Editorial - Grußwort des Forschungsprojektleiters «BayWiDI» Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur zwischenzeitlich sechsten Ausgabe des BayWiDI-Newsletters, welche ganz im Zeichen des European Cyber Security Month (ECSM) 2017 steht.

Cyber-Sicherheit kennt keine Landesgrenzen

Der unter der Leitung der europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Jahr 2012 initiierte und seit 2013 jährlich stattfindende europaweite Aktionsmonat verdeutlicht, dass Cyber-Sicherheit keine Landesgrenzen kennt. Die Digitalisierung ist eine der zentralen Herausforderungen innerhalb der Europäischen Union.[1] Ein digitalisiertes Europa kann allerdings nur dann gelingen, wenn es im gleichen Maße die mit der Digitalisierung verbunden Sicherheitsanforderungen gewährleistet. Diese Herausforderungen kann Brüssel jedoch nicht alleine bewältigen, vielmehr sind wir alle, die wir letztlich von der ubiquitären Vernetzung profitieren, aufgefordert, ebenfalls zum Schutz des Cyberraums beizutragen.

Cyber-Sicherheit geht uns alle an

In diesem Kontext trägt der ECSM maßgeblich dazu bei, die Bürgerinnen und Bürger für das Thema Cyber-Sicherheit zu sensibilisieren und zugleich Hilfestellung für einen verantwortungsbewussten Umgang in der digitalen Wirklichkeit zu leisten.

Die Koordination und Organisation der Aktionen und Veranstaltungen unterschiedlichster Mitwirkender übernimmt in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI). Für den fünften ECSM wurde jeder Kalenderwoche ein spezielles IT-sicherheitsrechtliches Thema zugewiesen.

Als Wissensnetzwerk mit besonderem Fokus auf das IT-Sicherheitsrecht war es uns eine große Freude, auch in diesem Jahr an dem Aktionsmonat mittels kompakter und leicht verständlicher Artikel rund um das Thema IT-Sicherheit und Datenschutz teilzunehmen. Dazu erschien zwischen dem 1. und dem 31. Oktober 2017 wöchentlich ein Beitrag, der aktuelle datenschutzrechtliche und IT-sicherheitsrechtliche Probleme mit Blick auf das Motto der jeweiligen Woche aufgriff, wissenschaftlich aufbereitete und erläuterte. Mit dem vorliegenden Newsletter möchten wir Ihnen die Arbeit der letzten Wochen zusammengefasst übersenden und zugleich einen Einblick in IT-sicherheitsrechtliche Fragestellungen in unterschiedlichsten Lebensbereichen geben.

Beginnend mit der IT-Sicherheit am Arbeitsplatz (S. 2) beschäftigt sich der darauf folgende Beitrag umfassend mit der Neugestaltung des Datenschutzrechts, als wesentlicher Teil der IT-Sicherheit, durch die Datenschutz-Grundverordnung ab dem Jahr 2018 (S. 4). Die zunehmende Vernetzung des Privaten, sei es in Gestalt von WLAN-Netzen, Self-Tracking oder aber durch das Smart Home, erhöht auch in diesem Bereich die Anforderungen an die IT-Sicherheit. Hierzu möchte ich auf den Artikel in diesem Newsletter auf Seite 7 verweisen. Abgerundet wird der Newsletter durch praktische Hinweise zur Gestaltung der IT-Sicherheit im Einzelfall (S. 10). Neben dem Aufzeigen grundlegender Anforderungen an die Cyber-Sicherheit werden etablierte Sicherheitsstandards beleuchtet und miteinander verglichen. Entsprechende Verweise auf unsere digitale Wissensplattform BayWiKI ergänzen diese Ausführungen.

Damit wünsche ich Ihnen eine unterhaltsame und allen voran informative Lektüre.

Ihr
Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

1 Vgl. dazu: Europäische Kommission, Mitteilung der Kommission vom 10.05.2017, COM(2017) 228 final, S. 4.

Woche 1: Cyber-Sicherheit am Arbeitsplatz

Cyber-Sicherheit als zentraler Faktor im Unternehmen

Bereits im Jahr 2006 wies *Dirk Heckmann* darauf hin, dass die Bewältigung der Herausforderung Cyber-Sicherheit wesentliches Kennzeichen moderner Unternehmensführung und -kultur sein muss.[1] Dem wird zwischenzeitlich unter anderem dadurch Rechnung getragen, dass Cyber-Sicherheit als entscheidender Bestandteil unternehmerischer Compliance anerkannt ist.[2] Eine erfolgreiche Digitalisierung ist ohne die hinreichende Beachtung der Cyber-Sicherheit nicht möglich.[3]

Cyber-Sicherheit ist dabei aber auch eine Frage der Rechtssicherheit. Insbesondere die mangelnde einheitliche Kodifizierung des IT-Sicherheitsrechts stellt für kleine und mittelständische Unternehmen eine nicht zu unterschätzende Hürde dar.

Wenngleich sowohl auf nationaler als auch auf europäischer Ebene legislative Schritte zur Sicherstellung der grundrechtlich garantierten IT-Sicherheit unternommen wurden,[4] richten sich diese regelmäßig lediglich an die Betreiber kritischer Infrastrukturen[5].

Dass der Schutz derjenigen Einrichtungen, „die für das Funktionieren [des] Gemeinwesens zentral sind […] von größter Wichtigkeit [ist]“[6], steht außer Frage. Eine aktuelle Studie[7] des Digitalverbands Bitkom, welche in Zusammenarbeit mit dem Bundesverfassungsschutz erstellt wurde, zeigt allerdings eindrucksvoll, dass IT-Sicherheit für alle Formen und Branchen des deutschen Unternehmertums von existenzieller Bedeutung ist.

Rund die Hälfte der befragten Unternehmen wurde im Zeitraum 2015 – 2016 Opfer eines digitalen Angriffs, wie etwa Datendiebstahl oder Sabotage.[8] Jährlich entstehen dadurch allein in Deutschland Schäden in Höhe von bis zu 55 Milliarden Euro, wobei insbesondere Ermittlungen und Ersatzmaßnahmen, Umsatzeinbußen, Patentrechtsverletzungen sowie Imageschäden wesentliche Kostenfaktoren sind.[9]

Die Angst vor Letzterem sorgt oftmals dafür, dass entsprechende Vorfälle nicht gemeldet werden. Eine transparente Handhabung würde aber letztlich maßgeblich zur Stärkung der gesamtdeutschen IT-Sicherheit beitragen.[10]

Die Wahrung beziehungsweise Herstellung der Cyber-Sicherheit ist daher nicht nur eine gemeinsame Aufgabe für Staat und Wirtschaft im Allgemeinen,[11] sie muss gleichsam zur „Chefsache“[12] im konkreten Unternehmen erklärt werden.

Cyber-Sicherheit am Arbeitsplatz

Im Folgenden soll nunmehr dargestellt werden, wie sich das abstrakte Schlagwort Cyber-Sicherheit auf den konkreten Arbeitsplatz auswirkt. Allen voran, da Cyber-Sicherheit nicht nur ein Problemfeld der Unternehmensleitung, des Systemadministrators oder gegebenenfalls des IT-Sicherheitsbeauftragten ist, soll gezeigt werden, welche Gefährdungslagen den einzelnen Arbeitsplatz betreffen.

I. Zum Begriff des Arbeitsplatzes

Vorab gilt es dabei zu klären, wie der Begriff des Arbeitsplatzes zu verstehen ist. Ein gesetzlicher Anhaltspunkt lässt sich der Arbeitsstättenverordnung (ArbStättV) entnehmen. Diese definiert den Arbeitsplatz in § 2 Abs. 4 als den

1 *Heckmann*, MMR 2006, 280, 282.

2 *Beucher/Utzerath*, MMR 2013, 362, 367.

3 *Bundesamt für Sicherheit in der Informationstechnik*, Die Lage der IT-Sicherheit in Deutschland 2016, S. 61.

4 *Heckmann*, MMR 2015, 289, 290; vgl. dazu auch https://www.baywidi.de/wiki/gesetzliche-grundlagen/gesetzliche-grundlagen-fuer-betreiber-kritischer-infrastrukturen/.

5 *Rockstroh/Kunkel*, MMR 2017, 77, 78.

6 BT-Drs. 18/4096, S. 1.

7 *Bitkom*, Wirtschaftsschutz in der digitalen Welt, 2017. Online abrufbar unter: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf; zuletzt abgerufen am 12.09.2017.

8 *Bitkom*, Wirtschaftsschutz in der digitalen Welt, 2017, S. 2.

9 *Bitkom*, Wirtschaftsschutz in der digitalen Welt, 2017, S. 5.

10 *Bitkom*, Spionage, Sabotage, Datendiebstahl, online abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html, zuletzt abgerufen am 12.09.2017.

11 So das *Bundesministerium des Innern*, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 9.

12 *Bundesamt für Sicherheit in der Informationstechnik*, Leitfaden Informationssicherheit – IT-Grundschutz kompakt, S. 10.

Bereich, in dem die Beschäftigten im Rahmen ihrer Arbeit tätig sind.

Die juristische Literatur versteht den Begriff dabei allerdings weit,[13] so dass beispielsweise auch Zugangswege, die Kantine oder aber auch sanitäre Einrichtungen als Teil des Arbeitsplatzes zu werten sind.[14] Eine Mindestdauer der Tätigkeit an einem bestimmten Platz, wie dies früher noch vorgesehen war, ist ebenfalls nicht mehr erforderlich.[15] Auch der zeitlich begrenzte Beschäftigungsort ist als Arbeitsplatz anzusehen.[16]

Für den Arbeitgeber, aber auch für den Arbeitnehmer, hat das zur Folge, dass Cyber-Sicherheit nicht am Schreibtisch endet. Es ist vielmehr dafür zu sorgen, dass das gesamte Beschäftigungsumfeld IT-sicher gestaltet wird.

II. Die Gefährdungslagen am lokalen Arbeitsplatz

Cyber-Sicherheit ist eine Frage des Einzelfalls, es kann keine absolute Cyber-Sicherheit geben.[17] Die Anforderungen an die IT-Sicherheit hängen daher von der jeweiligen Gefährdungslage am konkreten Einsatzort innerhalb des Unternehmens ab.[18] Für den Bereich des Arbeitsplatzes lassen sich dabei drei wesentliche Faktoren identifizieren, die bei einer sicheren Ausgestaltung desselben zu beachten sind:[19]

- Technische Versäumnisse
- Organisationsverschulden
- Fehlverhalten der eigenen Beschäftigten

Welche konkreten Gefährdungssituationen sich aus den einzelnen abstrakten Gefahrenquellen ergeben können, soll im Folgenden in Kürze dargestellt werden.

1. Technische Versäumnisse

Cyber-Sicherheit ist maßgeblich von der am Arbeitsplatz eingesetzten Technik abhängig. Insbesondere im unternehmerischen Bereich potenziert sich die Gefährdungslage bei dem Einsatz veralteter Hardware oder entsprechend mangelhafter Softwarepflege.[20] Darüber hinaus kann aber auch die administrative Verwaltung der Systeme, die unzureichend gesicherte Anbindung an das Internet oder aber die schlichte Nichtbeachtung von tatsächlich existierenden Sicherheitsvorgaben zu zahlreichen Sicherheitslücken in der IT des Unternehmens führen.[21] Weiterhin ist zu beachten, dass aufgrund der sich stets wandelnden technischen Gegebenheiten auch die Gefahrenquellen dynamisch sind; diese gilt es laufend im Auge zu behalten.[22]

2. Organisationsverschulden

Dass mit der zunehmenden Digitalisierung zugleich die Anforderungen an die IT-Sicherheit steigen, liegt auf der Hand. Ebenso ist es nicht immer zielführend, Feuer mit Feuer zu bekämpfen, es bedarf neben der technischen Aufrüstung daher stets auch analoge organisatorische Maßnahmen.[23] Gefahren für die Cybersicherheit am Arbeitsplatz können aus organisatorischer Sicht insbesondere dann entstehen, wenn es an Zugangs- und Zugriffskontrollen fehlt oder ein entsprechendes Risikomanagement samt Benennung der zuständigen Personalien nicht vorhanden ist. Darüber hinaus kann auch das Fehlen eines umfassenden Notfallmanagements zu weitreichenden Gefahren für die allgemeine Cyber-Sicherheit führen. Insbesondere bei neuen Formen der Cyber-Attacken, wie beispielsweise dem sog. CEO-Fraud, kann ein grundlegendes und wohldurchdachtes Notfallmanagement dabei helfen, schnell zu reagieren und dadurch letztlich die Verluste zu minimieren.[24]

3. Fehlverhalten der eigenen Beschäftigten

Der IT-sichere Arbeitsplatz ist in besonderem Maße von der aktuellen und ehemaligen Belegschaft des Unternehmens abhängig. Auf Grundlage der aktuellen Bitkom-Studie ist davon auszugehen, dass die Mehrzahl der Cyberattacken im Unternehmensbereich von (ehemaligen) Beschäftigten durchgeführt wird.[25] Im Bereich der Vorsatzhandlungen kommen dabei insbesondere Hard- und Softwaremanipulationen sowie Diebstahl und Sachbeschädigung in Betracht.[26] Darüber hinaus kann aber auch schlicht menschliches Versagen, in Gestalt von Bedienfehlern oder beispielsweise der leichtsinnige Umgang mit E-Mails, zu gravierenden Schäden führen.[27]

Mit Blick auf die zahlreichen unterschiedlichen Gefährdungssituationen sowie die Besonderheiten des jeweiligen Unternehmens sind pauschalisierte Lösungen kaum anzubieten. Vielmehr bedarf es zum Zwecke der bedarfs- und gesetzeskonformen IT-Sicherheit am Arbeitsplatz einer gezielten und individualisierten Risikoanalyse.[28]

Allerdings kann bereits die Beachtung einiger grundlegender IT-Sicherheitsregeln zu einer signifikanten Erhöhung des Sicherheitsniveaus führen. Entsprechende Ausführungen finden sich gesondert im Beitrag zur Vermittlung der Cyber-Sicherheit auf Seite 10.

Scheurer

13 *Schlachter*, in: Müller-Glöge/Preis/Schmidt, Erfurter Kommentar zum Arbeitsrecht, 17. Aufl. 2017, § 2 MuSchG Rn. 2; *Schrader*, in: Rolfs/Giesen/Kreikebohm/Udsching, BeckOK Arbeitsrecht, 44. Edit. Stand: 01.06.2017, § 2 MuSchG Rn. 4.

14 *Schrader*, in: Rolfs/Giesen/Kreikebohm/Udsching, BeckOK Arbeitsrecht, 44. Edit. Stand: 01.06.2017, § 2 MuSchG Rn. 4.

15 *Wiebauer*, NZA 2017, 220, 221.

16 *Wiebauer*, NZA 2017, 220, 221.

17 *Rockstroh/Kunkel*, MMR 2017, 77, 78; *Gaycken/Karger*, MMR 2011, 3, 4.

18 *Mehrbrey/Schreibauer*, MMR 2016, 75, 80.

19 Nach *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz, B. 2.3.

20 *Scheurer*, AnwZert ITR 6/2017 Anm. 2.

21 Vgl. dazu m. w. N.: *Bundesamt für Sicherheit in der Informationstechnik*, Leitfaden Informationssicherheit, S. 26 ff.

22 *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 16.

23 So bereits *Heckmann*, MMR 2006, 280.

24 Vgl. dazu m. w. N.: *Aufderheide/Fischer*, CCZ 2017, 138, 140.

25 *Bitkom*, Wirtschaftsschutz in der digitalen Welt, 2017, S. 6.

26 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz, B. 2.3.

27 *Kramer/Meints*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 44. EL Januar 2017, Teil 16.5 Rn. 12.

28 *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 16.

Woche 2: Sicherheit und Schutz persönlicher Daten

Datenschutzrecht – wieso? weshalb? warum?

Die Sicherheit und der Schutz der persönlichen Daten mögen auf den ersten Blick nicht für jedermann bedeutsam erscheinen. Dabei ist dieses Thema allgegenwärtig und geht mit der Bewahrung zentraler Grundrechte einher. Das Verständnis für den Datenschutz ist elementar, um Datensicherheit wirksam umsetzen zu können.

I. Anwendungsbereich: Personenbezogene Daten

Persönliche beziehungsweise personenbezogene Daten sind gemäß § 3 Bundesdatenschutzgesetz (BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)." Doch was für einen großen Vorteil hat eine andere Person schon, wenn sie beispielsweise das Geburtsdatum einer fremden Person kennt? Bei der Diskussion rund um den „gläsernen Bürger" wird zudem immer wieder das Argument vorgebracht, dass der, der nichts zu verbergen hat auch nichts dagegen habe, dass seine Daten gespeichert und verwertet werden.[1] Aber warum müssen wir einerseits regeln, welche Daten wie von wem verarbeitet werden dürfen (Datenschutz) und wie unsere Daten vor illegalen Zugriffen geschützt werden (Datensicherheit)?

II. Persönliche Daten als Teil des allgemeinen Persönlichkeitsrechts

Zentrale Punkte sind dabei einmal die Sensibilität der Daten an sich, denn sie geben Aufschluss über den individuellen Lebensstil, d.h. Angewohnheiten und Verhaltensmuster, sodass die Handlungen einer Person sogar vorhersehbar werden;[2] die unbegrenzte Speicherdauer, die es ermöglicht niemals „zu vergessen"; der schnelle Transfer der Daten auf unendlich viele Medien sowie die mangelnde Transparenz, die sich für jeden Einzelnen in Bezug auf seine Daten ergibt.

Diese Wichtigkeit im Kontext des Schutzes persönlicher Daten erkannte das Bundesverfassungsgericht bereits 1983 – weit vor dem heutigen „Zeitalter des Internets": „[Persönliche Daten sind] technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar […]. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann."[3]

Durch das Sammeln, Speichern und Verwenden von Daten kommt es somit zur Beeinträchtigung von Grundrechten. Namentlich sind dies neben dem Fernmeldegeheimnis, Art. 10 GG, und dem Schutz der Wohnung, Art. 13 GG, vor allem die Ausprägungen des allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Bedeutsam sind hierbei insbesondere das Recht auf informationelle Selbstbestimmung[4] und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme[5] – auch bekannt als „IT-Grundrecht". Um den Interessen des Einzelnen, dem am Schutz durch die Grundrechte gelegen ist, und den gegenläufigen Interessen von öffentlichen oder nicht-öffentlichen Stellen, welche die persönlichen Daten be- oder verarbeiten, Rechnung zu tragen, gibt es das Datenschutzrecht.

Demnach ist Datenschutz weniger Schutz der Daten oder Schutz vor ihnen, sondern vielmehr der Schutz der Persönlichkeitssphäre jedes Einzelnen in Bezug auf seine persönlichen Daten[6] und damit auch Schutz der Grundrechte.[7]

Datenschutzrecht im Laufe der Zeit: von Hessen nach Europa

Seit seinen Anfängen 1970 mit dem hessischen Landesdatenschutzgesetz[8] hat das Datenschutzrecht zahlreiche Neuerung erlebt. Gab es zu Beginn nur Empfehlungen und Richtlinien (beispielsweise von der OECD) oder vor dem ersten BDSG nur

1 Vgl. *Schellenberg*, ZRP 2014, 24, 25.

2 *Graf von Westphalen*, BB 2017, Heft 01-02, Umschlagteil I.

3 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 = NJW 1984, 419, 421.

4 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 = NJW 1984, 419, 422.

5 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 = DÖV 2008, 459 f.

6 BT-Drucks. 7/1027 S. 1.

7 *Frye/Simitris*, Forschung Frankfurt 1/2015, 44, 49.

8 HDSG vom 06.10.1970; vgl. *Frye/Simitris*, Forschung Frankfurt 1/2015, 44, 46.

bundeslandspezifische Regelungen, so ist Datenschutz und Datensicherheit inzwischen ein europäisches Thema geworden.

1977 trat das erste BDSG in Kraft, welches im Laufe der Jahre ständig reformiert wurde. Mit der Datenschutzrichtlinie der EU 1995[9] und der Einführung des Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) 1997 erlangte das Thema einen europäischen Regelungsrang. Nach turbulenten Zeiten, u.a. durch den Safe-Harbor-Beschluss der Europäischen Kommission[10], gilt nun ab 25.05.2018 nach einer zweijährigen Übergangszeit die Datenschutz-Grundverordnung (DS-GVO)[11] der EU.

Datenschutz heute

I. Rechtsrahmen

Neben völkerrechtlichen beziehungsweise europarechtlichen Normen wie Art. 16 AEUV, Art. 7, 8 der Grundrechtecharta, ist der zentrale Normenkatalog des Datenschutzrechts das BDSG, welches wiederum die Datenschutzrichtlinie umsetzt. Bis zum 25.05.2018 gilt in Deutschland das BDSG in der aktuellen Fassung sowie die unterschiedlichen Landesdatenschutzgesetze. Diese sind subsidiär zu den spezialgesetzlichen Regelungen wie beispielsweise dem Telemediengesetz (TMG), vgl. u.a. § 1 Abs. 3 Satz 1 BDSG. Die gesetzlichen Regelungen richten sich dabei nicht nur an private Dritte, sondern ebenso an staatliche bzw. öffentliche Stellen, § 1 Abs. 2 BDSG. Denn spätestens seit dem NSA-Skandal, der 2013 mit der Veröffentlichung der von Edward Snowden entwendeten Dokumente begann, ist erkennbar, dass eine Verletzung des Persönlichkeitsrechts nicht nur durch private Firmen wie Google, Facebook und Co., sondern ebenfalls durch öffentliche Stellen stattfindet.

II. Das BDSG heute

Zentrale Inhalte des BDSG sind Vorgaben darüber, wer welche Daten wann erheben und verarbeiten darf, wann sie zu löschen sind und ob sie an bestimmte andere Personen weitergegeben werden dürfen, vgl. §§ 4, 13 ff., 28 ff. BDSG. Die Datenerhebung, -verarbeitung, und -nutzung ist dabei grundsätzlich nur erlaubt, soweit dies durch eine Rechtsvorschrift gestattet ist oder die Einwilligung des Betroffenen vorliegt, § 4 BDSG (Verbot mit Erlaubnisvorbehalt). Wichtig ist außerdem, dass die Daten lediglich für den Zweck verarbeitet und genutzt werden, für den sie auch erhoben wurden (Zweckbindung), vgl. beispielsweise § 14 Abs. 1 BDSG. Zudem stattet das BDSG die einzelne Person mit Abwehr- und Auskunftsrechten aus, §§ 6, 19, 20, 34, 35 BDSG. Verstöße können außerdem mit einem Bußgeld geahndet werden oder zur strafrechtlichen Verfolgung führen, §§ 43, 44 BDSG.

Zentrales Element informationeller Selbstbestimmung und damit des Datenschutzes ist das Instrument der Einwilligung. Die konkreten Anforderungen an eine solche und die Frage, ob diese auch konkludent ergehen kann, sind umstritten. Auf jeden Fall bedarf es der freien Entscheidung des Betroffenen, einer ausführlichen Information und der Möglichkeit des Widerrufs der Einwilligung. Zudem setzt § 4a Abs. 1 BDSG bis auf wenige Ausnahmefälle die Schriftform voraus.

Die Zukunft: DS-GVO und BDSG 2018

I. Die DS-GVO

Die DS-GVO treibt das Ziel der Vereinheitlichung des europäischen Binnenraums auch auf dem Gebiet des Datenschutzes voran. Da die Verordnung unmittelbar Anwendung in den einzelnen Mitgliedstaaten findet, Art. 288 Abs. 2 AEUV, ist kein weiterer Umsetzungsakt mehr nötig. Wie auch das BDSG ist die DS-GVO als Verbot mit Erlaubnisvorbehalt konzipiert: Eine Datenverarbeitung ist grundsätzlich untersagt, nur in den gesetzlich abschließend geregelten Fällen ist sie erlaubt, vgl. Art. 6 DS-GVO.

1. Grundsätze und Anwendungsbereich

Die Ziele der DS-GVO sollen durch bestimmte, festgelegte Grundsätze erreicht werden, die den gesamten Normenkatalog prägen. Diese sind gemäß Art. 5 DS-GVO: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht.

Wichtig ist, dass die DS-GVO nicht auf alle Sachverhalte Anwendung findet, sondern nur soweit dies Art. 2 und 3 DS-GVO bestimmen. Ausgenommen ist dabei beispielsweise die Datennutzung durch natürliche Personen zu rein persönlichen oder familiären Tätigkeiten, Art. 2 Abs. 2 lit. c DS-GVO oder durch zuständige Behörden bei der Strafverfolgung,

9 RL 95/46/EG vom 24.10.1995.

10 Entscheidung der Kommission vom 26.07.2006, ABl. EU, 25.08.2000, L 215/7.

11 Verordnung (EU) 2016/679 vom 27.04.2016.

Art. 2 Abs. 2 lit. d DS-GVO. Art. 3 DS-GVO ist indes relevant, wenn es darum geht, ob die Verarbeitung von Daten in den räumlichen Anwendungsbereich fällt. Dies kann auch dann der Fall sein, wenn die Datenverarbeitung nicht in der Europäischen Union stattfindet, vgl. Art. 3 Abs. 1 DS-GVO.

2. Rechte des Betroffenen

In den Art. 12 bis 22 DS-GVO werden dem Betroffenen der Datenverarbeitung verschiedene Rechte eingeräumt: Informationsrecht (Art. 13, 14 DS-GVO), Auskunfts- und Widerspruchsrecht (Art. 15 DS-GVO), Recht auf Berichtigung (Art. 16 DS-GVO), Löschung (Art. 17 DS-GVO) und Einschränkung (Art. 18 DS-GVO) und das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO).

In dieser Hinsicht zeigt sich, dass der Schutz der Betroffenen und ihrer Rechte im Vergleich zu der bisher geltenden Datenschutzrichtlinie weiter ausgebaut werden. Hervorzuheben ist das nunmehr kodifizierte „Recht auf Vergessenwerden", das Betroffenen einen Rechtsanspruch gegen die Unternehmen gibt Daten zu löschen. Dies war bisher nur schwer durchzusetzen; dabei rückte die Problematik vor allem 2012 mit dem Urteil des EuGH[12] in der Rechtssache gegen Google Spain SL und Google Inc. in den Fokus.

3. Datenverarbeiter in der Pflicht

Darüber hinaus werden die Verantwortlichen verpflichtet, sich mehr mit dem Thema Datenschutz und Datensicherheit zu befassen. Allen voran ist dabei die Bestellung eines Datenschutzbeauftragten sowie die Integration der Grundsätze Privacy by Design sowie Privacy by Default zu nennen. Letztere sollen sicherstellen, dass Datenschutz sowie Datenminimierung bereits während des Entwicklungsprozesses beachtet werden.[13] Darüber hinaus sollen Voreinstellungen stets so standardisiert eingestellt sein, dass die geringstmögliche Grundrechtsbeeinträchtigung gegeben ist.[14]

Des Weiteren müssen die Sicherheit der Verarbeitung und die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, Art. 32 Abs. 1 lit. b DS-GVO, entsprechend dem Stand der Technik gewährleistet werden. Vergleichbar mit der Regelung des derzeitigen BDSG (§ 9), richtet sich der (technische) Aufwand zur Datensicherung nach der Art der Daten,[15] sodass auf diesem Weg IT-Sicherheit hergestellt wird.

Zudem ist ein Verzeichnis von Verarbeitungstätigkeiten anzulegen, Art. 30 DS-GVO. Für den Fall, dass ein hohes Risiko für den Schutz der zu verarbeitenden personenbezogenen Daten besteht, ist eine Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO durchzuführen. Verschärft wird zudem die Meldepflicht an die zuständige Aufsichtsbehörde und an den Betroffenen, Art. 33-35 DS-GVO. Diese hat nach der DS-GVO grundsätzlich bei jedem Verstoß zu erfolgen.

Bezüglich der aus § 11 BDSG bekannten Auftragsdatenverarbeitung (ADV) ändert sich wenig. Die europäische Regelung hat sich dabei stark an der deutschen Rechtslage orientiert, lediglich die Haftung wird ausgeweitet, sodass Verantwortlicher und Auftragsverarbeiter nach der DS-GVO gemeinsam gegenüber dem Betroffenen haften. Umstritten ist hingegen die Frage, ob Wartungsarbeiten, die bisher gemäß § 11 Abs. 5 BDSG als ADV eingestuft wurden, auch unter Art. 28 DS-GVO fallen und somit weiterhin als ADV zu qualifizieren sind.[16]

4. Weitgehende Angleichung

Mit der Einführung des Kohärenzverfahrens, Art. 63 DS-GVO, und der Einrichtung des Europäischen Datenschutzausschusses, Art. 68 DS-GVO, soll sichergestellt werden, dass die angestrebte Angleichung auch in der Praxis Niederschlag findet. Gerade bei europaweiten Sachverhalten kann so gewährleistet werden, dass das Datenschutzrecht für einen einheitlichen Fall auch in den unterschiedlichen Mitgliedstaaten einheitlich angewendet wird.

II. Das BDSG 2018

Um weiterhin mit dem BDSG einen europarechtskonformen Normenkatalog zu haben, bedarf es einiger Neuregelungen. Diese Änderungen wurden bereits vom Gesetzgeber beschlossen, sodass das reformierte BDSG zeitgleich mit der DS-GVO ab Mai 2018 gilt. Gleichzeitig nutzte der Gesetzgeber seinen durch die sog. „Spezifizierungsklauseln" in der DS-GVO gegebenen Spielraum um sicherzustellen, dass es nicht zu einem Absinken der datenschutzrechtlichen Standards in Deutschland kommt.

Beispielhaft dafür ist der Bereich des Arbeitnehmerdatenschutzes. Abgesehen von der Regelung in Art. 9 Abs. 2 lit. h DS-GVO normiert diese den Beschäftigtendatenschutz nicht. Jedoch hat der europäische Verordnungsgeber mit Art. 88 DS-GVO eine Spezifizierungsklausel geschaffen, sodass es den Mitgliedstaaten freisteht, spezielle Regelungen im Kontext des Arbeitnehmerdatenschutzes einzuführen. Von dieser Möglichkeit hat der deutsche Gesetzgeber mit § 26 BDSG 2018 Gebrauch gemacht, sodass ein entsprechendes Schutzniveau gewährleistet wird.

Ausblick / Resümee

Das Datenschutzrecht ist in Zeiten der zunehmenden Digitalisierung essenziell, um den Schutz des Rechts auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten. Es ist Vermittlungselement in zentralen Bereichen des Lebens zwischen den gegenläufigen Interessen und es ist Absicherung für jeden Einzelnen, dass nicht irgendwo ohne sein Wissen Unmengen an persönlichen Daten angehäuft und zu willkürlichen Zwecken genutzt werden.

Rachut

12 vgl. EuGH, Urt. v. 13.05.2014 – C – 131/12 = NJW 2014, 2257 ff.

13 *Baumgartner*, in: Ehmann/Selmayr DSGVO, 1. Aufl. 2017, Art. 25 Rn.9.

14 *Baumgartner*, in: Ehmann/Selmayr DSGVO, 1. Aufl. 2017, Art. 25 Rn.13.

15 *Baumgartner/Gausling*, ZD 2017, 308, 310 f.

16 Für die Anwendung von Art. 28 DS-GVO: *Schmidt/Freund*, ZD 2017, 14, 16 f.; a.A.: *Lisser*, DSRI 2016, 401, 414.

Woche 3: Cyber-Sicherheit zuhause

Vernetzung zuhause

Die zunehmende Digitalisierung hat auch im privaten Bereich Einzug gefunden. Laut Statistischem Bundesamt finden sich in 88 % der deutschen Haushalte Computer für den privaten Gebrauch; der Anteil der Mobilfunktelefone ist mit 95 % noch einmal höher.[1] Nahezu jeder ist inzwischen auch zuhause „online".[2] Doch damit gehen nicht nur dauerhafte und vielfältige Kommunikationsmöglichkeiten, sowie der Zugang zu unendlich scheinendem Wissen einher, sondern auch Risiken und Probleme, die gerade auch den technischen Eigenheiten und der zunehmenden Vernetzung entspringen.

WLAN: unüberschaubare Haftungsrisiken?

Wiederkehrendes Thema sind dabei die Haftungsproblematiken, die sich bei der Einrichtung und Nutzung eines WLAN ergeben. So verfügten im Jahr 2016 87 % der Haushalte über einen Internetzugang.[3] Dabei ist die Einrichtung eines WLAN in den eigenen vier Wänden heutzutage der wohl gängigste Weg allen Geräten Zugang zum Internet zu gewähren. In diesem Zusammenhang stellt sich die Frage, wie damit umgegangen wird, wenn diese Netzwerke unbefugt oder rechtswidrig genutzt werden. Häufig geht es dabei um die Verletzung von geistigem Eigentum.

I. Haftung des WLAN-Betreibers nach den Grundsätzen der Störerhaftung

Bisher kommt eine Haftung des WLAN-Betreibers in Form der sogenannten Störerhaftung in Betracht. Nach den allgemeinen Grundsätzen wird dabei zwischen Handlungs- und Zustandsstörer unterschieden.[4] Handlungsstörer ist, wer die rechtswidrige Beeinträchtigung durch eigenes Handeln oder pflichtwidriges Unterlassen adäquat verursacht. Zustandsstörer ist hingegen, wer aufgrund seiner Rechtsstellung für eine Sache, von der die Beeinträchtigung ausgeht, verantwortlich ist. Dabei muss die Beeinträchtigung allerdings zumindest mittelbar auf seinen Willen zurückgehen.[5] Die Person, auf dessen Namen das WLAN eingerichtet ist, kommt bei Rechtsverletzungen, die über dieses Netzwerk begangen werden, somit als Zustandsstörer in Betracht. Der BGH hat genau dies angenommen und dabei eine verschuldensunabhängige Haftung des Betreibers für alle Rechtsverletzungen, die mithilfe „seines" Netzwerkes begangen werden, bejaht. Das hat eine Haftung des Netzwerkbetreibers zur Folge, selbst wenn eine andere Person die eigentliche Rechtsverletzung (schuldhaft) begangen hat.[6] Die Haftung des Anschlussinhabers ist aber auf Grundlage dieser Rechtsprechung auf Unterlassungsansprüche beschränkt.[7] Diese, nicht auf ausdrückliche gesetzliche Kodifizierung fußende, Rechtsprechung argumentiert mit einer Anschlusssicherungspflicht des Betreibers.[8] Allerdings führt eine solche Pflicht zu Rechtsunsicherheit und birgt ein, vor allem für den privaten Nutzer unüberschaubares, Haftungsrisiko. Darüber hinaus besagt eine solche Anschlusssicherungspflicht, dass der WLAN-Betreiber das Netzwerk gegen unbefugtes Benutzen zu sichern, d.h. mit einem Passwort zu versehen hat.[9] Dies wiederum verhindert, dass „offene" Netzwerke, beispielsweise an öffentlichen Plätzen, möglich sind. Im Vergleich zu anderen Ländern ist Deutschland Nachzügler in diesem Bereich: Betreiber von Hotels oder Cafés müssen fürchten, wenn sie ihren Kunden ein offenes Netzwerk zur Verfügung stellen, für das Handeln jener haftbar gemacht zu werden.

Letztlich stellt sich die Frage, ob die vom BGH benannte „Anschlusssicherungspflicht" auch das Instruieren und Überwachen derer Personen beinhaltet, die befugt Zugang zu einem Netzwerk erhalten. Dies wurde in der Vergangenheit durch die Rechtsprechung angenommen.[10] Teilweise wurde zusätzlich verlangt, dass der Betreiber des WLAN den Zugang zu diesem Netzwerk nur durch Eingabe eines eigenen Passworts anderen Personen ermöglichen dürfe.[11]

---

1 https://www.destatis.de/DE/Zahlen-Fakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html#Fussnote1 (abgerufen am 30.08.2017).

2 Vgl. *Koch/Frees*, ARD/ZDF-Onlinestudie 2016, S. 418.

3 siehe Fn.1.

4 *Bassenge*, in: Palandt BGB, 76. Aufl. 2017, § 1004 Rn.15.

5 *Bassenge*, in: Palandt BGB, 76. Aufl. 2017, § 1004 Rn.16 ff.; *Berger* in: Jauernig BGB, 16. Aufl. 2015, § 1004 Rn. 15 ff.

6 BGH, Urt. v. 12.05.2010 - I ZR 121/08 = GRUR 2010, 633, 636.

7 BGH, Urt. v. 12.05.2010 - I ZR 121/08 = GRUR 2010, 633 ff.

8 *Borges*, NJW 2010, 2624, 2625; *Haun*, BB 2017, 780, 781; BGH, Urt. v. 12.05.2010 - I ZR 121/08 = GRUR 2010, 633, 636.

9 BGH, Urt. v. 12.05.2010 - I ZR 121/08 = GRUR 2010, 633, 636; *Stang/Hühne*, GRUR-RR 2008, 273, 274.

10 Bspw. LG Hamburg, Beschl. v. 21.04.2006 – 308 O 139/06 = MMR 2007, 131; LG Hamburg, Beschl. v. 02.08.2006 – 308 O 509/06 = BeckRS 2010, 17613; a.A. OLG Frankfurt a.M., Beschl. v. 20.12.2007 – 11 W 58/07 = MMR 2008, 169, 170.

11 LG Düsseldorf, Urt. v.. 26.08.2009 – 12 O 594/07 = NJOZ 2010, 680, 681 f.

Die Regelungen der Störerhaftung haben in der Praxis für den Verletzten den Vorteil lediglich den WLAN-Betreiber ausfindig machen und darüber hinausgehend keine Nachforschungen anstellen zu müssen. Allerdings führt dies, sowohl für Betreiber von Netzwerken mit einer großen Reichweite beziehungsweise ohne Passwortschutz, als auch für Private zu erheblichen Haftungsrisiken: Verschafft sich ein Dritter Zugang zu dem Netzwerk haftet trotzdem der Betreiber.
Aufsehen erregte im letzten Jahr das Urteil des EuGH,[12] der Art. 12 der RL 2000/31/EG (E-Commerce-Richtlinie) dahingehend auslegte, dass die Richtlinie einer verschuldensunabhängigen Haftung des WLAN-Betreibers entgegenstehe. Demnach besteht gegen den Betreiber auch kein Unterlassungsanspruch wie bisher angenommen.

II. Aktuelle Entwicklung: Dritte Änderung des Telemediengesetzes

Der Zustand der Rechtsunsicherheit soll nun durch die dritte Änderung des Telemediengesetzes (TMG) beseitigt werden. Wurde mit der zweiten Änderung des TMG[13] klargestellt, dass auch das WLAN als Funknetzwerk § 8 TMG unterfällt, reicht die diesjährige Neuregelung weiter: Zukünftig ist eine Schadensersatzhaftung des WLAN-Betreibers oder ein Anspruch auf Beseitigung / Unterlassung gegen ihn nicht mehr verschuldensunabhängig möglich, § 7 Abs. 1 Satz 2 TMG n.F. Als ultima ratio kann bei einer Verletzung des geistigen Eigentums von dem WLAN-Betreiber verlangt werden, eine Sperrung bestimmter Informationen vorzunehmen, um so eine erneute Rechtsverletzung zu verhindern, § 7 Abs. 4 TMG n.F. Aber auch hierbei dürfen ihm keine außergerichtlichen Kosten auferlegt werden. Zudem hat der Gesetzgeber von einer Pflicht zur Verschlüsselung oder Absicherung, wie sie der EuGH für möglich hält,[14] mittels eines Passwortes abgesehen.

Durch die Änderung des TMG kommt es somit zur Abschaffung der Störerhaftung und damit insgesamt zu weniger Rechtsunsicherheiten. Auch der Private kann sich nun unbeschwerter seines Netzwerkes erfreuen.

Mobile-Health – Fluch oder Segen?

Auch der aktuelle Fitness-/Health-Trend findet sich in der digitalen Umgebung wieder: Smartphones oder Smartwatches werden zur Messung der wichtigsten Körperfunktionen[15] und dem Tracking des absolvierten Trainings genutzt, Kontaktlinsen können den Blutzucker messen[16] und Apps bieten eine Schnelldiagnostik anhand der Symptome an[17]. Die Wichtigkeit dieser Thematik spiegelt sich nicht nur an der Zahl von mindestens einhunderttausend Mobile-Health-Apps auf den gängigen Plattformen wie iTunes und GooglePlay[18] wieder, sondern auch darin, dass sich die Europäische Kommission seit 2014 damit beschäftigt[19].
Doch dieser Trend hat nicht nur Vorteile: Einerseits ermöglicht die Auswertung der sensiblen Daten zwar eine schnellere Diagnostik, die Förderung des internationalen Austausches, sodass seltene Krankheiten besser erkannt werden, individuelle Erinnerungen an die Einnahme von Medikamenten sowie Einsparungen im Gesundheitswesen.[20]
Andererseits ergibt sich genau aus der Sensibilität dieser Daten ein großes Problem. Denn aus ihnen entsteht nicht nur ein aufschlussreiches Bewegungsprofil des Nutzers, sondern die Daten ermöglichen auch einen Rückschluss auf den Gesundheitszustand und die Lebensgewohnheiten des Einzelnen.[21] Durch die Aufzeichnung und Speicherung dieser hochsensiblen Daten korreliert indes das Bedürfnis nach entsprechenden Sicherheitsvorkehrungen.[22] Risiken ergeben sich hierbei an den unterschiedlichen Stellen der Aufzeichnung, Nutzung und Weitergabe: Durch die Verwendung entsprechender Software (beispielsweise Apps), bei der Speicherung auf dem eigenen Smartphone oder in einer Cloud und durch das Übermitteln an andere Geräte macht sich der Nutzer angreifbar, sodass seine Daten in die Hände unberechtigter Dritter fallen könnten.

Smart Home – das „intelligente" Zuhause

Doch dies scheint erst der Anfang der zunehmenden Vernetzung zu sein: Seit Jahren präsentieren die Hersteller auf der Internationalen Funkausstellung (IFA) Haushaltsgegenstände, die untereinander kommunizieren oder beispielsweise über das Smartphone ferngesteuert werden. Live-Bilder von Kameras aus dem Kühlschrank während des Einkaufens,[23] eine KI (künstliche Intelligenz) die veranlasst, dass Fenster bei unerwartetem Regen geschlossen werden[24] oder eine Kaffeemaschine die ihren Besitzer morgens mit frisch gebrühtem Kaffee weckt[25] sind keine Zukunftsfantasien mehr.

I. „smart" und risikobehaftet

Ungeachtet der Vorteile und Annehmlichkeiten, die eine solche Vernetzung mit sich bringt, ergeben sich vor allem für die eigenen Wohnräume, als Teil der Privatsphäre, Risiken. Dieser Bereich ist gerade vor der Öffentlichkeit

12 EuGH, Urt. v. 15.09.2016 – C – 484/14 = ZD 2016, 578, 582.

13 Zweites Gesetz zur Änderung des Telemediengesetzes vom 21.07.2016, BGBl. I S.1766 – 1767.

14 EuGH, Urt. v. 15.09.2016 – C – 484/14 = ZD 2016, 578, 582.

15 Grünbuch der Europäischen Kommission über Mobile-Health-Dienste vom 10.04.2014, abrufbar unter: http://europa.eu/rapid/press-release_IP-14-394_de.htm (12.09.2017), S. 3.

16 https://www.welt.de/gesundheit/video123964775/Die-Google-Kontaktlinse-misst-Blutzucker.html (12.09.2017).

17 Bspw. Hustenerkennung durch eine App, Fraunhofer IDMT, Presseinformation: Neue App erkennt Hustenart am Klang, vom 09.12.2013, S.1.

18 *Al Issawi*, Forschungsbeiträge der eResult GmbH, abrufbar unter: http://www.eresult.de/ux-wissen/forschungsbeitraege/einzelansicht/news/ (12.09.2017); Research-2Guidance, „The mobile health global market report 2013-2017: the commercialisation of mHealth apps", S.7.

19 Siehe Fn.16.

20 *Heimhalt/Rehmann*, MPR 2014, 197, 198; Alich, in: Teager (Hrsg.) IT und Internet – mit Recht gestalten, S. 561; Grünbuch der Europäischen Kommission (siehe Fn. 16), S. 4 f.

21 *Kremer* in: Auer-Reinsdorff/Conrad (Hrsg.) Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 28 Rn.64.

22 *Alich*, in: Teager (Hrsg.) IT und Internet – mit Recht gestalten, S. 561, 570 ff.

23 U.a. http://www.bosch-home.com/de/produktliste/kuehlen-gefrieren/kuehl-gefrier-kombinationen/freistehende-kuehl-gefrier-kombinationen-gefrierteil-unten/KGN36HI32 (12.09.2017), Cimiano/Herlitz, NZM 2016, 409, 412 f.

24 Vgl. BPatG, Beschl. v. 13.06.2017 – 29 W (pat) 531/17 = BeckRS 2017, 122179, Rn. 18.

25 Vgl. „The Barisieur", http://www.barisieur.com/ (12.09.2017).

verschlossen, sodass kein unbefugter Dritter die Möglichkeit haben soll einzudringen. Schwachstellen, die es Dritten ermöglichen auf das Smart Home zuzugreifen, sind dabei nicht nur in der Hard- und Software der Hersteller,[26] sondern auch in dem unbedarften Verhalten der Nutzer zu finden. Wird der Zugang nicht durch ein Passwort geschützt und werden keine regelmäßigen Updates durchgeführt, so hat ein Außenstehender leichtes Spiel.

Neben der Möglichkeit abzuschätzen, wann niemand im Haus ist, und dem Abstellen der Alarmanlage, um einen Diebeszug einfacher zu gestalten, ist auch denkbar, das Smart Home mit einer Malware zu infizieren und erst nach Zahlung eines Lösegeldes den Bewohnern wieder die Steuerung zu überlassen. Bei der klassischen Form des Eindringens, dem Einbruch, macht den Opfern neben dem Verlust von materiellen Gütern vor allem zu schaffen, dass es jemandem gelungen ist, in diesen intimen Teil ihres Lebens einzudringen;[27] sie fühlen sich schlicht nicht mehr sicher.

Dabei sind beim Einbruch „immerhin" unübersehbare Spuren des Eindringens vorhanden, die sich im Gegensatz dazu bei einem „digitalen Einbruch" nicht, oder nicht so offensichtlich zeigen.

II. Smart Home und Datensicherheit

Darüber hinaus sammeln auch alle vernetzten Geräte des Smart Homes bei jeder Nutzung Daten, sodass ein umfassendes Profil über die Lebensgewohnheiten der darin lebenden Menschen entsteht.[28]

Gerade in diesen Punkten zeigt sich das gesteigerte Bedürfnis nach Sicherheit und Schutz dieser Systeme:[29] Einerseits geht es um einen höchstpersönlichen Teil des Lebens und um empfindliche Daten, andererseits sind die Spuren eines Eindringens in diesen Bereichen nur schwer erkennbar.

Fazit

Der Digitalisierungsprozess schlägt sich zunehmend auch im privaten Bereich und damit auch zuhause nieder. Doch die Vernetzung bietet nicht nur Vorteile, sondern birgt aufgrund der besonders sensiblen Daten auch Risiken, insbesondere durch Angriffe von Dritten, die fast spurlos erfolgen können. Daher besteht in diesem Bereich des Lebens ein besonderes Interesse an einem umfassenden Schutz.

Rachut

26 Vgl. *Vogelgesang/Hessel*, ZD 2017, 269 ff.

27 BT/Drs. 13/8587, S.43.

28 *Guckelberger*, DÖV 2012, 613, 618 ff.; *Keppeler*, EnWZ 2016, 99, 100.

29 *Keppeler*, EnWZ 2016, 99, 100.

Woche 4: Cyber-Sicherheit vermitteln - an Profis und Anwender

2017 scheint, zumindest was die Sicherheit in der Informationstechnik anbelangt, als das „Jahr der Ransomware“ in die Geschichte eingehen zu wollen. Nachdem bereits im Mai dieses Jahres das Schadprogramm „WannaCry“ über 200.000 Organisationen und Einzelpersonen in 150 Ländern infiziert hatte,[1] erfolgte Ende Juni ein zweiter Angriff, diesmal mithilfe des „Petya“-Trojaners, der vorwiegend die Ukraine traf. In beiden Fällen waren jedoch auch namhafte deutsche Unternehmen betroffen, etwa die Deutsche Bahn AG oder die Beiersdorf AG. Bei Ransomware handelt es sich um Software, die sämtliche Daten des infizierten IT-Systems verschlüsselt und nur gegen Zahlung einer Geldsumme in vorgegebener Höhe (möglicherweise) wieder freigibt.[2] Im besten Fall reduzieren sich die Folgen eines Ransomware-Angriffs auf einen wirtschaftlichen Schaden, im schlimmsten Fall droht der Totalverlust sämtlicher betroffener Daten.

Diese beiden Vorfälle, von denen insbesondere letzterer vermeidbar gewesen sein soll, machen deutlich, wie wichtig ein angemessenes IT-Sicherheitsniveau in unserer globalisierten und digitalen Welt ist. Deshalb soll im Folgenden aufgezeigt werden, wie sich möglichst effektiv und ohne zu großen Aufwand ein hinreichendes IT-sicherheitsrechtliches Schutzniveau verwirklichen lässt.

Grundlagen und Ansatzpunkte für IT-Sicherheit

Nach der Legaldefinition des § 2 Abs. 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) ist IT-Sicherheit die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen. Dabei lassen sich grundsätzlich zwei Ansatzpunkten unterscheiden, um IT-Sicherheit im Unternehmen herzustellen: zum einen durch Organisation, zum anderen durch Technik.[3]

Die organisatorische Komponente bezweckt die sichere Interaktion von Mensch mit Maschine. Hierbei geht es darum, Sicherheitslücken, die unbewusst durch den Benutzer geschaffen werden, zu schließen, bzw. von Anfang an zu vermeiden. Die folgende, nicht abschließende Aufzählung soll einen ersten Überblick über mögliche organisatorische Handlungsmaßnahmen bieten:

- Schulung und Sensibilisierung der Mitarbeiter
- Einrichtung kompetenter Ansprechpartner
- Erstellung von IT-Sicherheitsrichtlinien sowie Verpflichtung der Mitarbeiter diese einzuhalten
- Verbot der Nutzung privater Endgeräte sowie der privaten Computer- und Internetnutzung
- Meldung und Dokumentation von Zwischenfällen
- Erstellung eines qualifizierten Notfallplans
- Einrichtung von Zutrittskontrollen

Weitere Informationen können Sie unter https://www.baywidi.de/wiki/allgemeine-handlungsempfehlungen-zur-it-sicherheit/allgemeine-organisatorische-handlungsempfehlungen/ einsehen.

Die technische Komponente auf der anderen Seite erfasst die Sicherheit des IT-Systems selbst. Dadurch sollen externe Zugriffe erschwert sowie technisch induzierte Fehler vermieden werden. Insbesondere die folgenden, wiederum nicht abschließenden Handlungsempfehlungen sind zu beachten:

- Verschlüsselung lokaler Computer sowie sensibler Daten
- Absicherung mobiler Geräte
- Beschränkung der Zugriffsrechte
- Regelmäßige Softwareupdates
- Einsatz geschützter Kommunikation sowie von Firewalls

Weitere Informationen können Sie unter https://www.baywidi.de/wiki/allgemeine-handlungsempfehlungen-zur-it-sicherheit/allgemeine-technische-handlungsempfehlungen/ einsehen.

Eine besonders wichtige Rolle kommt dem IT-Sicherheitsbeauftragten zu. In den meisten Bereichen ist dieses Amt zwar nicht gesetzlich vorgeschrieben,[4] dessen Beschäftigung empfiehlt sich jedoch bereits im eigenen Interesse eines jeden Unternehmens.[5] Der IT-Sicherheitsbeauftragte ist für die Wahrung der IT-Sicherheit sowie für deren Überwachung zuständig, sorgt also dafür, dass

1 Vgl. http://www.n-tv.de/technik/Nordkorea-findet-Cyber-Vorwurf-laecherlich-article19850909.html (abgerufen am 28.09.2017).

2 *Scheurer*, AnwZert ITR 6/2017 Anm. 2.

3 So auch *Karg*, in: Wolff/Brink, BeckOK DatenSR, 20. Edition Stand 01.05.2017, BDSG § 9 Rn. 83.

4 Zu dessen Funktion und Aufgaben ferner *Grützner/Jakob*, in: Compliance von A-Z, 2. Aufl. 2015, IT-Sicherheitsbeauftragter.

5 *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 251.

das jeweilige IT-sicherheitsrechtliche Konzept entsprechend umgesetzt und eingehalten wird.[6] Er ist damit der Hauptansprechpartner im Unternehmen, was sämtliche Fragen rund um IT-Sicherheit anbelangt.[7]

IT-Sicherheitsstandards

Anknüpfend an die eingangs vorgestellte Definition der IT-Sicherheit genügt es nicht nur vereinzelt Maßnahmen zu treffen, um ein angemessenes IT-Sicherheitsniveau zu erreichen. Zwar lässt sich auch auf diese Weise ein Information Security Management System (ISMS, Managementsystem für Informationssicherheit) einrichten. Um jedoch garantieren zu können, dass ein Unternehmen einem bestimmten IT-Sicherheitsniveau entspricht, besteht die Möglichkeit der Zertifizierung nach einem anerkannten Sicherheitsstandard. Diese Standards werden weltweit von zahlreichen verschiedenen Gremien entwickelt. Damit wird das Ziel verfolgt, ein in sich kohärentes und abgeschlossenes Schutzniveau zu präsentieren, um letztlich einen umfassenden Schutz auf einem vordefinierten Sicherheitsniveau garantieren zu können. Die Umsetzung nur vereinzelter Aspekte resultiert dagegen in einem lückenhaften Schutz. Zwar wird die Zertifizierung gesetzlich nur im Ausnahmefall, so etwa für kritische Infrastrukturen[8], vorgeschrieben, doch empfiehlt sich diese auch aus anderen Gründen. Insbesondere kann sich eine IT-sicherheitsrechtliche Zertifizierung nach einem anerkannten Sicherheitsstandard haftungsreduzierend auswirken, im Wettbewerb aufgrund der Erwartungen des Kunden einen Vorteil gegenüber anderen Unternehmen, die nicht zertifiziert sind, bringen sowie letzten Endes Kosten, die durch unerwartete Ausfälle und Störungen entstehen könnten, vermeiden.[9]

Angesichts der Vielzahl an Standards und der diese umsetzenden Konzepte sollen an dieser Stelle einige der wichtigsten und gebräuchlichsten Standards, insbesondere hinsichtlich deren Eignung für kleine bis mittelständische Unternehmen dargestellt werden.

I. IT-Grundschutzkatalog

Der IT-Grundschutzkatalog wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und laufend dem Stand der Technik angepasst. Ursprünglich für Behörden entwickelt, ist das Konzept mittlerweile an den nachfolgend erläuterten ISO/IEC 27001 Standard angepasst worden, sodass auch die Zertifizierung nach ISO/IEC 27001 auf Basis des Grundschutzkatalogs möglich ist.[10]

Positiv zu bewerten ist die Aufteilung in die Kataloge Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge. Dies hat die praktische Folge, dass auch nur einzelne Kataloge umgesetzt werden können, wenn die Anwendung des Grundschutzkatalogs im Ganzen nicht erwünscht ist. Dies wiederum kommt aufgrund der umfangreichen Ausführungen des Grundschutzkatalogs insbesondere kleineren Unternehmen zugute, die lediglich hinsichtlich bestimmter Bereiche Hinweise zur IT-sicherheitsrechtlich konformen Ausgestaltung ihres Betriebs suchen. Auch die Kompatibilität mit ISO/IEC 27001 einschließlich Zertifizierung spricht für den IT-Grundschutzkatalog.[11]

Allerding ist die Umsetzung des gesamten Konzepts mit einem erheblichen Aufwand verbunden, sodass sich dies tendenziell nur für mittelständische und größere Unternehmen empfiehlt. Auch die Komplexität sowie Ausführlichkeit der Erläuterungen des IT-Grundschutzkatalogs können ohne entsprechende Vorkenntnisse zu einer Überforderung des Anwenders führen.[12]

II. ISO/IEC 27001

Der Standard ISO/IEC 27001 zeichnet sich insbesondere durch einen individuellen Ansatz aus. Ziel der Norm ist, anhand des „Plan-Do-Check-Act"-Zyklus[13] ein am individuellen Bedarf angepasstes Sicherheitskonzept zur Verfügung zu stellen, um auf diesem Weg ein hinreichendes Sicherheitsniveau zu erzielen. Demnach wird vor allem ein prozessorientierter Ansatz verfolgt.

Positiv hervorzuheben ist der geringe technische Detaillierungsgrad, der sich aus dem prozessorientierten Ansatz ergibt.[14]

Demgegenüber stehen jedoch hohe Kosten, die sich zwangsläufig aus dem Aufbau der zugrundeliegenden Organisation sowie des Zertifizierungsprozesses ergeben. Für kleine bis mittelständische Unternehmen kann mit einer Umsetzungsdauer von 30-50 Tagen bei einer Vollzeitstelle gerechnet werden. Die Zertifizierung selbst kann erst nach drei Jahren erfolgen.[15]

Dieser Standard wird ferner durch ISO/IEC 27002 erweitert. Dabei handelt es sich um Empfehlungen nach dem »Best-Practise«-Ansatz, die je nach Bedarf eingesetzt, weggelassen oder ersetzt werden können.[16] Eine eigene Zertifizierung hierfür gibt es nicht.

III. ISIS 12

Hierbei handelt es sich um ein eine „Light"-Version des IT-Grundschutzkatalogs, die deren wesentliche Punkte einbezieht, weshalb ein späteres Upgrade auf den Grundschutzkatalog in vollem Umfang möglich ist.[17] Folglich eignet sich dieses gut für den Einstieg. Zusätzlich werden regelmäßig Schulungstermine

6 *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 274 ff, 289 ff.

7 Vgl. weiterführend https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Muster/muster_bestellung_it-sibe_doc.doc?__blob=publicationFile&v=1 (abgerufen am 21.09.2017).

8 Weiterführend *Hornung*, NJW 2015, 3334, 3336 ff.

9 https://www.pct.eu/blog/blog-lesen/zertifizierung-warum-das-von-vorteil-ist.html (abgerufen am 21.09.2017).

10 Details abrufbar unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html (abgerufen am 21.09.2017).

11 So i.E. auch *Schröder*, in: Datenschutzrecht, 2. Aufl. 2016, 6. Kapitel Technische Organisatorische Maßnahmen/Datensicherheit, II. 2. a).

12 *Greveler/Reinermann*, CCZ 2015, 274, 275.

13 *Greveler/Reinermann*, CCZ 2015, 274, 275.

14 *Greveler/Reinermann*, CCZ 2015, 274, 275.

15 *Wittmann*, ISO 27001 - Stempel mit Aussagekraft?, https://www.computerwoche.de/a/iso-27001-stempel-mit-aussagekraft,2555531 (abgerufen am 21.09.2017).

16 Vgl. *Schmidl*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 127.

17 So auch *Stoklas*: ZD-Aktuell 2016, 05146.

durchgeführt. Zu berücksichtigen ist, dass Handbuch und Katalog nur gegen eine Schutzgebühr von etwa 150 Euro erhältlich sind.[18]

IV. VdS Cyber-Richtlinie 3473

Auch bei dem Maßnahmenkatalog der VdS-Richtlinie[19] handelt es sich, wie bei ISIS 12, um reduzierte technische und organisatorische Vorgaben. Dies hat eine grundsätzlich leichte Implementierung zur Folge, was sich auf der anderen Seite allerdings auch in einem geringeren Schutzniveau niederschlägt.[20]

Beispiel: Ein Viren-Schutzkonzept nach IT-Grundschutz

Einen Einblick in ein mögliches Schutzkonzept nach IT-Grundschutz gegen Computer-Viren soll der nachfolgende Maßnahmenkatalog jedenfalls in Ansätzen ermöglichen, einen Anspruch auf Vollständigkeit erhebt dieser nicht.

Zunächst ist erforderlich, die Mitarbeiter hinsichtlich der Verwendung von E-Mails, des Internets und des internen Netzes sowie der Nutzung von Wechseldatenträgern zu sensibilisieren. Auf diese Weise kann die Infektion des Systems mit Viren von vornherein vermieden werden. Zusätzlich sind die Mitarbeiter über die Bedeutung des IT-Systems sowie das Gefährdungspotential von Viren

für dieses zu informieren. Auch über die korrekte Benutzung des Anti-Virenprogramms sowie über Verhalten im Falle des Auftretens von Schadsoftware sind diese zu unterrichten.

Ferner sind sämtliche IT-Systeme zu ermitteln, die grundsätzlich für Viren anfällig sind. Zu beachten ist, dass Geräte, die nicht zwingend mit anderen Rechnern im Netzwerk verbunden sein müssen, auch nicht verbunden sein sollten. Weiterhin ist ein zentraler Virenschutz durch die Installation eines Anti-Virenprogramms einzurichten.

Dem IT-Sicherheitsbeauftragten ist die Funktion des zentralen Computer-Viren-Verantwortlichen als Aufgabe zu übertragen.

> Weitere Musterbeispiele können Sie unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html abrufen.

Eine erste Bestandsaufnahme

Angesichts der vielen verschiedenen Konzepte kann der Schritt hin zu einer sicheren IT-Infrastruktur Schwierigkeiten bereiten. Zu Beginn ist in jedem Fall immer eine Sicherheitsanalyse durchzuführen, die etwaige bestehende Schwachstellen aufzeigen kann. Erst danach, wenn der konkrete Bedarf hinsichtlich eines bestimmten IT-Sicherheitsbedürfnisses ermittelt ist, kann und sollte die Wahl eines für das Unternehmen passenden Konzepts getroffen werden.

Einen ersten Anhaltspunkt hierfür bietet der Online-Sicherheitscheck des Vereins Deutschland sicher im Netz, DsiN e.V., der unter der Schirmherrschaft des Bundesministeriums des Inneren entwickelt wurde und sich vor allem an kleine und mittelständische Unternehmen richtet. Unmittelbar anschließend an die Beantwortung eines Fragenkatalogs werden erste Handlungsempfehlungen sowie weiterführende Informationen zur Verfügung gestellt. Der Sicherheitscheck kann unter www.dsin-sicherheitscheck.de/ kostenlos abgerufen und durchgeführt werden.

Brand/Scheurer

18 Weitere Informationen stehen unter https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12/isis12-fuer-kmu.html (abgerufen am 21.09.2017) zum Abruf bereit.

19 Abrufbar unter https://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf (abgerufen am 21.09.2017).

20 Vgl. weiterführend *Greveler/Reinermann*, CCZ 2015, 274, 277 ff.

Der nächste Newsletter erscheint im Januar 2018.

Sie finden den Newsletter und die Möglichkeit, sich an-, bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie einfach an baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.