gegeben, können Verantwortliche der betroffene Unternehmenseinheiten, im Fall einer externen Kontrolle, kaum valide Angaben machen und somit im schlechtesten Fall die geforderten Ansprüche nicht erfüllen.

Ausschlaggebend für die Einschätzung, wie der Schutz sensibler Daten organisiert werden kann, ist, in welcher der oben genannten Sphären IT-Systeme zur Datenverarbeitung verwendet werden und wie stark deren Durchdringung für die jeweiligen Geschäftsprozesse sind. Anhand dieser Betrachtung kann sich eine konkrete Risikoanalyse anschließen.

III. Risikoanalyse

Datenverarbeitende Unternehmen unterliegen der Gefahr, dass ihre Daten gestohlen, ungewollt verändert, unsachgemäß behandelt werden oder nicht zeitgerecht verfügbar sind. Das Risiko, Opfer eines Angriffs oder einer technischen Störung zu werden, ist in komplexen Systemen, wie sie etwa stark vernetzte Unternehmen darstellen, außerordentlich hoch. Risiko ist immer die Relation zwischen Ereigniseintrittswahrscheinlichkeit und Schadenshöhe bei Eintritt des Ereignisses. Jedes Unternehmen muss sich daher die Frage stellen, welche Schwachpunkte in den eigenen Prozessabläufen bestehen und welche Schadensszenarien sich daraus ergeben können. Bezüglich der erkannten Risiken muss eine Strategie definiert werden, die präventive Maßnahmen zur Risikomeidung oder zumindest Risikominderung benennt. Die Führungsebene eines Unternehmens muss die innerbetrieblichen Prozesse, die Lage des Unternehmens am Markt, aber auch scheinbar banale Dinge wie die räumliche Lage des Unternehmens und der einzelnen Untergliederungen kennen und verstehen, um daraus resultierende Risiken für die Informationssicherheit zu bewerten. Das ist Teil des Risikomanagements. Ein effektives Risikomanagement beurteilt die Gefahrenquellen, die durch IT-Systeme entstehen können. Werden Risiken nicht ausgeschlossen, muss die Strategie bei Eintritt eines Schadenfalls Mittel und Wege fixieren, die die Schadenshöhe soweit wie möglich begrenzen. Verbleibende Restrisiken müssen dann im Schadensfall durch das Unternehmen getragen werden.[20] In den folgenden Ausführungen sollen die wichtigsten Risiken betrachtet werden, die in den einzelnen Sphären für ein Unternehmen auftreten können.

a) Risikoanalyse für die „Kundenkontaktsphäre“

Zu weitgehende Datenerfassung, mangelnde Datenverschlüsselung, unzureichende Informationen zum Datenschutz, unzulässige Datenweitergabe – so lassen sich die Schwerpunktrisiken für die „Kundenkontaktsphäre“ zusammenfassen.

Eine Vielzahl von gesetzlichen Regelungen und Urteilen geben für den Onlinehandel mit Endkunden die Richtlinien bezüglich

20 Zu Definition der Begrifflichkeiten im Risikomanagement siehe: ebd., S. 29f. Risikomanagement wird dort als „Führungsprozess zur Bewältigung der in einer Unternehmung entstehenden Risiken“ verstanden. Damit wird deutlich, dass auch die Risiken, die im Rahmen der IT-Sicherheit und des Datenschutzes benannt werden, den Führungsverantwortlichen eines Unternehmens klar sein sollten und die Unternehmensführung die Haftung im Schadenfall zugewiesen werden kann.

korrekter Kundeninformation und Kundenunterrichtung vor. Neben Impressumspflicht, rechtskonformer AGB und korrekter Preisangaben spielt die Datenschutzerklärung eine herausragende Rolle[21]. Sie ist überall dort gefordert, wo der Dienstanbieter Daten vom User (nicht nur dem Käufer) erfasst. Diese Datenerfassung betrifft z. B. IP-Adressen[22]. Werden diese ungekürzt erfasst und gespeichert ohne dass der User sein Einverständnis dazu gegeben hat, liegt ein Rechtsverstoß vor. Ebenso verhält es sich bei anderen personenbezogenen Daten, die nicht zur Erfüllung des unmittelbaren Auftrages dienen. Ein bekanntes Beispiel ist die Datenweitergabe an Soziale Netzwerke wie Facebook oder Google+. Wer Facebooks „Like-Button" (in der deutschen Sprachversion „Gefällt mir") einbindet, sollte in der Datenschutzerklärung daraufhin hinweisen.[23] Auch die Integration von Werbebannern von Drittfirmen birgt datenschutzrechtliche Risiken, wenn Daten (z. B. die IP-Adresse) zum Klickverhalten an diese weitergeleitet werden ohne ein entsprechendes Einverständnis dokumentiert zu haben. Eine der jüngsten Formen der Datenerfassung ist die Geodatenerfassung. Diese erfolgt über mobile Endgeräte (Smartphones, Laptops oder Navigationsgeräte) und soll dem User ortsabhängig Produkt- und Dienstleistungsangebote zur Verfügung stellen. Auch Geodaten zählen zu den personenbezogenen Daten, womit die Einwilligung des Users für solche Dienste zwingend ist. Die wohl größten Einfallstore bieten jedoch immer noch sogenannte Tracking Tools. Diese analysieren das Besucherverhalten auf einer Website, um dem Internetanbieter die Möglichkeit zu geben, seine Angebote im Netz zu optimieren. Ein Tracking Tool, wie Google Analytics, webtrekk oder eTracker wird in den Quellcode der Website integriert. Mit Hilfe von Cookies, die im Browser des jeweiligen Users abgelegt werden, wird dann eine Verbindung zwischen den Servern des Tracking Tool Anbieters und dem Kundenrechner hergestellt und dabei die relevanten Daten übermittelt. Werden diese Cookies nicht gelöscht oder verfallen nach kurzer Zeit nicht automatisch, findet ein dauerhafter Datenstrom zwischen dem User und dem Tracking Tool Anbieter immer dann statt, wenn der User die Website des Onlineanbieters aufsucht. Über diese Tracking-Anwendungen ist daher eine Unterrichtung des Users im Vorab nicht möglich. Dieser muss schließlich erst die Seite besuchen, um überhaupt mitgeteilt zu bekommen, dass Trackingtools sein Surfverhalten analysieren. Auch hier sind Informationen zum Tracking Tool in der Datenschutzerklärung rechtlich zwingend[24] und IP-Adressen der User sollten nur gekürzt erfasst werden.

21 Seit 2009 wurde das BDSG durch drei Novellen präzisiert, die vor allem auf den Onlinehandel Auswirkungen haben. Die Novellen regeln die Weitergabe von Kundendaten zu Scoringzwecken (Bonitätsprüfung) und die Übermittlung von Negativdaten sowie die Informationspflicht gegenüber den Aufsichtsbehörden bei unrechtmäßiger Weitergabe von personenbezogenen Daten.

22 Die Frage, ob eine ungekürzte, feste IP-Adresse ein personenbezogenes Datum ist oder nicht, war lange Zeit in der Diskussion. Die Rechtssprechung tendiert seit kurzem dazu, diese den personenbezogenen Daten hinzuzurechnen.

23 Mangelhafte Datenschutzerklärung zu Facebooks Like Button sind nach aktuellem Stand der Rechtsprechung nicht wettbewerbswidrig und damit nicht abmahnfähig. Jedoch liegt ein Verstoß gegen das TMG und das BDSG vor. Dagegen wiederum können die entsprechenden Aufsichtsbehörden einschreiten. Solmecke, C. (2011). Urteil zum Like Button. LG Berlin entscheidet über Wettbewerbswidrigkeit / Fragen zum Datenschutz bleiben offen. Internet World Business (7/2011), S. 45. Siehe auch: Lischka, K. (2011). Like-Button. Datenschützer nennen Facebookpraxis rechtswidrig. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,782939,00.html (28.08.2011).

24 Weiterhin muss dem User in der Datenschutzerklärung eine Möglichkeit genannt werden, wie er einer Datenweitergabe wirksam widersprechen kann.

Für die eigene Datenerfassung sollte schon im Vorab geklärt sein, welche Angaben für die Auftragserfüllung unbedingt notwendig sind und welche freiwillig durch den Kunden eingegeben werden können. Dieser Prozess kann nur in enger Abstimmung zwischen i.d.R. dem Marketingbereich, der IT (die die dahinter liegenden Datenbanken sowie den entsprechenden Quellcode aufsetzen muss) und dem Datenschutzbeauftragten erfolgen. Nur so kann das Unternehmen sicherstellen, dass alle daran beteiligten Unternehmensbereiche für den notwendigen Datenschutz sensibilisiert sind. Ein weiterer Vorteil der Einbindung des Datenschutzbeauftragten liegt, wie auch weiter unten noch gezeigt werden wird, darin, dass eine Vorabkontrolle des datenerfassenden Systems durch den Datenschutzbeauftragten leichter dokumentiert werden kann.

Werden die Angaben in der Datenschutzerklärung nur unvollständig hinterlegt, besteht das Risiko der Ordnungswidrigkeit und der Abmahnung durch Wettbewerbszentralen oder Wettbewerber.

Ein weiterer Risikofaktor liegt in der Übertragung von besonders personenbezogenen Kundendaten oder Zahlungsdaten an die Server des Unternehmens. Ist die Verbindung nicht verschlüsselt[25], können diese Daten durch Dritte abgefangen werden. Als Folge sind Haftungsforderungen an das Unternehmen möglich – wenn auch die Schadenszuordnung durch den einzelnen User sehr schwer nachweisbar wird. Zumindest liegt bei mangelnder Verschlüsselung aber eine Fahrlässigkeit des Unternehmens vor, die ggf. durch Aufsichtsbehörden oder Drittunternehmen (z. B. Zahlungsdienstleister) geahndet werden können[26].

Im Nachgang an den erteilten Kundenauftrag lauern weitere Risiken. Eines liegt in der Kontaktaufnahme des Kunden zum Unternehmen. Wird bei einer aktiven Anfrage durch einen Kunden an das Unternehmen die richtige Identität des Anfragenden nicht eindeutig abgeklärt, besteht die Gefahr, dass Mitarbeiter Kundendaten ohne Legitimation herausgeben. Eine Legitimationsabfrage durch Identitätsnachweis (z. B. durch Abfrage von Kundennummer, Kundenname und Bestelldatum) sollte deshalb für jeden Kundendienstmitarbeiter verpflichtend sein. Hier kommt es oft zum Spannungsfeld zwischen Kundenfreundlichkeit und Barrierefreiheit einerseits und dem Datenschutz andererseits. Begegnen lässt sich dieses im Konfliktfall nur, wenn man dem jeweiligen Kunden die Schutzwürdigkeit seiner Daten darlegt.

Fallschlingen im Kontaktaufbau vom Unternehmen an dem Kunden liegen besonders im Bereich Aftersales. Ist die Versendung von E-Mails, die den Status der Auftragsbearbeitung werbefrei mitteilen, unkritisch[27], sind Aktionsangebote über Newsletter, SMS oder Postsendungen nur mit nachvollziehbarer Kundeneinwilligung möglich, da diese mit der eigentlichen Auftragserfüllung, für die die personenbezogenen Kundendaten übermittelt wurden, nicht mehr in Verbindung stehen. Eine Risikoverquickung von wettbewerbsrechtlichen Abmahnungen, Ordnungswidrigkeitsstrafen und ggf. Einordnung der Versenderadresse in die Black Lists der E-Mail

25 Diese kann durch eine SSL-128 Bit oder SSL-256 Bit Verschlüsselung realisiert werden.

26 Bei der Speicherung oder Durchleitung von Kreditkartendaten müssen z. B. die Payment Card Industry Data Security Standards (PCI DSS) eingehalten werden. Details zu diesem Regelwerk sind aufgeführt in: PCI Security Standards Council LLC (2010). Payment Card Industry (PCI) Datensicherheitsstandard. Anforderungen und Sicherheitsbeurteilungsverfahren. Version 2.0.

27 Dies ist der Fall, wenn ein Anbieter den Kunden über den Arbeitsstand seiner jeweiligen Bestellung informiert.

Provider (die versendeten E-Mails werden dann als Spam gewertet und erreichen einen geringeren Kundenanteil mit dem Ergebnis von Umsatzseinbußen) sind die drohende Folge. Letztlich kann der Firmenruf durch Kundenreaktionen in sozialen Netzwerken und Blogs noch angegriffen werden.

b) Risikoanalyse für die „innerbetriebliche Sphäre"

Das Gefährdungspotenzial in einem Unternehmen ist bedingt durch seinen jeweiligen strukturellen Aufbau äußerst vielfältig und komplex. Die wichtigsten Determinanten für eine Risikoanalyse liegen in:

1. den vorhandenen physikalischen Schutzmaßnahmen,
2. Art und Umfang der verwendeten Technik,
3. den Verfügbarkeitsanforderungen an die genutzten Systeme,
4. der Anzahl und dem Kenntnisstand der Mitarbeiter,
5. der unternehmenseigene Sicherheitskultur der Mitarbeiter.

Sich daraus ergebende Gefahrenszenarien sind:

- Opfer eines internen oder externen Angriffes auf seine Datenressourcen und die eigene IT-Infrastruktur zu werden,
- Opfer eines Sabotageaktes auf die Datenressourcen und gegen die eigene IT-Infrastruktur zu werden,
- Opfer eines technischen Defekts kritischer IT-Systeme oder Elemente dieser zu werden,
- Schadensfälle durch unsachgemäße Nutzung hervorzurufen,
- nur unzureichend über die Ressourcen zu verfügen, die für den regulären Betrieb sowie die Wiederherstellung des Betriebs nach einer Störung oder Ausfall nötig sind,
- nicht zu erkennen, dass das Unternehmen bereits in eine der vorgenannten Gefährdungen geraten ist.

Angriffe durch Hacker auf interne Datenbanken mit dem Ziel Kundendaten oder Zahlungsdaten zu erlangen oder die Platzierung von so genannter Schadsoftware zu Sabotage- oder Spionagezwecken sind ebenso bekannt wie DDoS-Attacken[28], die das Ziel verfolgen, einen Server durch Massenanfragen in die Knie zu zwingen. Die entstehenden Schäden können je nach Erfolg des Angriffs verheerend sein und das Ende eines Unternehmens bedeuten. Ein IT-Sicherheitsbeauftragter kennt i.d.R. die IT-Systemlandschaft und weiß diese durch Abtrennung einzelner Areale zu schützen[29]. Auch wird er Angriffsszenarios einplanen, regelmäßig Belastungstests und Penetrationstests veranlassen sowie Softwareupdates einspielen, um die vorhandenen Systeme zu härten. Noch herausfordernder als das Management dieser technischen Komponenten ist hingegen die menschliche Komponente verbunden mit den Anforderungen der modernen Arbeitswelt. Für die IT-Sicherheitsverantwortlichen steigt das Risiko mit jedem neuen Mitarbeiter, der an die bestehenden IT-Systeme angebunden wird. Dass fängt bei der Frage der Zugriffsberechtigungen, die ein Mitarbeiter haben soll an und hört bei der Frage der Password-Policy noch lang nicht auf, wie folgende Beispiele[30] zeigen.

Beispiel 1: Einem Mitarbeiter im Außendienst, der über einen Heimarbeitsplatz mit einem Firmenlaptop arbeitet, wird dieser

28 DDoS steht für Distributed Denial of Service.

29 Zum Beispiel durch die Abtrennung von Produktivsystemen und Testsystemen oder die Abtrennung von Datenbankservern vom Produktivsystem.

30 Die folgenden Beispiele sind zwar alle frei erfunden, können sich aber so oder ähnlich durchaus zutragen.

Laptop bei einer Dienstreise gestohlen. Da der Rechner in diesem Fall nicht verschlüsselt ist und zudem auf dessen Festplatte Kundendaten gespeichert waren, sind Daten verloren gegangen (soweit keine aktuelle Sicherungskopie vorhanden war) und ein unautorisierter Fremdzugriff auf Kundendaten ist möglich. Sind Passwörter und Zugänge zu firmeninternen Netzen möglich, aber auf dem Rechner nicht ausreichend geschützt, steht der Zugriff auf die zentralen IT-Ressourcen im Unternehmen für den Dieb nun offen. Noch plastischer wird der Fall, wenn das Unternehmen ungesicherte Smartphones oder Tablet PCs ausgibt, die leichter zu entwenden sind[31].

Auch im Unternehmen selbst sind Angriffe einfach realisierbar. Schon der Zugang zu den Betriebsräumen birgt Risikopotenzial. Haben alle Mitarbeiter Zutritt zu allen Räumlichkeiten, existiert also kein differenziertes Zutrittssystem zu einzelnen Bereichen, können Unbefugte (egal ob Mitarbeiter oder Fremde) schnell und nahezu ungehindert auch zu sensiblen Daten vordringen.

Beispiel 2: Ein Mitarbeiter, der unzufrieden über seine Jobsituation ist, verschafft sich Zutritt zur Einkaufsabteilung und fotografiert dort mit seinem fotofähigen Handy die Verträge mit den wichtigsten Zulieferern. Schließlich überträgt er die aktuellen Abverkaufszahlen und Margen auf einen privaten USB Memory Stick. Dies war ihm möglich, weil durch die Mittagspause alle Kollegen das Büro verlassen haben – ohne ihre Rechner zu sperren. Auch eine Portsperre für den USB-Stick war nicht vorhanden. Nur wenig später wechselt der Mitarbeiter zu einem Wettbewerber.[32]

Eine gezielte wie auch perfide Form des externen Angriffs ist die auf dem Weg des Social Engineering[33]. Dabei versucht der Angreifer, Kenntnisse über das persönliche Umfeld oder Verhalten eines Opfers zu erlangen. Diese Kenntnisse nutzt er dann, um eine Vertrauensbasis zu erschleichen, die es ihm erlaubt, das Opfer dazu zu bringen, Daten und Informationen preiszugeben, wie folgendes Ereignis zeigt.

Beispiel 3: Ein Anrufer kontaktiert das Call Center eines Versandunternehmens und gibt sich am Telefon als Polizeibeamter aus. Er bittet den Mitarbeiter im Call Center um Auskunft über einen konkreten Kunden und droht mit einer Durchsuchung des Unternehmens, wenn der Mitarbeiter der Forderung nicht nachkommt. Merkt der Angreifer, dass sein Opfer sich von der angeblichen Autorität einnehmen lässt, kann er durch geschickte Fragen Daten, die eigentlich dem Datenschutz unterliegen, abfragen.[34]

„Menschliches Versagen" kann aber auch in der Anwendung der zur Verfügung gestellten Systeme auftreten. Mitarbeiter, die nicht wissen, welche Folgen das Überspielen von Daten hat, werden keine Sicherungskopie erstellen oder Versionsverwaltungen nutzen. Besonders bei der Bearbeitung von Massendaten kann der Schaden schnell eintreten.

Beispiel 4: Ein Mitarbeiter hat die Berechtigung, mehrere tausend Preisdaten für einen Webshop bei einem Preisvergleichsdienst einzuspielen. Er konnte nicht alle

31 Die Studie des Wirtschaftsprüfungsunternehmens KPMG ergab, dass mobile Datenträger als die am einfachsten angreifbaren Informationsträger wahrgenommen werden. Weiss, S., Fritzsche T. (2010), S.10f.

32 Vgl. ebd., S. 11f.

33 Angriffsmuster und Strategien des Social Engineering siehe: Schumacher, S. (2010). Psychologische Grundlagen des Social Engineering. Die Datenschleuder, 2010 (94), S. 52–59.

34 Vgl. Weiss, S., Fritzsche, T. (2010), S. 17.

diese Preise einzeln kontrollieren. Durch einen kleinen Fehler verschob er jedoch den Datensatz ohne es zu bemerken. Als Folge entstand ein vollkommenes Chaos, das Kunden verärgerte, Abmahnungen hervorrief und erhebliche Kosten verursachte.

Abschließend noch ein Beispiel für Schäden, die auf Grund technischen Versagens auftreten können.

Beispiel 5: Ein Unternehmen muss einen Einzeldatennachweis über Wareneinkäufe im Zuge einer Betriebsprüfung abgeben. Die Daten, die vor vier Jahren erhoben wurden, sind jedoch nicht mehr lesbar, da das Speichermedium, ein Bandlaufwerk, durch eine Materialermüdung defekt ist. Die Festplatten der Server, auf denen die Daten vorher lagerten, sind nach dem Ende des Leasingvertrags für diese Geräte bereits vor einem Jahr wieder abgeben worden. Ein Zugriff auf diese Daten ist also auch nicht mehr möglich. Bei der Übergabe der Server nach dem Leasingende wurde auf eine Überprüfung der Bandlaufwerke verzichtet. Ein teurer Fehler, denn dem Unternehmen droht nun eine Steuernachzahlung, da das prüfende Finanzamt nun ungünstigere Schätzwerte in Bezug auf die Einkaufskonditionen annimmt. Zusätzlich droht eine Strafe wegen Verletzung der Aufbewahrungspflicht.

Die Zahl der Beispiele lässt sich für jeden Risikofaktor beliebig erweitern. Ausschlaggebend sind aber folgende Schlussfolgerungen. In allen Fällen finden Rückkopplungen zwischen den Unternehmensangehörigen und der verwendeten Technik statt. In allen Fällen fehlen organisatorische Handlungsrahmen, die entweder das Risiko eindämmen oder den Schadenfall minimieren könnten. Und schließlich fehlte in allen Fällen der jeweils betroffenen bzw. verantwortlichen Person das Wissen um die Folgen oder das Wissen um die richtige Handhabung der genutzten Systeme. Somit muss eine Risikoanalyse neben den „harten Fakten" wie Standort, Zahl der Mitarbeiter und Art der verwendeten Technik auch die „weichen Faktoren" wie die Mitarbeitermotivation, Kenntnisstand der Mitarbeiter und die gelebte Sicherheitskultur im Unternehmen berücksichtigen.

c. Risikoanalyse für die „intrabetriebliche Sphäre"

Die Risikobetrachtung für die IT- und Datensicherheit muss auch die Bereiche ins Auge fassen, in denen Prozesse an Drittunternehmen ausgelagert werden. Dies ist besonders dann der Fall, wenn

- personenbezogene Daten für die Auftragserfüllung weitergegeben werden (Auftragsdatenverarbeitung),
- betriebssensible Daten zur Speicherung oder zur weiteren Verarbeitung weitergereicht werden,
- IT-Komponenten mit Anbindung an firmeninterne Netze ausgelagert werden,
- Dritte Zugang zu den Räumen des Unternehmens erhalten.

Zur Verdeutlichung soll dieses Mal als Beispiel ein Online-Versandunternehmen aus der Lebensmittelbranche herangezogen werden, welches mehrere Prozesse an verschiedenste Dienstleister ausgelagert hat.

Der Versender bietet über seinen Online-Shop neben Lebensmitteln, die trocken gelagert werden, auch Tiefkühlkost an. Die Tiefkühlkost lässt er durch ein darauf spezialisiertes Logistikunternehmen an seine Endkunden versenden. Dazu müssen die Kundendaten an den Logistiker über eine Schnittstelle übermittelt werden. Das Logistikunternehmen kommissioniert die Artikel und sendet diese in speziellen Kühlbehältern auch an die Adressen der

Endkunden. Die Adressdaten erhält der Logistiker täglich über eine Datenschnittstelle vom Auftraggeber. Damit ist der Logistikunternehmer für das Fulfillment im Namen des Online-Shops zuständig. Dies bedeutet jedoch auch, dass der Online-Shop die Verpflichtung eingeht, seinen Logistikdienstleister daraufhin zu prüfen, ob er die gesetzlichen Normen zum Datenschutz einhält. Kann der Logistikdienstleister diese Anforderungen nicht erfüllen, wird im Fall eines Datenverlusts der Online-Shop in der Haftung stehen, da er seiner Sorgfaltspflicht für die ihm überlassenen Daten nicht nachgekommen ist. Die Buchhaltung hat der Online-Shop ebenfalls fremd vergeben. Sie wird durch ein externes Steuerbüro geführt. Diesem werden tagesaktuell alle Eingangs- und Ausgangsrechnungen elektronisch übermittelt. Auch hier sind die Schnittstellen, die für die Datenübertragung sorgen und die Sicherheitsvorkehrungen im Steuerbüro relevant für die IT-Sicherheit. Weiterhin erhalten zur Wartung der betriebseigenen Warenwirtschaftsprogramme die Servicemitarbeiter der Herstellerfirma einen Fernwartungszugriff auf den Server, auf dem das Warenwirtschaftsprogramm läuft. Die Daten, die hier für den Servicemitarbeiter einsehbar sind, sind zwar keine personenbezogenen Daten, aber geben über das Geschäftsvolumen des Online-Shops viel Auskunft. Für die Sauberkeit der Betriebsräume ist eine externe Reinigungsfirma zuständig, die Zutritt zu allen Betriebsräumen hat. Die Mitarbeiter der Reinigungsfirma erhalten natürlich keine sensiblen Daten. Durch ihre Zutrittsmöglichkeit sind sie aber in der Lage, sich Daten selbst anzueignen oder Schäden an Systemen, die für die IT-Sicherheit relevant sind, zu verursachen.

Welche Risikofaktoren lassen sich in den Wechselbeziehungen zwischen einzelnen Unternehmen für die IT-Sicherheit und den Datenschutz ausmachen? Aus dem obigen Beispiel lässt sich herleiten, dass das Risiko von der Art und dem Umfang der ausgelagerten Prozesse abhängt. Ein externer Dienstleister mit direktem Zutritt zu den eigenen Betriebsräumen stellt ein unmittelbares Risiko dar, wenn dieser keinen klaren Verhaltens- und Kontrollregeln unterliegt. Ob Reinigungsfirmen, Handwerker oder Zulieferer, alle können bestimmte Betriebsbereiche betreten und könnten damit direkt oder indirekt Zugriff auf datenverarbeitende Systeme und Klardaten haben. Eigene Verhaltensregeln für diese „In-House“ Dienstleister sind daher angebracht. Ebenso müssen die eigenen Mitarbeiter wissen, wie sie sich gegenüber Betriebsfremden verhalten müssen, wenn diese in das unmittelbare Arbeitsumfeld treten. Ansonsten kann die ungewollte Einsicht in vertrauliche Daten oder im schlimmsten Fall auch deren Diebstahl drohen.

Neben externen Dienstleistern, die „In-House“ agieren, werden Daten und Informationen auch zu externen Dienstleistern übermittelt, die ihre Leistungen außerhalb des Betriebssitzes des Auftraggebers haben. Im obigen Beispiel waren dies der Logistikdienstleister für die Tiefkühlkost, das Steuerbüro und der Wartungsservice für das Warenwirtschaftsprogramm.

Die hier entstehenden Risiken lagern einerseits in der Art der Datenübertragung von Auftraggeber zum Dienstleister. Dies betrifft vor allem die Fragen, wie die technischen Schnittstellen aufgebaut und gesichert sind, damit die Daten konsistent und ohne bei der Übermittlung abgefangen zu werden, übermittelt werden. Im Anschluß muss die Speicherung und Verarbeitung

der Daten beim Dienstleister geregelt sein. Unterläßt der Auftraggeber die Einbindung vertraglicher Regelungen zum Datenschutz und damit verbundene Prüfmöglichkeiten, drohen ihm sowohl Bußgelder im Fall der Aufdeckung als auch das Risiko, einem technischen Datenleck angebunden zu sein. Befindet sich der Dienstleister im selben Rechtsraum, sprich im selben Land, so finden die gleichen geltenden Rechtsnormen für diese Geschäftsbeziehung Anwendung. Auch die Kontrolle der einzuhaltenden vertraglichen und gesetzlichen Normen gestaltet sich in diesen Fällen leichter, da die räumlichen, sprachlichen und kulturellen Barrieren zur Kontrolldurchsetzung geringer sind.[35] Im Sinne der Risikominimierung ist dies ein Vorteil. Wenn der Dienstleister hingegen in einem anderen Land und damit einer anderen Rechtsnorm unterliegt, kann das Herausforderungen für die Datensicherheit bergen. Denn einerseits ist der direkte Zugang zum Dienstleister erschwert – die Kosten der Kontrolle sind somit höher. Der Risikograd ist damit abhängig von der Kontrolldurchsetzung. Andererseits können Differenzen bezüglich der angewandten Rechtslage auftreten. Die Durchsetzung des eigenen Rechtsstandards, dem der Auftraggeber unterliegt, wird gegenüber dem ausländischen Auftragnehmer schwieriger durchsetzbar. Die eigenen Unternehmensverantwortlichen müssen dies als Risiko extra in ihre Betrachtungen mit einbeziehen.

Einfluss in die Risikobewertung sollte auch die „Kontrollsphäre" finden. Das Unternehmen muss abschätzen, welche Nachweise es aufbewahrt und welche Kosten aus einer mangelnden Dokumentation entstehen könnten. Diese Kosten werden gegenüber den Aufsichtsbehörden in Form von Bußgeldzahlungen oder Unterlassungen in Erscheinung treten. In Bezug auf andere Unternehmen, die Geschäftsbeziehungen unterhalten oder solche aufbauen wollen, kann an der Einhaltung der Datensicherheitsanforderungen die Vertragswirksamkeit abhängen.

V. Aufbau einer betriebsinternen Sicherheitsarchitektur

Die benannten Gefahrenszenarien verdeutlichen, dass die IT-Sicherheit und der Datenschutz in alle Betriebsbereiche übergreifen müssen. Unternehmen, die ihre IT-Struktur und damit auch ihre Daten effektiv schützen wollen, schaffen dies nur mit einem Gesamtkonzept, das organisatorische Maßnahmen mit physikalischen und technischen Maßnahmen verbindet. In Anlehnung an die „8 Gebote zum Datenschutz"[36] sollte ein wirksames Konzept zur Sicherheitsarchitektur den Anforderungen von Zutritts-, Zugriffs- und Zugangskontrollen gerecht werden. Es soll also gewährleisten, dass keine unbefugten Personen Räume betreten dürfen, in denen datenverarbeitende Prozesse durchgeführt werden, nur berechtigte Personen auf da-

35 „Die Neuerungen zur Auftragsdatenverarbeitung werden in fast der Hälfte der Unternehmen nicht vollständig umgesetzt. Die meisten Großunternehmen (83%) beauftragen externe Dienstleister mit der Verarbeitung personenbezogener Daten. Gerade hier muss der Datenschutzbeauftragte seit der Novellierung des §11 BDSG detaillierte Vorgaben zur Vertragsgestaltung von sogenannten Auftragsdatenverarbeitungen beachten. Dies betrifft beispielsweise die Weisungs- und Kontrollrechte des Auftraggebers hinsichtlich der Einhaltung der Datenschutzvorgaben beim Auftragnehmer." PricewaterhouseCoopers (2010). Daten schützen. Stand des Datenschutzes in deutschen Großunternehmen, S. 30. www.pwc.de/de_DE/de/compliance/assets/Studie-Daten-schuetzen.pdf (21.08.2011).

36 Erläuterungen dazu finden sich auf der Website des Landesdatenschutzbeauftragten von Schleswig-Holstein. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2011). Technische und organisatorische Datenschutzmaßnahmen. http://www.datenschutz.de/technik/t_o_massnahmen (14.08.2011).

tenverarbeitende Systeme zugreifen dürfen und somit Unbefugten der Zugang zu diesen Systemen verwehrt wird. Das Sicherheitskonzept sollte zudem berücksichtigen, wie die Eingabe von Daten nachvollzogen (Eingabekontrolle) und unter welchen Voraussetzungen Daten so weitergegeben werden können, ohne dass diese abgefangen oder verändert werden (Weitergabekontrolle). Weiterhin muss das Konzept definieren, wie bei einer Auftragsdatenverarbeitung durch externe Unternehmen die Daten gemäß den unternehmenseigenen Weisungen verarbeitet werden können (Auftragskontrolle) und wie der Schutz vor der Zerstörung von Daten sichergestellt ist (Verfügbarkeitskontrolle). Ebenso sollte im Sicherheitskonzept die Umsetzung des Trennungsgebots festgelegt sein, d. h. es sollte erläutern, wie sichergestellt werden kann, dass Daten, welche zu unterschiedlichen Zwecken überlassen worden sind, auch nur für den ursprünglichen Zweck verarbeitet werden.

Unter diesen acht Kontrollmaßnahmen lassen sich die jeweiligen Einzelmaßnahmen durch das Sicherheitskonzept definieren. Die Erarbeitung und Umsetzung des Konzepts wird auch zentrale Fragen zur Unternehmensorganisation und Unternehmenskultur an den Tag bringen. Um Reibungsverluste gering zu halten, sollte deswegen ein Change Management Mitarbeiter auf die Anpassungen vorbereiten und diese Fragen wie die folgenden vorab klären.

- Welche Räume sind besonders schutzwürdig (Serverräume, Forschungsbereiche, Personalbüro, Buchhaltung etc.) und müssen von anderen Räumen getrennt werden?
- Welcher Mitarbeiter hat in welche Unternehmensbereiche Zutritt und warum?
- Auf welche IT-Systeme hat welcher Mitarbeiter Zugriff und welchen Beschränkungen unterliegt er dabei?
- In welcher Weise erfolgt die Auswahl von Mitarbeitern für eine bestimmte Gruppenrolle und wie wird diese dokumentiert?
- Welche Verhaltensweisen werden Mitarbeiter zukünftig nicht mehr gestattet sein?
- Welche Geräte dürfen Mitarbeiter an ihren Arbeitsplätzen nicht mehr nutzen (CD/DVD-Brenner oder USB-Stick)?
- Wie ist mit Datenmüll (auf elektronischen Datenträger oder Papier) umzugehen?
- Wie können Dienstleister vertraglich an die Sicherheitsregeln gebunden werden?
- Wie wird die IT-Struktur gegen Naturgewalten oder gegen Stromausfall geschützt?

Die Erstellung eines solchen Schutzkonzeptes bedarf der Einbindung mehrerer Unternehmensbereiche. Nach der Geschäftsleitung, die in der Gesamtverantwortung steht und eine IT- und Datenschutzstrategie zur Umsetzung freigibt, kommt dem DSB eine zentrale Rolle[37] für die Konzept-erarbeitung zu. Ähnlich wie bei anderen gesetzlich verankerten betriebsinternen Beauftragungen (z. B. Arbeitschutzbeauftragte) verlagert der Gesetzgeber Kompetenzen von den staatlichen Aufsichtsbehörden in den Verantwortungsbereich des Unternehmens selbst[38]. Der DSB ist damit ein gesetzlich gefordertes Aufsichtsorgan im Unternehmen, das auch Berichtspflichten gegenüber staatlichen Aufsichtsbehörden hat. Der DSB wird in vielen Unternehmen

37 Zu den Einzelheiten siehe §4f BDSG.

38 § 4d BDSG.

deswegen kritisch angenommen und im Unternehmensalltag nur bedingt mit den nötigen Kompetenzen ausgestattet, ja teilweise nur mit Alibifunktionen versehen[39]. Die Stelle verursacht Personalkosten und dem Mitarbeiter, der sie ausfüllt, müssten eigene Ressourcen an die Seite gestellt werden.[40] Zudem ist der DSB in seiner Arbeit der Geschäftsleitung nicht weisungsgebunden und genießt einen besonderen Kündigungsschutz.[41] Insgesamt keine förderliche Basis für die Einrichtung einer solchen Stelle. Eine Geschäftsleitung, die jedoch diese Ressource nicht nutzt, verkennt ihren Wert für die strategische Weiterentwicklung der Sicherheitsstruktur. Der DSB kann der Geschäftsleitung als zentrales Relais für Fragen zum Datenschutz und (!) zur IT-Sicherheit dienen. Denn durch seine Aufgaben ermöglicht er der Unternehmensleitung, Einblick in die datenverarbeitenden Geschäftsprozesse und Geschäftsvorfälle zu nehmen. In der „Kundenkontaktsphäre" ist er Ansprechpartner bei Kundenanfragen zum Datenschutz sowie bei der Meldung von Datenschutzvorfällen. Weiterhin nimmt er im Zuge der Vorabkontrolle neue Prozesse, die personenbezogene Kundendaten verarbeiten, ab bzw. dokumentiert bereits bestehende datenverarbeitende Verfahren. Auch betriebsintern kann er aktiv auf Mitarbeiter und Prozesse einwirken. Es ist der DSB, der den innerbetrieblichen Datenstrom kennt bzw. kennen sollte. Im Optimalfall weiß er um die Art der Datenerfassung, -speicherung, -verarbeitung, -weitergabe und schließlich der Datenlöschung und macht dies der Unternehmensleitung kenntlich. Die Mitarbeiterunterrichtung und Sensibilisierung ist eine weitere seiner zentralen Aufgaben. Unternehmen, die sich gegen (Spear) Phishing, Social Engineering oder Verhaltensfehler der Mitarbeiter wappnen möchten, werden gezielte regelmäßige Schulungen nicht umgehen können, um eine eigene Sicherheitskultur aufzubauen. In Bezug auf die intrabetriebliche Sphäre obliegt dem Datenschutzbeauftragten die Prüfung der Dienstleister, die Auftragsdaten verarbeiten.[42] Diese Prüfung umfasst die vertraglichen Regelungen, wie auch die Umsetzung der Sicherheitsstandards des Dienstleisters. Und schließlich ist der DSB Kontaktperson für anfragende Aufsichtsbehörden sowie ein zentraler Ansprechpartner bei Unternehmensaudits.

Schon aus der Fülle der Aufgabenbereiche ergibt sich, dass der DSB nicht als Einzelkämpfer im Unternehmen agieren kann. Er würde an der Themendichte schlicht scheitern. Die Aufgaben sind nur in dem anfangs erwähnten unternehmensinternen Personennetzwerk umsetzbar. Und aus diesem Netzwerk müssen auch die zentralen Elemente des Datenschutz- und des IT-Sicherheitskonzepts stammen. Damit besitzt das Sicherheitskonzept eine breitere Grundlage zur Durchsetzung im eigenen Unternehmen, die Sensibilisierung zentraler Unternehmensbereiche ist leichter umzusetzen und die Kommunikation kann effektiver gestaltet werden. Besonders der letzte Punkt ist dann von unmessbarem Vorteil, wenn ein Schadenfall eintritt und das Notfallmanagement greifen muss.

Abgesehen vom DSB ist der IT-Verantwortliche oder ein beauftragter Mitarbeiter für die IT-Sicherheit zentraler Baustein für die eigene Sicherheitsarchitektur. Denn während der DSB „nur" die Prozesse kennt, in denen personenbezogene Daten

39 Siehe dazu: PricewaterhouseCoopers (2010). Vielen deutschen Unternehmen fehlt eine funktionierende Datenschutzkultur.http://www.pwc.de/de/compliance/vielen-deutschen-unternehmen-fehlt-eine-funktionierende-datenschutzkultur.jhtml (21.08.2011).

40 § 4f BDSG.

41 § 4f Abs. 3 BDSG.

42 Vgl. Weiss, S., Fritzsche, T. (2010), S. 26f.

be- und verarbeitet werden, sollte der IT-Sicherheitsverantwortliche die gesamte IT-Landschaft kennen. Dieser weiß somit um die technischen Details aller Informationssysteme und -prozesse. Und dieser muss die Anforderungen an den Datenschutz in die IT-Sicherheit integrieren und auch an den übrigen IT-Bereich kommunizieren. Nur durch das technische Hintergrundwissen des IT-Sicherheitsverantwortlichen lassen sich eine Risikobewertung und ein Notfallplan entwickeln bzw. die richtige Notfallvorsorge betreiben. Bei der Einbindung neuer technischer Systeme obliegt es ihm, die notwendigen Informationen dazu aufzubereiten und dem DSB sowie ggf. anderen Nutzern zur Verfügung zu stellen. Ebenso kann er technische Anfragen des DSB beantworten, technische Sicherheitsstandards konfigurieren und kritische Systemmeldungen auswerten.

Ein einmal erstelltes IT-Sicherheitskonzept wird zusammen mit seinem untergeordneten Maßnahmenkatalog in das unternehmenseigene QM-System integriert werden, um seine Wirkungen auf das Prozessmanagement und damit die relevanten Betriebsabläufe zu entfalten. Andernfalls würden Reibungsverluste ein solches IT-Sicherheitskonzept entweder in die Bedeutungslosigkeit fallen lassen oder ad absurdum führen, da zum aktuell zu haltenden QM-System auch Aktualisierungen des IT-Sicherheitskonzept parallel implementiert werden müssten. Nur die Verzahnung des Sicherheitskonzepts und dessen Umsetzungsmaßnahmen mit dem QM-System kann der Grundstein für die erfolgreiche Umsetzung desselben sein. Zudem bietet die Verzahnung den Vorteil der Transparenz gegenüber den innerbetrieblichen Stellen, die es anwenden sollen. Daraus ergibt sich aber auch eine klarere Richtschnur für interne Kontrollsysteme. Denn Verantwortlichkeiten können eindeutig nachvollzogen und Funktionstrennungen besser organisiert werden.

VI. Ausblick

Dieser Abschnitt soll in Thesenform Entwicklungstendenzen für den Datenschutz und die IT-Sicherheit in Unternehmen skizzieren. Diese Thesen werden nicht abschließend sein, dennoch fassen sie einzelne Strömungen zusammen, die in den kommenden Jahren aufkommen können.

1. Mit der fortschreitenden Vernetzung von Alltags- und Arbeitsgeräten werden Unternehmen immer stärker dazu gedrängt, den Datenschutz und die IT-Sicherheit gesamtheitlich für alle Prozesse zu betrachten.
2. Gegenüber Kunden werden vertrauensbildende und werbewirksame Maßnahmen zum Thema Datenschutz und Datensicherheit an Bedeutung gewinnen. Dadurch werden Stammkunden an etablierte und datenschutzreife E-Commerce-Unternehmen dauerhafte Vertrauensbindungen aufbauen und personenbezogene Daten gezielt zur Verfügung stellen – auch außerhalb einer direkten Auftragsbearbeitung.
3. Datenverarbeitende Unternehmen werden auf ihre datenverarbeitenden Dienstleister einen eigenen starken Kontrolldruck ausüben, um ihr Sicherheitsinteresse umzusetzen.
4. Die Nachweisführung für die datenrechtliche Eignung von Technik und Prozessen (=Validierung) durch die Unternehmen gegenüber Aufsichtsbehörden wird deutlich in den Vordergrund rücken.
5. Die Löschung nicht mehr benötigter Massenkundendaten wird in den kommenden zwei bis fünf Jahren eine zentrale Herausforderung für die Unter-

nehmen im Bereich des Datenschutzes werden.

VII. Zusammenfassung

Unternehmen halten in ihrem Verantwortungsbereich sowohl personenbezogene als auch betriebssensible Daten. Beide Datenarten sind zentrale immaterielle Unternehmenswerte, die ebenso geschützt werden sollten wie Maschinen und Anlagen. Daraus folgt, dass IT-Sicherheit und Datenschutz einen wesentlichen Teil der Betriebssicherheit bilden. Anhand der drei Sphären in denen ein Unternehmen mit personenbezogenen oder betriebssensiblen Daten arbeitet konnte gezeigt werden, welche grundlegenden Risiken für die Datenverarbeitung bestehen. Unabhängig davon, ob die Risiken durch Datendiebstahl, einer unsachgemäßen Verwendung von technischen Komponenten oder durch höhere Gewalt bestehen, müssen diese unter möglichst wirtschaftlichen Gesichtspunkten minimiert werden. Für solche Risiken, die nicht eingedämmt werden können, müssen stringente Notfallpläne vorliegen, um einen Schadensfall wirtschaftlich akzeptabel zu halten. Durch die immer komplexeren Strukturen, die Unternehmen in sich und in den Beziehungen zu Kunden und anderen Unternehmen aufbauen, kann ein umfassendes IT-Sicherheits- und Datenschutzkonzept nur unter der Mitwirkung zentraler unternehmensinterner Stellen sinnvoll umgesetzt werden. An diesem Konzept sollten neben dem Datenschutzbeauftragten und der Geschäftsleitung auch die Stellen des IT-Sicherheitsverantwortlichen, des Qualitätsmanagements und ggf. betriebsspezifische Stellen mit Verantwortung für betriebssensible Daten mitwirken. Nur durch diese vernetzte Zusammenarbeit kann der Schutz der sensiblen Daten und gleichzeitig auch der Schutz der IT-Infrastruktur gewährleistet werden. Neben dem technischen Schutz kommt der Sensibilisierung der eigenen Mitarbeiter und verbundener externer Dienstleister eine bedeutende Rolle zu. Diese Sensibilisierung auf einem hohen Niveau zu halten wird nur mittels transparenten Vorgaben und regelmäßigen Eigenkontrollen möglich.

Angaben zum Autor:

Robert Kudrass, geboren am 20. März 1980 in Leipzig.

Magisterstudium der Mittleren und Neueren Geschichte, Politikwissenschaft und Volkswirtschaft an der Universität Leipzig und der Università degli Studi di Milano von 1999 bis 2006.

1998/99: Grundwehrdienst als Fernmelder. Seit 2001 im Verband der Reservisten der Bundeswehr; dort seit 2002 Beauftragter für Sicherheitspolitische Arbeit der Landesgruppe Sachsen.

Mitglied der Deutschen-Atlantischen-Gesellschaft und der Gesellschaft für Wehr- und Sicherheitspolitik (GfW)

Seit 2007 in einem mittelständischen Pharmalogistikunternehmen tätig als Beauftragter für Qualitätsmanagement und als Personalverantwortlicher.