Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft

Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Datum: 20.02.2018

Autoren

Goldmedia GmbH
Strategy Consulting
Prof. Dr. Klaus Goldhammer
Dr. André Wiegand
Sebastian Lehr

if(is) - Institut für Internet-Sicherheit,
Westfälische Hochschule, Gelsenkirchen
Prof. Norbert Pohlmann
Chris Wojzechowski
Johnny Hoang
Ole Jötten

IRNIK - Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie
Dr. Alexander Koch

Inhalt

1 Fragestellung und Methodik

1.1 Ziel der Studie

Der Einsatz elektronischer Verschlüsselung von Daten und der Datenkommunikation gewährleistet im Unternehmensumfeld sowohl den Schutz des geistigen Eigentums vor Wirtschaftsspionage als auch den Schutz der Unternehmens- und Kundendaten vor Missbrauch.

Verschlüsselungslösungen werden Marktanalysen zufolge gerade in kleinen und mittleren Unternehmen (KMU) bislang nur begrenzt eingesetzt.

Die Projektpartner Goldmedia Strategy, Consulting, Institut für Internet-Sicherheit, if(is) und Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie (IRNIK) wurden vom Bundesministerium für Wirtschaft und Energie (BMWi) damit beauftragt,

1. die **bestehenden Motivationsgründe und Hemmnisse** beim Einsatz elektronischer Verschlüsselung in KMU strukturiert zu erfassen und
2. **Ableitungen und Handlungsempfehlungen zur Senkung von Umsetzungsschwellen und zur gezielten Förderung des Einsatzes** von elektronischen Verschlüsselungslösungen zu erstellen.

1.2 Inhalte der Studie

Die **Analyse der spezifischen Hemmnisse und Motivationsgründe beim Einsatz von Verschlüsselungslösungen** in KMU erfolgte auf Basis einer kombinierten Online- und Telefon-Befragung von rund 200 Unternehmen unterschiedlicher Größe und aus unterschiedlichen Branchen und wurde durch rund 25 Experteninterviews mit Anwendern und Herstellern von Verschlüsselungslösungen gestützt.

Parallel zur Bestimmung der Umsetzungshürden beim Einsatz von Verschlüsselungslösungen in KMU erfolgte eine **Analyse der aktuellen rechtlichen und organisatorischen Anforderungen an Unternehmen zu den Themen IT-Sicherheit und Datenschutz** mit Blick auf das Thema Verschlüsselung. Die zu analysierenden Rechtsbereiche umfassten u.a. das Datenschutzrecht, das Sozialrecht, das Abgaben- und Steuerrecht, das Gesellschaftsrecht sowie das Vertragsrecht. Ziel war es hier, rechtliche Treiber und Hebel zu identifizieren, die den stärkeren Einsatz von Verschlüsselungslösungen in Unternehmen vorschreiben oder nahelegen.

Zusätzlich wurde im Rahmen des Projekts der **Kompass IT-Verschlüsselung** als konkrete Orientierungshilfe für KMU entwickelt. Der Kompass IT-Verschlüsselung zeigt auf, welche Verschlüsselungslösungen sich für welchen Anwendungsfall und für welche Unternehmensgröße eignen.

1.3 Methodisches Vorgehen

Auftrag der Studie war es, im Rahmen einer **kombinierten Online- und Telefon-Befragung** die derzeitige Verbreitung von Verschlüsselungslösungen in KMU zu erheben und sowohl die Motivationsgründe als auch die Hemmnisse bei Implementierung und laufendem Betrieb zu erfassen.

Hierfür wurde im ersten, vorbereitenden Schritt im Februar 2017 **eine explorative Vorstudie** unter den Anbietern von Lösungen und Dienstleistungen für IT-Sicherheit durchgeführt. Die Teilnehmer an der Vorstudie wurden durch einen Aufruf per E-Mail an die Mitgliedsunternehmen des TeleTrusT - Bundesverband IT-Sicherheit e.V. gewonnen.

Ziel dieser explorativen Vorerhebung (schriftlicher Fragebogen mit offen formulierten Leitfragen) und begleitender Experten-Interviews war es, Motivationsgründe, Hemmnisse und Anwenderfreundlichkeit elektronischer Verschlüsselungslösungen aus Sicht der Anbieter und Hersteller zu erheben.

Die Ergebnisse der Vorerhebung flossen in die Hypothesenbildung und die Entwicklung der Gliederung und Formulierung des Fragebogens der Online-Unternehmensbefragung ein.

Die **anschließende Online-Unternehmensbefragung** von Unternehmen zum Einsatz von Verschlüsselungslösungen wurde wie folgt umgesetzt:

- Zielpersonen in den Unternehmen waren Personen, die Auskunft zum Status der IT-Sicherheit im Unternehmen geben konnten. Hierzu zählen vor allem: Geschäftsführer/CEO, Leiter IT/CIO/CTO und Information Security Manager/IT-Sicherheitsbeauftragter/CISO/CSO.
- Die Teilnehmer wurden unter Mithilfe zahlreicher Branchenverbände und Sicherheitsinitiativen gewonnen. Die Branchenverbände und Initiativen bewarben die Umfrage über ihre Kommunikationskanäle im Mitgliederkreis.
- Ergänzend wurden zusätzliche Teilnehmer über ein Online-Unternehmenspanel generiert.
- Vertiefende Experteninterviews wurden mit ausgewählten Teilnehmern der Online-Unternehmensbefragung geführt, die hierfür im Verlauf der Befragung explizit ihr Einverständnis erklärt hatten. Ziel dieser flankierenden Telefoninterviews war es, zusätzliche Erläuterungen und spezifische Begründungszusammenhänge direkt von den Teilnehmern der Online-Befragung zu erhalten.

Nach Auswertung der Datensätze sowie Abschluss der rechtlichen Analyse wurde im September 2017 in Bonn ein Ergebnisworkshop mit ausgewählten Experten aus dem IT-Sicherheitsbereich durchgeführt, in dem mögliche Handlungsempfehlungen und weitere Schritte zur Stärkung des Einsatzes von Verschlüsselungslösungen in KMU diskutiert wurden.

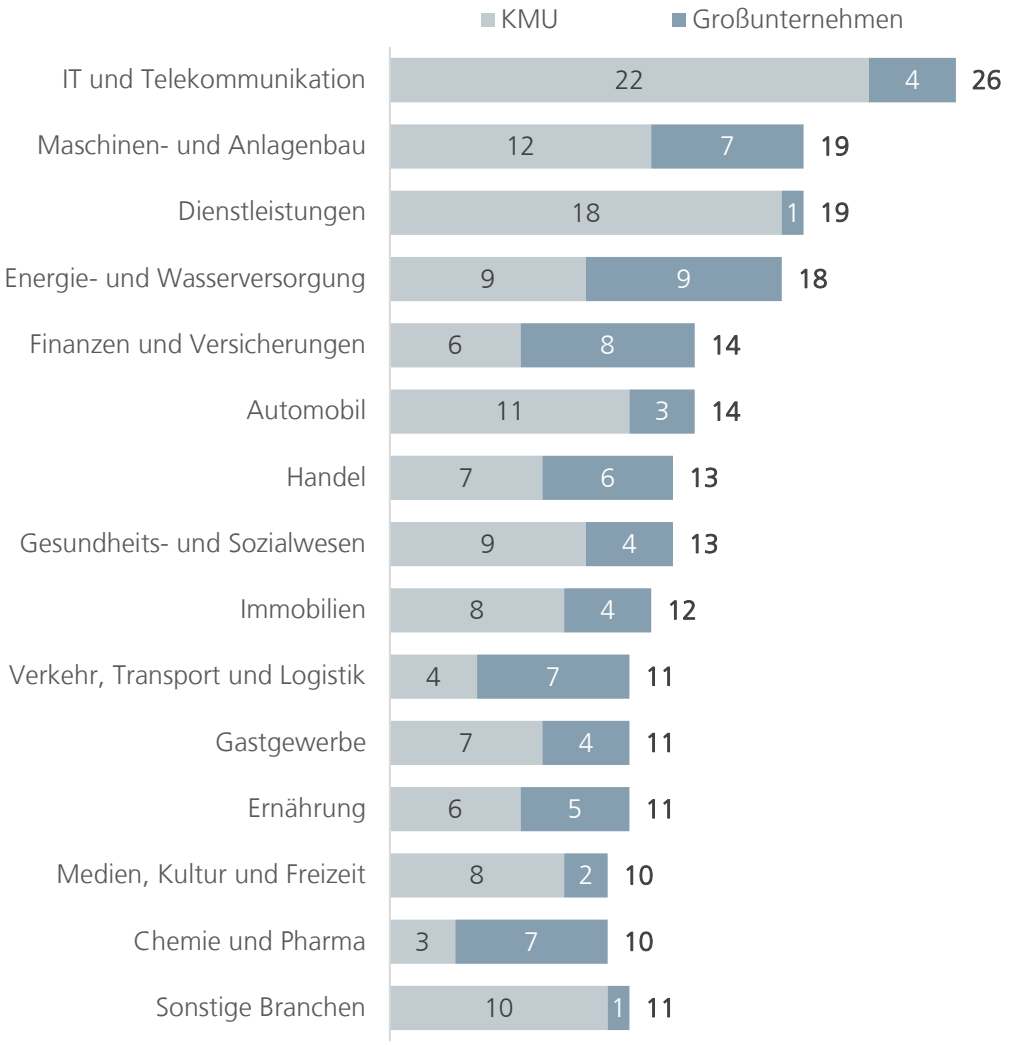
1.4 Erzielte Stichprobe

Die Durchführung der Befragung erfolgte vom 14.03. bis 31.05.2017. Hierbei konnte folgende Umfragebeteiligung realisiert werden:

- Über die Bewerbung der Umfrage durch die Verbände und Initiativen konnten 90 Unternehmen für die Befragung gewonnen werden. Mit 25 dieser Unternehmen wurde die Befragung telefonisch durchgeführt, um weitere Hintergrundinformationen und Einschätzungen der (Nicht-)Anwender aufnehmen und konkreter auf die Situation im Unternehmen eingehen zu können.
- Weitere 130 Unternehmen wurden über ein Online-Panel akquiriert, wovon nach Prüfung der Qualität (Plausibilität, semantische Prüfung, Entfernung von Durchklickern) 122 Antworten verwertet werden konnten.
- In Summe konnten so 212 verwertbare Datensätze generiert werden, davon 140 Antworten von Unternehmen mit weniger als 500 Mitarbeitern (KMU).
- Unter den KMU war vor allem aus den Branchen IT und Telekommunikation (n=22) sowie Dienstleistungen (n=18) eine vglw. starke Umfragebeteiligung zu verzeichnen. Im Gegensatz dazu haben sich Unternehmen aus der Chemie- und Pharmabranche (n=3) sowie Unternehmen aus dem Bereich Verkehr, Transport und Logistik (n=4) nur gering beteiligt. Zu den sonstigen Branchen zählen u.a. Unternehmen aus dem Handwerk oder der Wissenschaft und Forschung (n=10).
- Die Klassifizierung der Unternehmen nach Mitarbeitergrößenklassen zeigt eine robuste Datenlage für kleine und mittlere Unternehmen mit jeweils 30 oder mehr Umfrageteilnehmern. Im Vergleich dazu zeigt sich bei den Kleinstunternehmen (weniger als zehn Mitarbeiter) eine geringere Beteiligung (n=21).

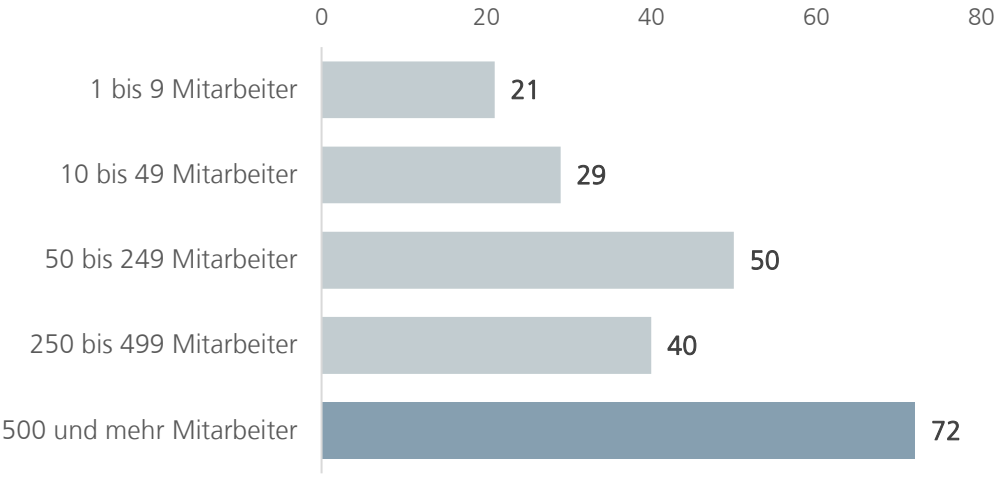
Die nachfolgende Darstellung der Ergebnisse konzentriert sich auf die Angaben der kleinen und mittleren Unternehmen als Kernzielgruppe der Studie. Dort, wo sich signifikante Unterschiede zu den Angaben der Großunternehmen (> 500 Mitarbeiter) ergeben, wird dies herausgestellt.

Abb. 1: Anzahl befragter Unternehmen nach Branche



Quelle: Goldmedia Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=212

Abb. 2: Anzahl befragter Unternehmen nach Mitarbeiterklassen



Quelle: Goldmedia Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=212

2 Struktur der Unternehmensbefragung

Die Online-Unternehmensbefragung gliedert sich in **vier wesentliche Abschnitte**, um sowohl allgemeine Aspekte der Unternehmen (z.B. Unternehmensgröße, Branchenzugehörigkeit) und allgemeine Einschätzungen zur Verschlüsselung ebenso strukturiert zu erfassen wie die konkreten Erfahrungen im (Nicht-)Einsatz von Verschlüsselungslösungen in spezifischen Anwendungsszenarien. Diese stellen sich wie folgt dar:

- Schutzbedarf des Unternehmens und der Branche
- Allgemeine Aspekte der Verschlüsselung
- Konkrete Nutzung von Verschlüsselung im Unternehmen
- Motivationsgründe und Hemmnisse bei der Nutzung

Schutzbedarf des Unternehmens und der Branche

Im einleitenden Befragungsabschnitt wurden neben der Branchenzughörigkeit und der Unternehmensgröße auch die IT-Abhängigkeit und der spezifische Grad des Schutzbedarfs von IT-Systemen und Daten im jeweiligen Unternehmen erfasst. Diese Fragen bilden die Grundlage für die spätere Branchenauswertung nach Verschlüsselungsbedarf und -umsetzung (Abb. 13).

Allgemeine Aspekte der Verschlüsselung

In diesem Abschnitt wurden die Teilnehmer grundlegend danach gefragt, ob und welche Verfahren der Kommunikations- und Datenverschlüsselung sie in ihrem Unternehmen einsetzen.

Bei Anwendern wurde danach gefragt, welches der ausschlaggebende Grund zur Einführung von Verschlüsselung im Unternehmen gewesen ist. Die Anwender von Verschlüsselungslösungen wurden darüber hinaus auch gefragt, ob und in welchem Umfang es durch die Einführung von Verschlüsselung zu Komfort- und Produktivitätsverlusten im operativen Geschäftsbetrieb gekommen ist.

Bei Nicht-Anwendern von Verschlüsselung wurde hingegen nach der allgemeinen Sensibilisierung für die Verschlüsselungsthematik gefragt und erhoben, ob es in der Vergangenheit bereits (nicht erfolgreiche) Bestrebungen gab, Verschlüsselung im Unternehmen einzuführen.

Konkrete Nutzung von Verschlüsselung im Unternehmen

Es folgten weitergehende Fragen zur Verschlüsselung in unterschiedlichen betrieblichen Anwendungsszenarien, zu den vorrangigen Schutzzielen sowie zur Verbreitung von Verschlüsselungslösungen auf verschiedenen Endgeräten (z.B. Laptops, Smartphones oder USB-Sticks).

Hierbei wurden auch einige spezifische Fragen zu Verschlüsselungsaspekten von Cloud-Lösungen im Unternehmenseinsatz integriert, da der Datensicherheit und -integrität hier ein besonderer Stellenwert zukommt und der Einsatz von Cloud-Lösungen in kleinen und mittleren Unternehmen zunehmende Verbreitung findet.

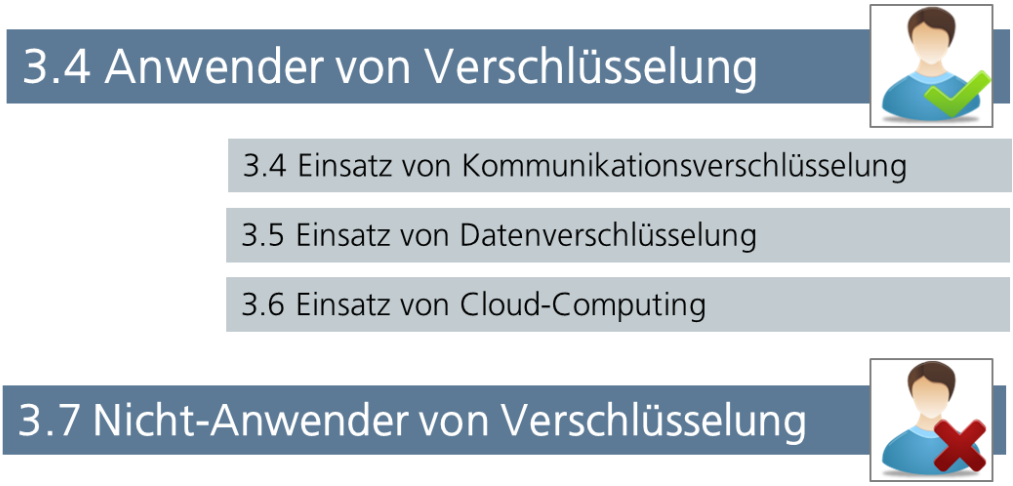
Des Weiteren wurde erhoben, inwiefern der konkrete Einsatz von Verschlüsselung im Unternehmen durch eine Unternehmensrichtlinie geregelt ist und inwieweit diese auch die Speicherung von persönlichen Passwörtern regelt.

Motivationsgründe und Hemmnisse bei der Nutzung

Zentraler Bestandteil der Befragung war die Abfrage der Motivationsgründe und Hemmnisse, die den (Nicht-)Einsatz von Verschlüsselungslösungen maßgeblich beeinflusst haben.

Die Unternehmensbefragung wurde hierbei so konzipiert, dass sie sowohl von Anwendern wie von Nicht-Anwendern von Verschlüsselungslösungen beantwortet werden konnte und diese weitestgehend vergleichbare Fragestellungen zu beantworten hatten. In der Analyse wurden Anwender und Nicht-Anwender zum Teil getrennt ausgewertet, um subjektiv „befürchtete" Hemmnisse von real erfahrenen Hemmnissen im Unternehmenseinsatz von Verschlüsselungslösungen zu unterscheiden.

Abb. 3: Auswertung von Subgruppen (Anwender sowie Nicht-Anwender von Verschlüsselungslösungen) in Kapitel 3



Quelle: Goldmedia

Antworten von Verschlüsselungsanwendern sind durch einen symbolischen grünen Haken zu erkennen, während die Antworten von Nicht-Anwendern symbolisch durch ein rotes Kreuz kenntlich gemacht sind. Die Auswertungen in den Abschnitten 3.4 bis 3.7 erfolgen getrennt für Anwender sowie Nicht-Anwender von Verschlüsselungslösungen.

Handlungsempfehlungen und Fazit

Die Ergebnisse der Befragung gehen unmittelbar in die strategischen Handlungsempfehlungen in Kapitel 5 ein. Dort werden die größten Defizite kleiner und mittlerer Unternehmen in spezifischen Maßnahmen adressiert.

Kapitel 6 zieht ein abschließendes Fazit aus den Studienergebnissen und den daraus entwickelten Handlungsempfehlungen.

3 Ergebnisse der Unternehmensbefragung

3.1 Bedeutung von Verschlüsselung in kleinen und mittleren Unternehmen (KMU)

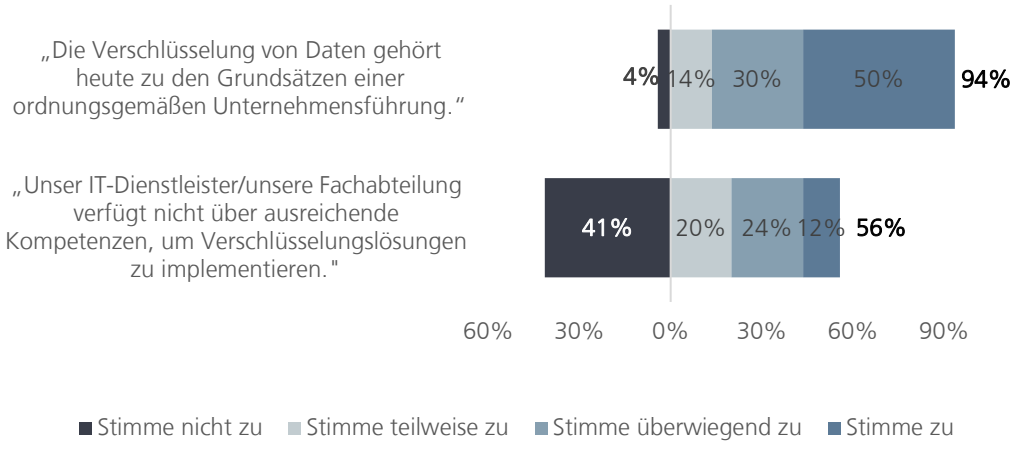
Um grundsätzliche Bedeutung von elektronischer Verschlüsselung in kleinen und mittleren Unternehmen (KMU) in Erfahrung zu bringen, wurde zu Beginn der Befragung erhoben, welcher allgemeine Stellenwert der elektronischen Verschlüsselung im Unternehmensalltag bereits zugemessen wird. Hierfür wurden thesenhaft formulierte Aussagen zur Verschlüsselung zur Diskussion gestellt.

Die Thesen zielten darauf ab, Hemmnisse für Verschlüsselung zu identifizieren und gleichzeitig Treiber für Verschlüsselung, z.B. eine rechtliche Verpflichtung, Kundenanforderungen oder eigene Schadensfälle auszumachen.

Im Ergebnis wiesen kleine und mittlere Unternehmen **grundsätzlich ein hohes Bewusstsein für die Bedeutung von Verschlüsselung im Unternehmen** auf (94 Prozent). Der Großteil der KMU erkannte die prinzipielle Notwendigkeit von Verschlüsselung an und schätzt diese folglich auch als einen Grundsatz einer ordnungsgemäßen Unternehmensführung ein.

Obwohl die Unternehmen sie als Notwendigkeit erkannten, **mangelt es jedoch häufig an der Kompetenz der Fachabteilungen**, Verschlüsselungslösungen zu implementieren: So gaben 56 Prozent der KMU an, nicht über ausreichende Kompetenzen zu verfügen, um Verschlüsselungslösungen zu implementieren.

Abb. 4 Zustimmung zu Thesen zur generellen Bedeutung von Verschlüsselung im eigenen Unternehmen (1/2)

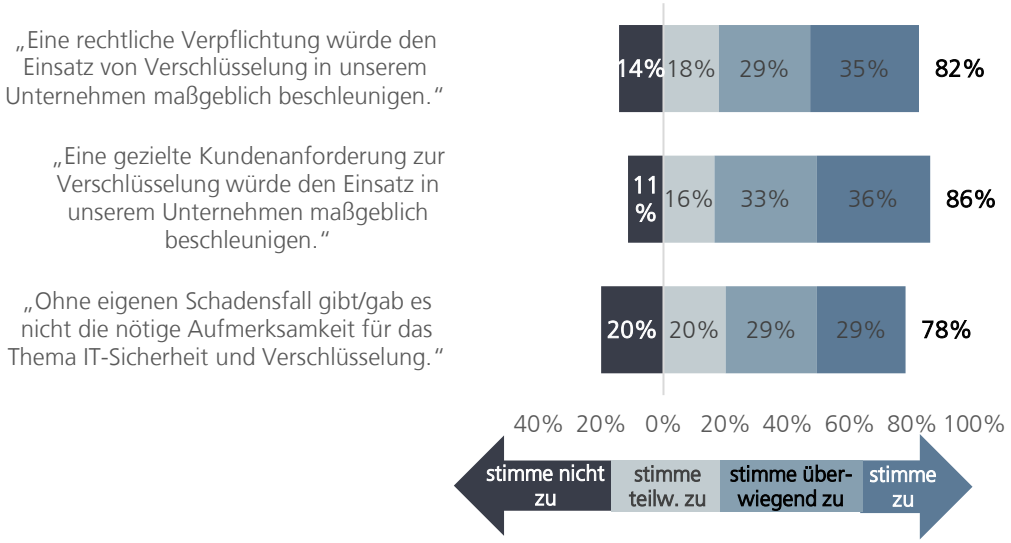


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=140.
Frage: Inwiefern können Sie folgenden Thesen zur generellen Bedeutung von Verschlüsselung in Ihrem Unternehmen zustimmen?

Mit Blick auf (zukünftige) Treiber für den Einsatz von Verschlüsselungslösungen gaben die befragten Unternehmen an, dass gesetzliche Regularien (82 Prozent) und Kundenanforderungen zur Verschlüsselung (86 Prozent) ein effektives Instrument sind, um die Implementierung von Verschlüsselungslösungen zu beschleunigen. Zusätzlich gaben 78 Prozent an, dass ohne eigenen Schadensfall im Unternehmen nicht genügend Aufmerksamkeit für Verschlüsselung generiert wird.

Regulierung, Nachfrage und interne Vorfälle sind demnach gleichrangig ausschlaggebend. Einen vorrangigen Treiber gibt es nicht.

Abb. 5 Zustimmung zu Thesen zur generellen Bedeutung von Verschlüsselung im eigenen Unternehmen (2/2)



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=140.
Frage: Inwiefern können Sie folgenden Thesen zur generellen Bedeutung von Verschlüsselung in Ihrem Unternehmen zustimmen?

3.2 IT-Reifegrad der befragten Unternehmen

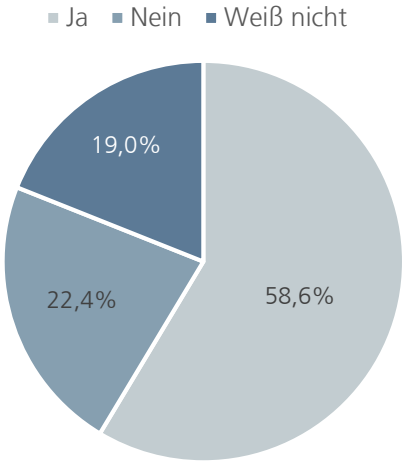
Im nächsten Schritt wurde der IT-Reifegrad der Unternehmen mit Bezug auf verschlüsselungsrelevante Aspekte anhand folgender drei Faktoren abgefragt:

- Verarbeitung personenbezogener Daten
- Grad der IT-Abhängigkeit
- Schutzbedarf und Betriebsgeheimnisse

In der Stichprobe unterlag die Mehrzahl der KMU mit mind. zehn Mitarbeitern höheren datenschutzrechtlichen Auflagen aufgrund der Verarbeitung personenbezogener Daten: 66 Prozent der befragten Unternehmen gaben an, dauerhaft mehr als neun Personen zu beschäftigen, die im Unternehmen personenbezogene Daten verarbeiten.[1]

[1] Goldmedia/if(is)-Befragung „Einsatz elektronischer Verschlüsselung in KMU" 2017, n=119

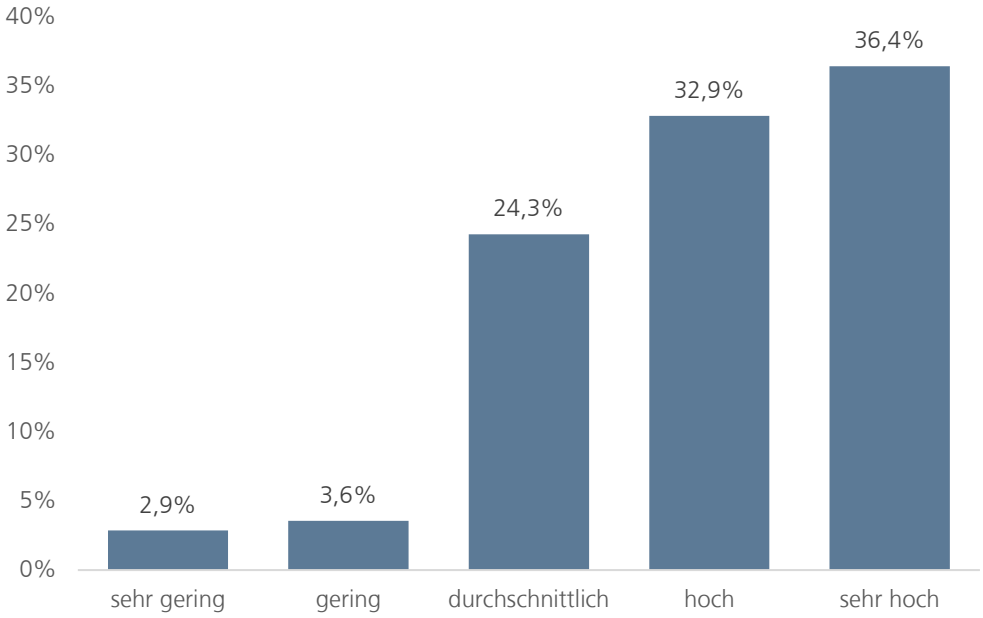
Abb. 6: Dauerhafte Beschäftigung von mehr als neun Personen mit der Verarbeitung personenbezogener Daten (KMU) (nur Unternehmen >9 Mitarbeiter)



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=119.
Frage: *Verarbeiten dauerhaft mehr als 9 Personen in Ihrem Unternehmen personenbezogene Daten?*

Der Grad der IT-Abhängigkeit in den wirtschaftlichen Kernprozessen ihres Unternehmens wird zudem von knapp 70 Prozent der befragten KMU als hoch bis sehr hoch eingeschätzt.

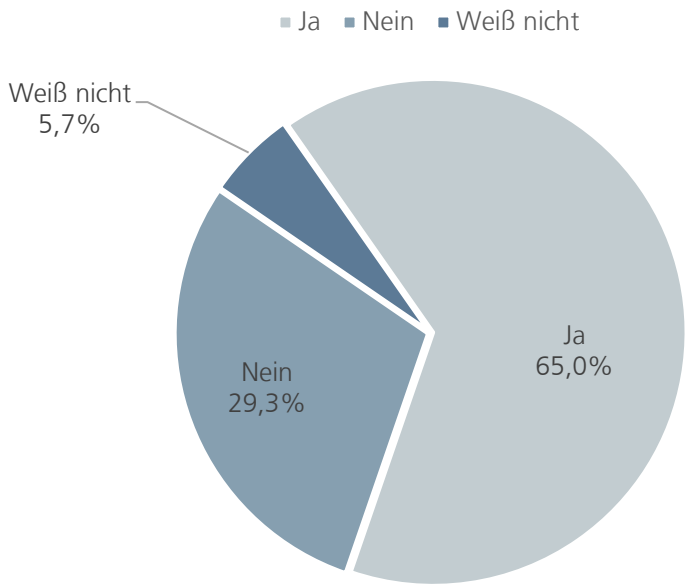
Abb. 7: Grad der IT-Abhängigkeit in den wirtschaftlichen Kernprozessen (KMU), 04/2017



Quelle: Goldmedia/if(is)-Befragung „Einsatz elektronischer Verschlüsselung in KMU" 2017; n=140. Frage: *Wie schätzen Sie den Grad der IT-Abhängigkeit in den wirtschaftlichen Kernprozessen Ihres Unternehmens ein?*

Auf die Frage, ob Geschäfts- und Betriebsgeheimnisse in größerem Umfang im Unternehmen vorhanden sind, antworteten die befragten KMU zu zwei Dritteln mit ja, knapp 30 Prozent der Unternehmen verneinten das Vorhandensein eines größeren Umfangs solcher Unternehmensgeheimnisse.

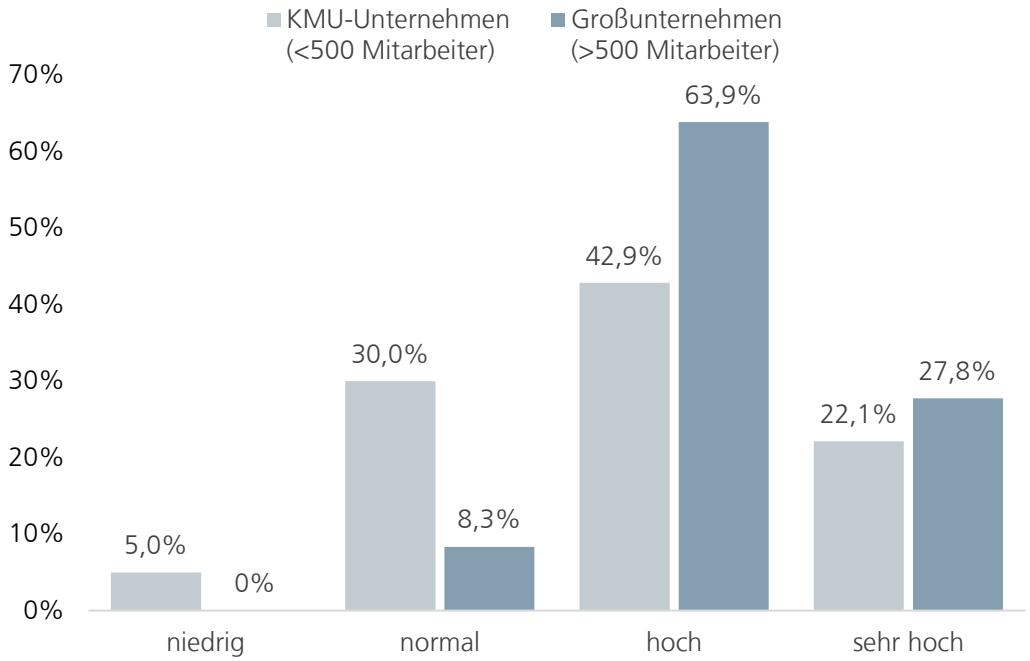
Abb. 8: Vorhandensein von wettbewerbsrelevanten Geschäfts- und Betriebsgeheimnisse in größerem Umfang (KMU)



Quelle: Goldmedia/if(is)-Befragung „Einsatz elektronischer Verschlüsselung in KMU" 2017; n=140.
Frage: *Müssen in Ihrem Unternehmen wettbewerbsrelevante Geschäfts- und Betriebsgeheimnisse in größerem Umfang (z.B. durch Forschung und Entwicklung) geschützt werden?*

Die Mehrheit der Großunternehmen attestiert sich davon unabhängig einen hohen Schutzbedarf (64 Prozent). Betrachtet man beide Kategorien mit überdurchschnittlichem Schutzbedarf gemeinsam, geben sogar 9 von 10 Großunternehmen die Auskunft, einen (sehr) hohen Schutzbedarf zu besitzen.

Abb. 9: Schutzbedarf von IT-Systemen und Daten des Unternehmens

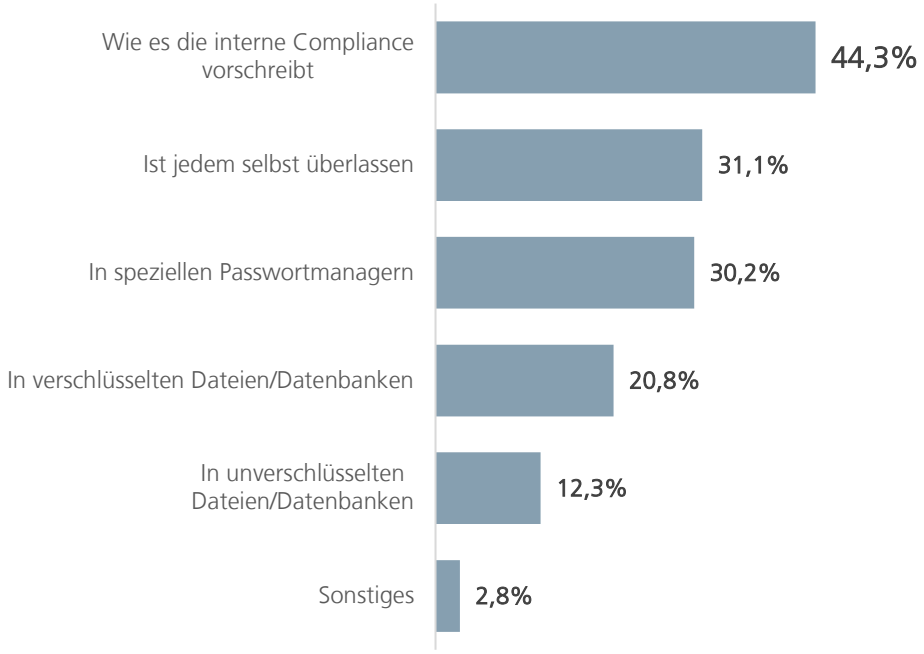


Quelle: Goldmedia/if(is)-Befragung „Einsatz elektronischer Verschlüsselung in KMU" 2017; n=212.
Frage: *Wie schätzen Sie den Schutzbedarf von IT-Systemen und Daten in Ihrem Unternehmen ein?*

Bei KMU ist der erkannte Schutzbedarf niedriger. Zwei Drittel der KMU geben an, einen überdurchschnittlichen Schutzbedarf zu besitzen. Einen durchschnittlichen Schutzbedarf haben 30 Prozent der KMU. 5 Prozent der KMU geben an, einen niedrigen Schutzbedarf zu besitzen. Die Antwortmöglichkeit „niedriger Schutzbedarf" wurde von keinem der befragten 72 Großunternehmen gewählt.

Bei der Verwaltung von Zugangsdaten und Passwörtern bestehen erhebliche Optimierungspotenziale in KMU, wie die folgende Auswertung zeigt. Um Verzerrungen bei den Angaben zur Speicherung von Zugangsdaten und Passwörtern zu vermeiden, wurden hierfür nur KMU berücksichtigt, die bereits grundsätzlich über die Möglichkeit der Datenverschlüsselung verfügen. Trotzdem zeigt sich, dass ein strukturiertes Passwortmanagement bislang größtenteils unterbleibt. Die Passwortverwaltung ist nur sehr unzureichend geregelt. Teilweise werden Passwörter sogar gänzlich unverschlüsselt abgelegt.

Abb. 10 Verwaltung von Zugangsdaten und Passwörtern bei KMU, die über Datenverschlüsselung verfügen



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=106; Mehrfachauswahl. Frage: Wie verwalten Ihre Mitarbeiter ihre Zugangsdaten und Passwörter?

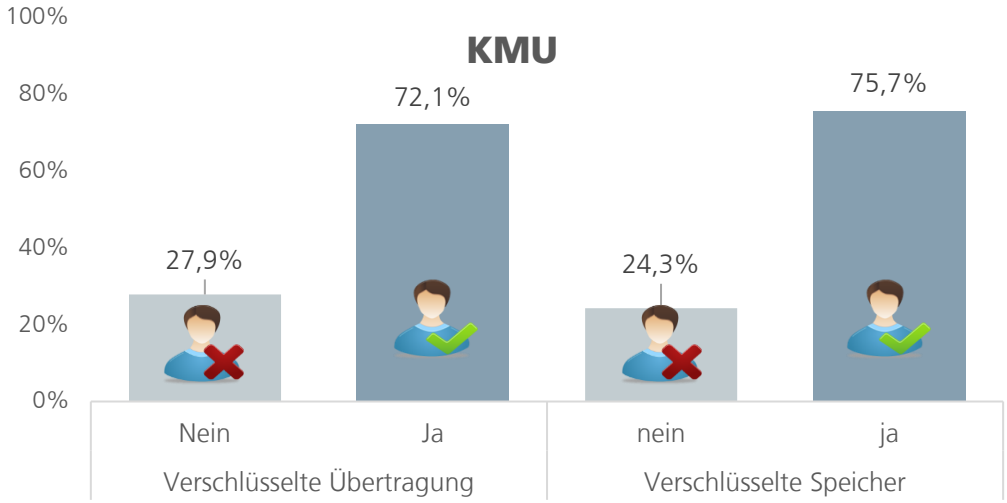
Weniger als die Hälfte der KMU (44 Prozent) geben an, ihre Zugangsdaten und Passwörter mithilfe ihrer internen Compliance zu verwalten. Bei jedem dritten Unternehmen (31 Prozent) ist es den Mitarbeitern selbst überlassen, wie sie Zugangsdaten und Passwörter verwalten. Nur ein Fünftel (21 Prozent) der KMU sichern ihre Zugangsdaten in verschlüsselten Datenbanken. 12 Prozent legen ihre Zugangsdaten sogar in unverschlüsselten Datenbanken ab.

Selbst bei KMU, die über Datenverschlüsselung verfügen (76 Prozent, vgl. Abb. 11), bestehen erhebliche Defizite bei der Verwaltung von Zugangsdaten und Passwörtern.

3.3 Nutzung von Verschlüsselungslösungen

Befragt man die Unternehmen nach dem Einsatz von Verschlüsselungslösungen für den Datentransport (Data in Motion) und die Sicherung von Festspeichern (Data at Rest), so zeigen sich ebenfalls **deutliche Unterschiede zwischen KMU und Großunternehmen**.

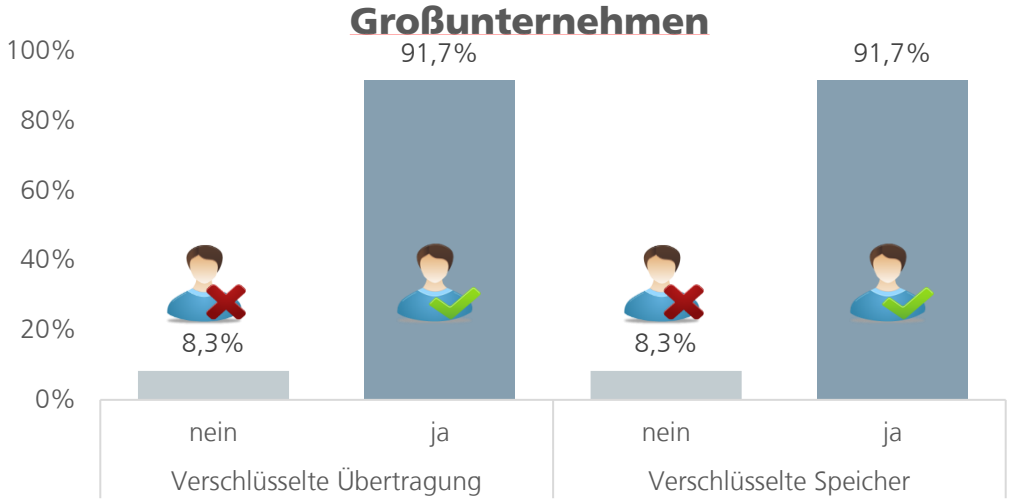
Abb. 11: Anteil der KMU, die Verschlüsselung einsetzen



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n =140.
Frage: *Setzen Sie Verschlüsselungstechnik in Ihrem Unternehmen ein?*

Während die Großunternehmen zu über 90 Prozent für beide Bereiche Verschlüsselungslösungen einsetzen, sind es bei den KMU nur drei Viertel der Unternehmen. Hierbei ist zu berücksichtigen, dass an dieser Stelle nicht der Umfang oder die durchgängige Implementierung, sondern nur der grundsätzliche (ggf. auf einzelne Clients beschränkte) Einsatz von Verschlüsselungslösungen abgefragt wurde. Demnach setzen ein Viertel aller KMU zu keinem Zeitpunkt bzw. in keinem Anwendungsfall Verschlüsselungslösungen ein.[2]

Abb. 12: Anteil der Großunternehmen mit Verschlüsselung

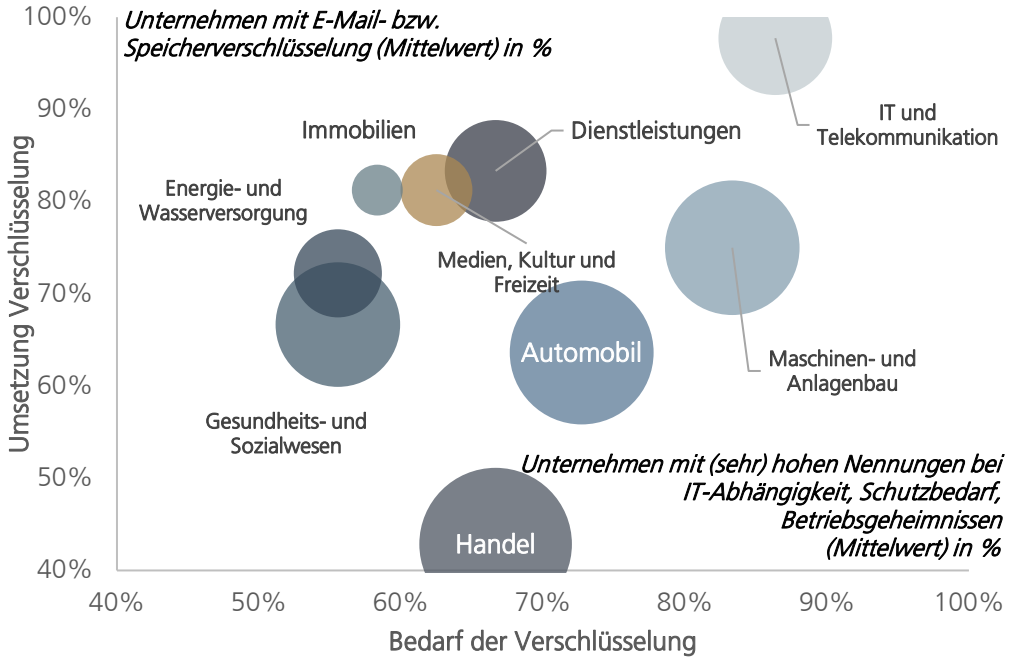


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=72.

2 Auszunehmen wären hiervon buchhalterische Datenverarbeitung (Online-Banking, Steueranmeldung, Kommunikation mit Krankenkassen) die verschlüsselt erfolgt, bei KMU jedoch vielfach von externen Dienstleistern übernommen wird.

Setzt man den derzeitigen Einsatz von Verschlüsselungslösungen in den KMU der einzelnen Branchen in Relation zur jeweiligen Selbsteinschätzung in den Reifegrad-Dimensionen IT-Abhängigkeit, Schutzbedarf sowie Betriebsgeheimnisse, zeigen sich deutliche Unterschiede zwischen den einzelnen Branchen.

Abb. 13 Mapping der Branchen nach Verschlüsselungsbedarf und Verschlüsselungsumsetzung (KMU), in Prozent



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=140

- Die **IT- und Telekommunikationsbranche** gibt einen sehr hohen IT-Reifegrad an und weist zugleich auch einen **sehr hohen Umsetzungsstand** bei der Verschlüsselung auf.
- KMU in der **Automobil- sowie Maschinen- und Anlagenbaubranche** weisen einen relativ hohen IT-Reifegrad und hohe IT-Abhängigkeit auf, haben aber einen **vergleichsweise niedrigen Umsetzungsstand** von Verschlüsselungstechnologien im Unternehmen.
- Der **Handel** hat im Verhältnis zum IT-Reifegrad mit unter 50 Prozent bei der Umsetzung von Verschlüsselungstechnologien **den geringsten Wert**.

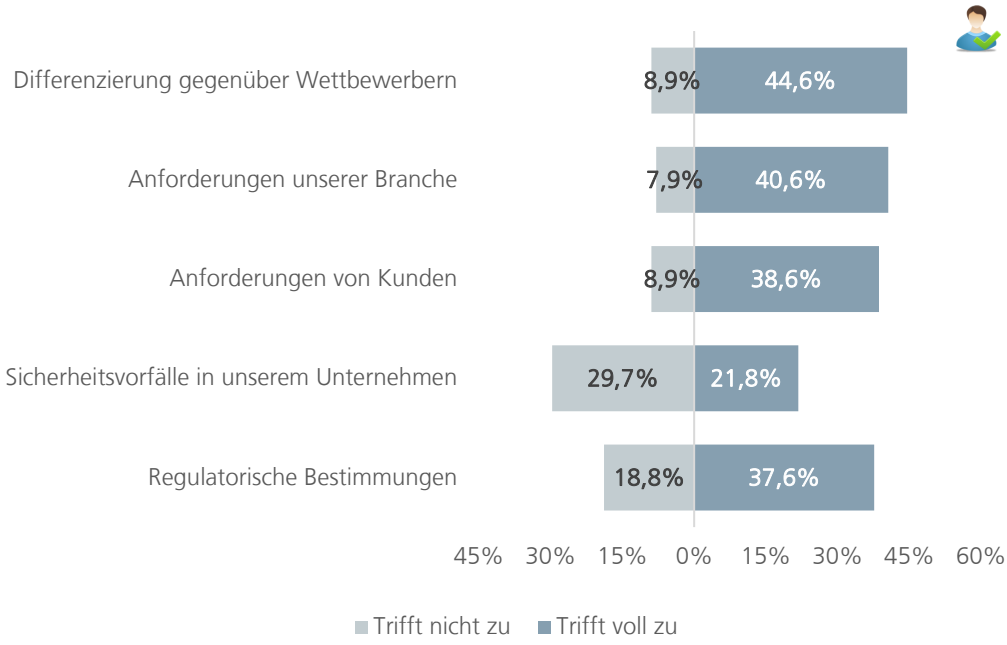
3.4 Einsatz von Kommunikationsverschlüsselung

In der Umfrage wurden im nächsten Schritt bei den Anwendern von Kommunikationsverschlüsselung die Motivationsgründe für eine Implementierung und die dabei entstandenen Herausforderungen an die Unternehmen erhoben. Im zweiten Schritt wurden konkrete Herausforderungen beim Einsatz der E-Mail-Verschlüsselung beleuchtet.

3.4.1 Motivationsgründe und Herausforderungen

Die Motivation von kleinen und mittleren Unternehmen für den Einsatz von Verschlüsselung ist derzeit vor allem durch das Wettbewerbsumfeld geprägt. 45 Prozent der KMU geben an, sich durch Kommunikationsverschlüsselung vor allem von anderen Wettbewerbern differenzieren zu wollen. Branchen- und Kundenanforderungen sind mit ca. 40 Prozent ebenfalls wichtige Faktoren für den Einsatz von Verschlüsselung. Tatsächlich eingetretene Sicherheitsvorfälle werden von 22 Prozent der KMU als Grund für den heutigen Einsatz von Verschlüsselungslösungen angegeben, ein deutlich geringerer Wert als bei den übrigen Motivationsgründen.

Abb. 14 Anwender von Kommunikationsverschlüsselung in KMU: Gründe für den Einsatz

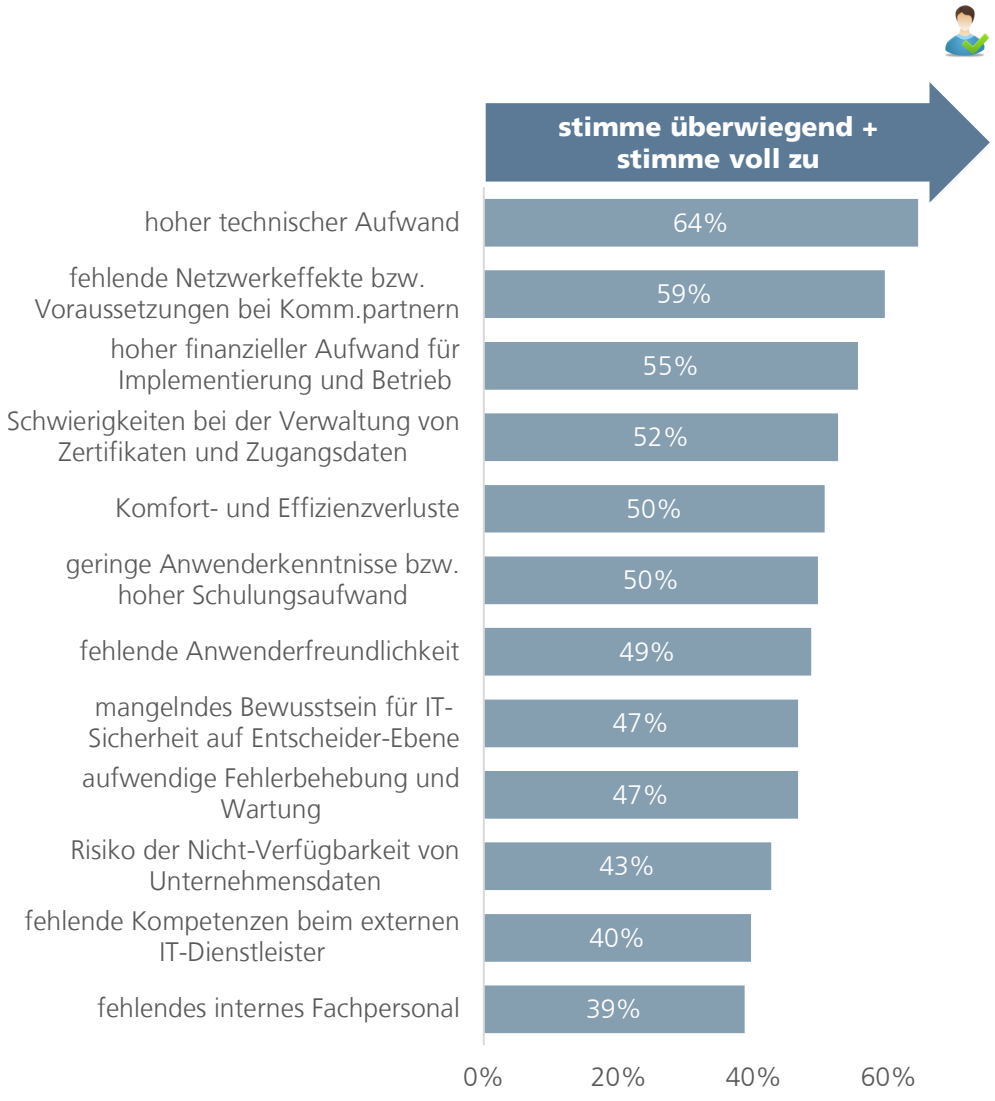


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=101. Frage: Was ist bzw. war in Ihrem Unternehmen der ausschlaggebende Grund, eine Verschlüsselungslösung zu implementieren?

Die gesteigerte Wettbewerbsfähigkeit sowie Anforderungen der Branche sind damit für KMU die wichtigsten Gründe, Verschlüsselungslösungen zu implementieren.

KMU, die Kommunikationsverschlüsselung einsetzen, sind anschließend dazu befragt worden, welche Hürden es bei der Einführung von verschlüsselter Kommunikation gegeben hat. Dabei stellte sich heraus, dass viele KMU (64 Prozent) den **hohen technischen Aufwand als Haupthürde** anführen. Auf Basis der Hintergrundgespräche mit IT-Sicherheits-Dienstleistern und Lösungsanbietern von Verschlüsselungslösungen sowie auf Basis der telefonisch durchgeführten Interviews mit KMU ist dieses Ergebnis so zu interpretieren, dass in vielen KMU **die technische Basis für eine durchgängige Implementierung von Kommunikationsverschlüsselung nicht gegeben ist**. Hierzu zählen z.B. ein zentrales IT- und Clientmanagement oder eine übergreifende Rechteverwaltung.

Abb. 15 Herausforderungen bei der Einführung von Kommunikationsverschlüsselung in KMU



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=101.
Frage: Was waren/sind die größten Herausforderungen bei der Einführung von verschlüsselter Kommunikation in Ihrem Unternehmen?

Ein weiterer größerer Aufwand entsteht bei der Konfigurierung und nachfolgenden Justierung des Verschlüsselungsregelwerkes für Gateways, sofern im Unternehmen bislang keine Vorgaben zum Einsatz der Verschlüsselung bestanden.

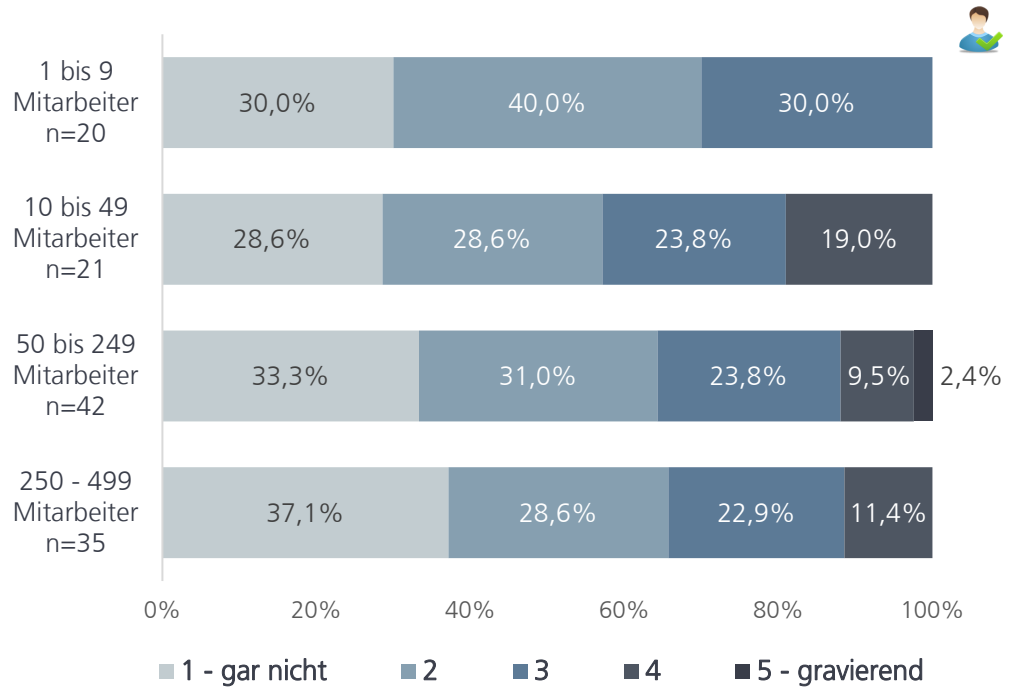
Fehlende Netzwerkeffekte durch fehlende technische Voraussetzungen (Zertifikate/Schlüssel) bei den E-Mail-Empfängern stellten nach Einschätzung von 59 Prozent der befragten KMU eine weitere Herausforderung beim standardisierten Einsatz von Verschlüsselungslösungen dar.

Dies ist der Hauptgrund, warum eine verschlüsselte Kommunikation und Übermittlung von Dokumenten (u.a. Rechnungen oder Kontoauszüge) gerade im B2C-Bereich über eine strukturierte Plattformkommunikation erfolgt, wo Dokumente über Login und Passwort geschützter Webportale abgerufen/ausgetauscht werden.

Etwa jedes zweite befragte Unternehmen gab zudem einen hohen finanziellen Aufwand für Implementierung und Betrieb an, was wiederum auch mit den Kosten zusammenhängt, die mit der Implementierung technischer Grundlagen verbunden sind.

Im weiteren Betrieb entstehen nach Einschätzung der Anwender von Kommunikationsverschlüsselung im KMU-Bereich danach hingegen kaum oder gar keine Komfort- oder Produktivitätseinbußen. Nur jedes fünfte Unternehmen mit 19 bis 49 Mitarbeitern hat nach der Einführung Komfortverluste in Kauf nehmen müssen.

Abb. 16 Komfort- Produktivitätsverluste beim Einsatz von Verschlüsselung bei KMU



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=118. Frage: Kam es aufgrund des Einsatzes von Verschlüsselung zu Komfort- und Produktivitätsverlusten?

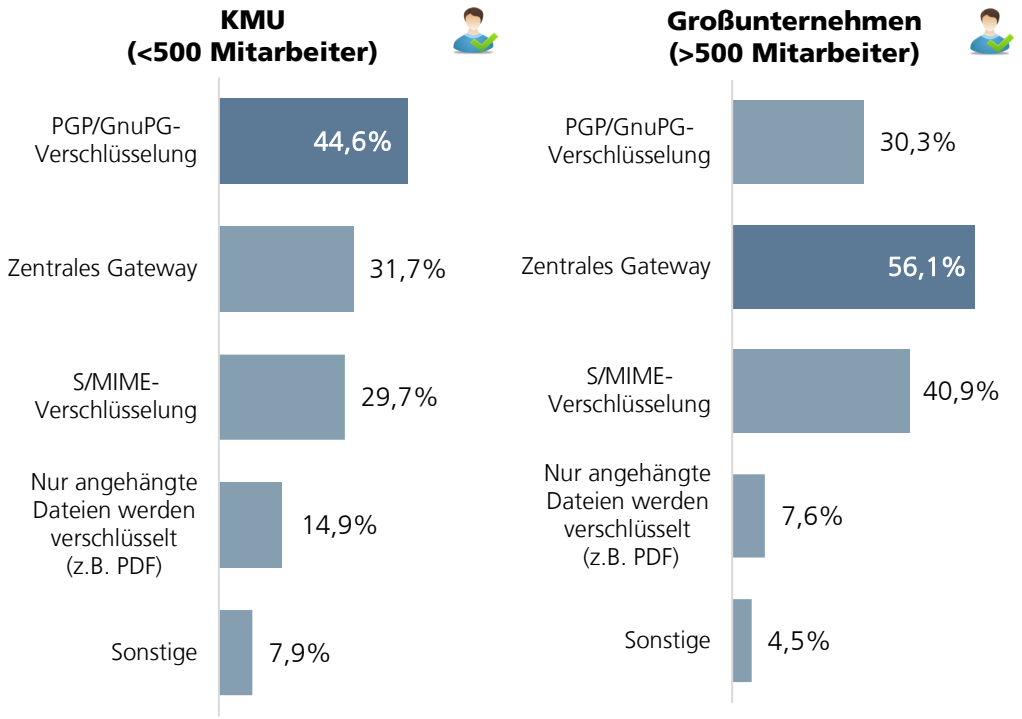
Die sehr positive Bewertung zum Thema Komfortverluste durch Kleinstunternehmen könnte damit zusammenhängen, dass in diesem Umfeld i.d.R. Consumer-Lösungen (Freeware-Client-Plug-Ins) installiert sind, die auch nur sporadisch genutzt werden, während insbesondere Unternehmen zwischen 10 und 49 Mitarbeitern darunter leiden, dass ihre Anforderungen für Ad-hoc-Lösungen zu komplex sind, sie jedoch nicht über die IT-Infrastruktur eines mittelgroßen Unternehmens verfügen.

3.4.2 Einsatz von E-Mail-Verschlüsselung

Während VPN-Verbindungen für den externen Zugriff auf das Unternehmensnetzwerk grundsätzlich verschlüsselt sind[3] und der Datentransport im LAN (mit Ausnahme des WLAN-Zugangs) i.d.R. unverschlüsselt erfolgt (abgesichert durch Zugangsberechtigungen, MAC-Filtern u.ä.), erfolgt der Einsatz von E-Mail-Verschlüsselung in KMU derzeit sehr heterogen.

Laut der Umfrageergebnisse nutzen 72 Prozent der KMU verschlüsselte Übertragungswege (vgl. Abb. 11), doch die Vielzahl an technischen Verschlüsselungslösungen im Einsatz erschweren hier die Entwicklung einheitlicher Verschlüsselungsstandards. **Bei KMU kommen hauptsächlich die kostenfreien PGP/GnuPG (45 Prozent) Technologien zum Einsatz.** Großunternehmen nutzen hingegen hauptsächlich zentrale Verschlüsselungs-Gateways (56 Prozent), vornehmlich mit S/MIME (41 Prozent) als Verschlüsselungslösung.

Abb. 17 Genutzte E-Mail-Verschlüsselungslösungen



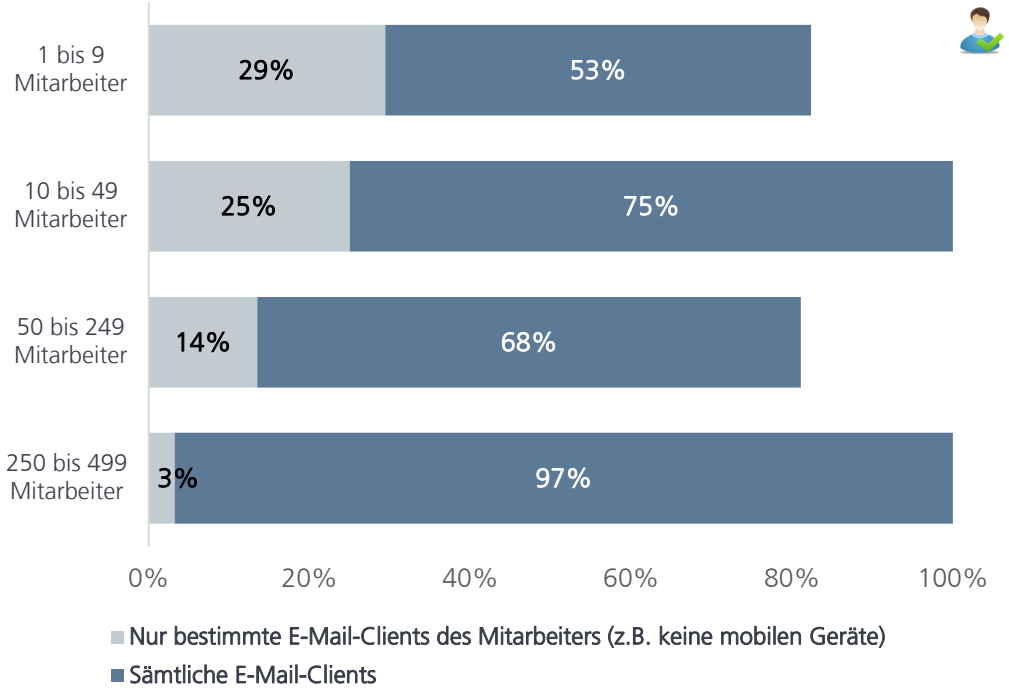
Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=101 KMU; n=66 Großunternehmen; Mehrfachantworten. Frage: Welche Verschlüsselungsart nutzen Sie beim E-Mail-Versand Ihrer Daten?

Tendenziell können kleinere Unternehmen mit Verschlüsselungslösungen häufiger nicht mit allen E-Mail-Clients auf verschlüsselte Nachrichten zugreifen. Mittlere Unternehmen mit 250 bis 499 Mitarbeitern haben unterdessen eine breitere Abdeckung von E-Mail-Clients mit der Möglichkeit, auf verschlüsselte Nachrichten zuzugreifen.

Je größer das Unternehmen ist, desto größer ist die Abdeckung von sämtlichen E-Mail-Clients zur Bearbeitung von verschlüsselten E-Mails (Abb. 18).

3 VPN-Lösungen unterscheiden sich v.a. beim Zugangsschutz, bspw. über eine 2-Faktor-Authentifizierung.

Abb. 18: Nutzung von E-Mail-Clients zur Bearbeitung von verschlüsselten E-Mails nach Mitarbeitergrößenklassen und Branchen

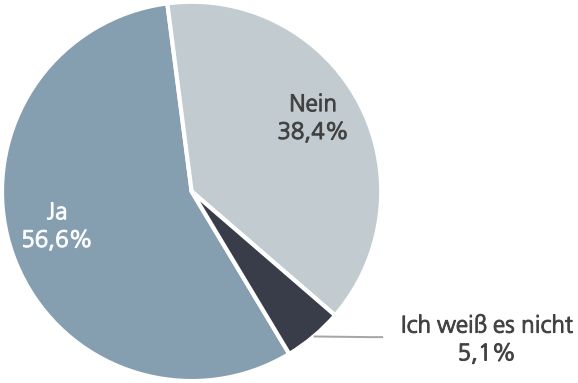


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=167.
Frage: Mit welchen E-Mail-Clients (Endgeräten) können Sie verschlüsselte E-Mails bearbeiten?

Dies ist vor allem dem Umstand zu verdanken, dass es im Vergleich mit lokal installierten Zertifikaten wesentlich einfacher ist, E-Mail-Verschlüsselung über ein zentrales E-Mail-Gateway auf heterogenen Endgeräten zur Verfügung zu stellen.

Die hohe Verbreitung von PGP/GNUPG bei KMU erschwert daher die Nutzung von Verschlüsselung auf mobilen Endgeräten, da es einen Mangel an praktikablen Lösungen gibt, die notwendigen Schlüssel auf allen Geräten zu verwalten. Insofern besitzen nur ca. 57 Prozent der befragten KMU die Möglichkeit, verschlüsselte E-Mails auf mobilen Endgeräten zu nutzen.

Abb. 19 Ergänzende mobile Nutzung von verschlüsselten E-Mails bei KMU, die E-Mail-Verschlüsselung einsetzen

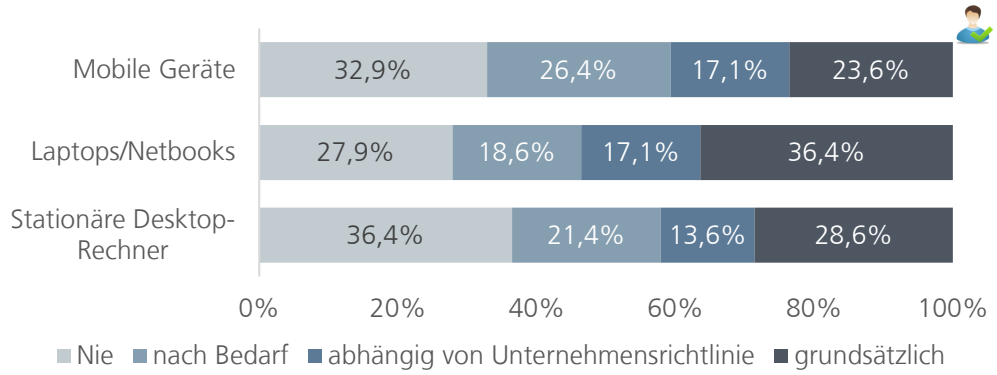


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=99.
Frage: Können Sie verschlüsselte E-Mails auch auf Ihrem Smartphone/Tablet nutzen?

3.5 Einsatz von Datenverschlüsselung

Die Antworten zur Nutzung von Datenträgerverschlüsselung bei verschiedenen Geräteklassen zeigen, dass auch hier künftig noch Optimierungsbedarf besteht. **Nur etwa ein Drittel (36 Prozent) der Unternehmenslaptops in KMU sind grundsätzlich verschlüsselt**. Bei stationären Desktop-Rechnern ist die Quote noch geringer (29 Prozent). Andere mobile Geräte liegen bei unter einem Viertel (24 Prozent). Insgesamt zeigt die Verteilung, dass Datenträgerverschlüsselung bei mobilen Endgeräten im Vergleich zum hierfür nötigen Aufwand zu selten eingesetzt wird.

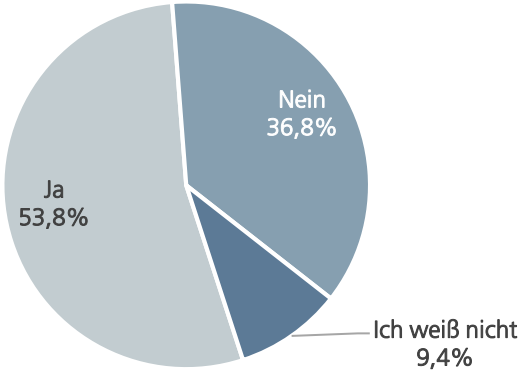
Abb. 20 Einsatz von Geräteverschlüsselung bei verschiedenen Gerätegruppen bei KMU



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=140.
Frage: Welche dieser Geräte sind durch Geräteverschlüsselung geschützt?

Es gibt zudem in nur 54 Prozent der KMU, die Datenverschlüsselung einsetzen, eine bekannte Unternehmensrichtlinie, welche die verschlüsselte Datenspeicherung regelt. Bei mind. 37 Prozent ist keine derartige Richtlinie vom Unternehmen definiert worden.

Abb. 21 Unternehmensrichtlinie zur Datenspeicherung bei KMU, die über Datenverschlüsselung verfügen



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=106. Frage: Existiert eine interne Unternehmensrichtlinie (Compliance), welche die verschlüsselte Datenspeicherung regelt?

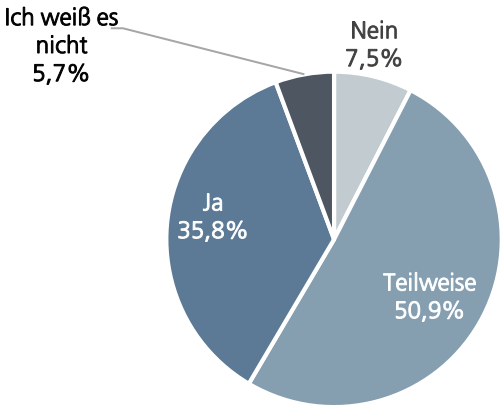
Dies ist insofern ein bemerkenswertes Ergebnis, da es verdeutlicht, dass nur etwa **die Hälfte der Unternehmen auch formalisiert festgeschrieben hat, wie der konkrete betriebliche Anwendungsfall für Verschlüsselung aussieht.** Die technische Verfügbarkeit allein gibt daher kaum darüber Auskunft, wie erfolgreiche Verschlüsselungslösungen im betrieblichen Alltag verankert sind.

3.6 Einsatz von Cloud-Computing

Auf die Frage, ob die gespeicherten Daten in der Cloud verschlüsselt werden, haben lediglich 36 Prozent aller befragten KMU mit „ja" geantwortet. Etwa die Hälfte gibt an, zumindest teilweise mit der Verschlüsselung von Daten in der Cloud zu arbeiten. Rund acht Prozent geben an, vollständig auf eine Cloud-Verschlüsselung zu verzichten. Damit besteht in Bezug auf eine durchgehende Nutzung von Verschlüsselung bei der Nutzung von Cloud-Speicherlösungen noch Verbesserungspotenzial.

Auf Basis der Hintergrundgespräche mit IT-Sicherheits-Dienstleistern und Lösungsanbietern von Verschlüsselungslösungen sowie auf Basis der telefonisch durchgeführten Interviews mit KMU ergab sich hier, dass viele KMU auf den Betrieb eigener verschlüsselter FTP-Server verzichten, jedoch zunehmend (kostenfreie) Cloud-Speicherlösungen für den temporären Austausch großer Datenmengen nutzen. Auf eine Dateiverschlüsselung wird dabei i.d.R. verzichtet. Ob eine Transportverschlüsselung zum Einsatz kommt, hängt jeweils vom Betreiber des Cloud-Dienstes ab.

Abb. 22 Vorhandene Verschlüsselung der Cloud-Dienste bei KMU

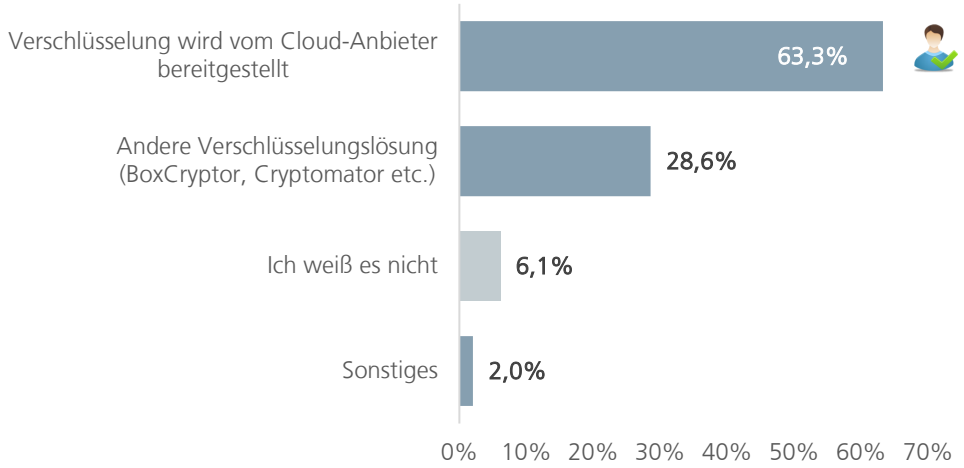


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=53.
Frage: Werden die in der Cloud gespeicherten Daten verschlüsselt?

Dies zeigt auch die konkrete Nachfrage nach der Form der Cloud-Verschlüsselung. Die vorwiegend eingesetzte Lösung für Cloud-Verschlüsselung ist die, die durch den Cloud-Anbieter bereitgestellt wird. Fast zwei Drittel (63 Prozent) der KMU nutzen diese.

Nur 29 Prozent der KMU greifen auf zusätzliche Cloud-Verschlüsselungs-Software zur Dateiverschlüsselung wie Boxcryptor oder Cryptomator zurück. Ein Großteil der KMU verlässt sich auf die Verschlüsselungsmethode der Cloud-Anbieter.

Abb. 23 Verschlüsselung der genutzten Cloud-Speicher bei KMU



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=49.
Frage: Mit welchem Verfahren werden die Daten in der Cloud verschlüsselt?

3.7 Nicht-Anwender von Verschlüsselung: Motive für die Nicht-Nutzung

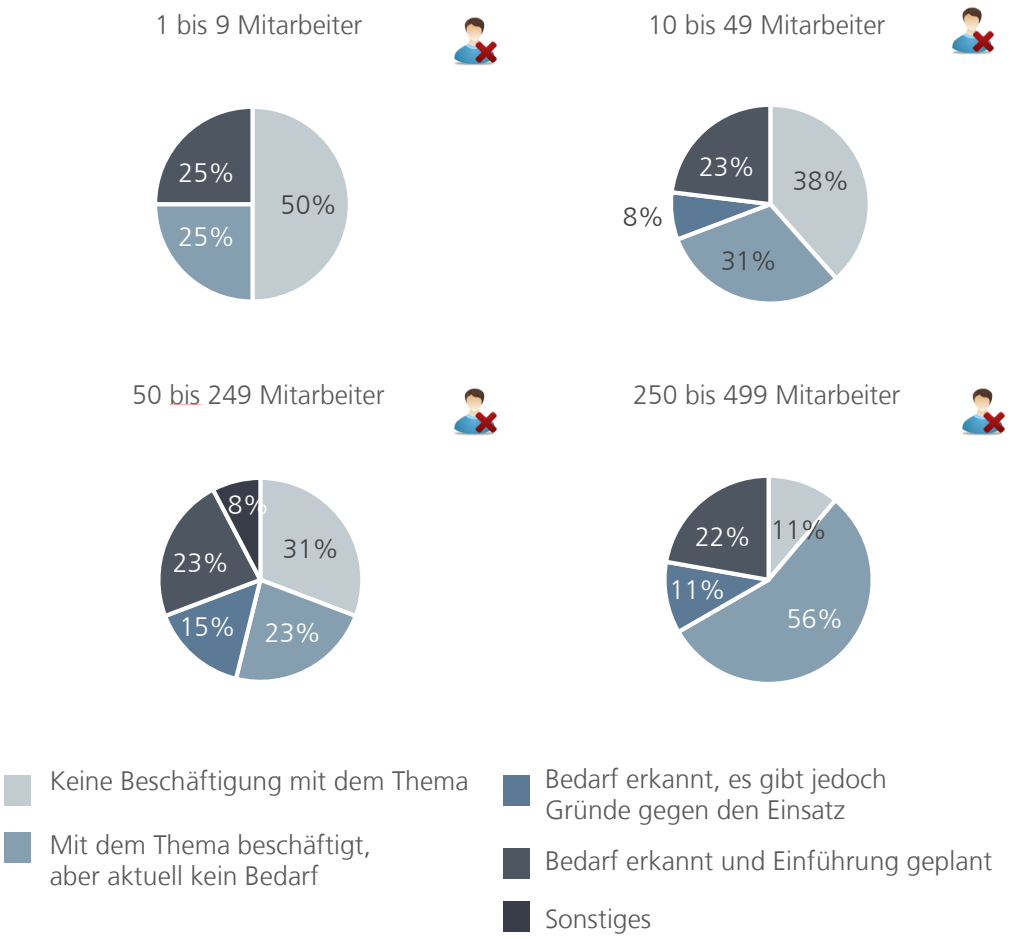
Um künftig eine größere Verbreitung von Verschlüsselung zu erreichen, muss analysiert werden, welche Gründe gegen den Einsatz von Verschlüsselungslösungen sprechen. Die KMU, die *keine Verschlüsselungslösungen* einsetzen, sind hierfür hinsichtlich ihrer Auseinandersetzung mit dem Thema Verschlüsselung spezifisch befragt worden (vgl. Abb. 24).

Über alle Größenklassen hinweg planen rund ein Viertel (22-25 Prozent) der heutigen Nicht-Anwender eine Einführung von Verschlüsselungslösungen.

Abgesehen hiervon zeigen sich jedoch einige Unterschiede in Abhängigkeit von der Unternehmensgröße. Je kleiner das Unternehmen, umso geringer wurde sich bislang mit Aspekten der Verschlüsselung aktiv auseinandergesetzt. Insbesondere in den Kleinstunternehmen (mit einem bis neun Mitarbeitern) wird das Thema kaum wahrgenommen: 50 Prozent der Unternehmen haben sich mit dem Thema Verschlüsselung bislang noch nicht beschäftigt. Bei den kleinen und mittleren Unternehmen (bis 249 Mitarbeiter) haben sich etwa ein Drittel der Unternehmen (31-38 Prozent) bislang mit Verschlüsselungstechnologien auseinandergesetzt.

„Entscheidende Gründe gegen den Einsatz" sind mit 15 Prozent am meisten in kleinen Unternehmen (50-250 Mitarbeiter) vorhanden. In Hintergrundgesprächen zu diesen entscheidenden Gründen, die gegen einen Einsatz sprechen, wurden am häufigsten fehlende Netzwerkeffekte (in Form von mangelnden Kommunikationspartnern) angeführt. Auch von zu hohen Kosten war in Einzelfällen die Rede. Kleine Unternehmen befinden sich hier strukturell in einer doppelten Zwickmühle: Einerseits können Sie – anders als Kleinstunternehmen mit kleinen Benutzergruppen – nicht mehr handhabbar mit selbstsignierten Zertifikaten umgehen. Andererseits profitieren sie im Gegensatz zu mittleren Unternehmen (und Großunternehmen) nicht in ausreichendem Maße von Skaleneffekten für einen effizienten Betrieb einer Verschlüsselungsinfrastruktur.

Abb. 24 KMU, die keine verschlüsselte Übertragung einsetzen: Auseinandersetzung mit Verschlüsselungslösungen



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=39.
Frage: Welche der folgenden Aussagen trifft am ehesten zu?

Bei Unternehmen von 250 bis 499 Mitarbeitern ist auffällig, dass sich 56 Prozent der Nicht-Anwender zwar einerseits bereits mit Verschlüsselungstechnologien beschäftigt haben und andererseits dennoch „aktuell keinen Bedarf" sehen. Eventuell wurde hier die Fragestellung als *weiterer* oder *zusätzlicher* Bedarf interpretiert, der bei Großunternehmen aufgrund ihres hohen IT-Reifegrades vergleichsweise gering ist.

Im Folgenden wurden die Unternehmen, welche keine Verschlüsselung verwenden, gebeten, die konkreten Hemmnisse zu benennen, die in ihrem Unternehmen vorhanden sind. Als größtes Hemmnis für Verschlüsselung werden die fehlenden Netzwerkeffekte bzw. fehlende technische Voraussetzungen bei den Kommunikationspartnern (69 Prozent) angegeben.

Geringe Anwenderkenntnisse im Haus und der damit verbundene Schulungsaufwand werden von 62 Prozent der Unternehmen als Hemmnis genannt. Immerhin 59 Prozent geben an, es gebe Defizite auf Entscheider-Ebene bzgl. eines starken Bewusstseins für IT-Sicherheit. Mehr als die Hälfte (54 Prozent) geben als Hemmnis Schwierigkeiten bei der Verwaltung von Zertifikaten und Zugangsdaten an.

Abb. 25 Hemmnisse für den Einsatz von Verschlüsselung bei KMU, die keine verschlüsselte Übertragung einsetzen

Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=39.
Frage: Inwiefern können Sie folgenden Hemmnissen für den Einsatz von Verschlüsselung zustimmen?

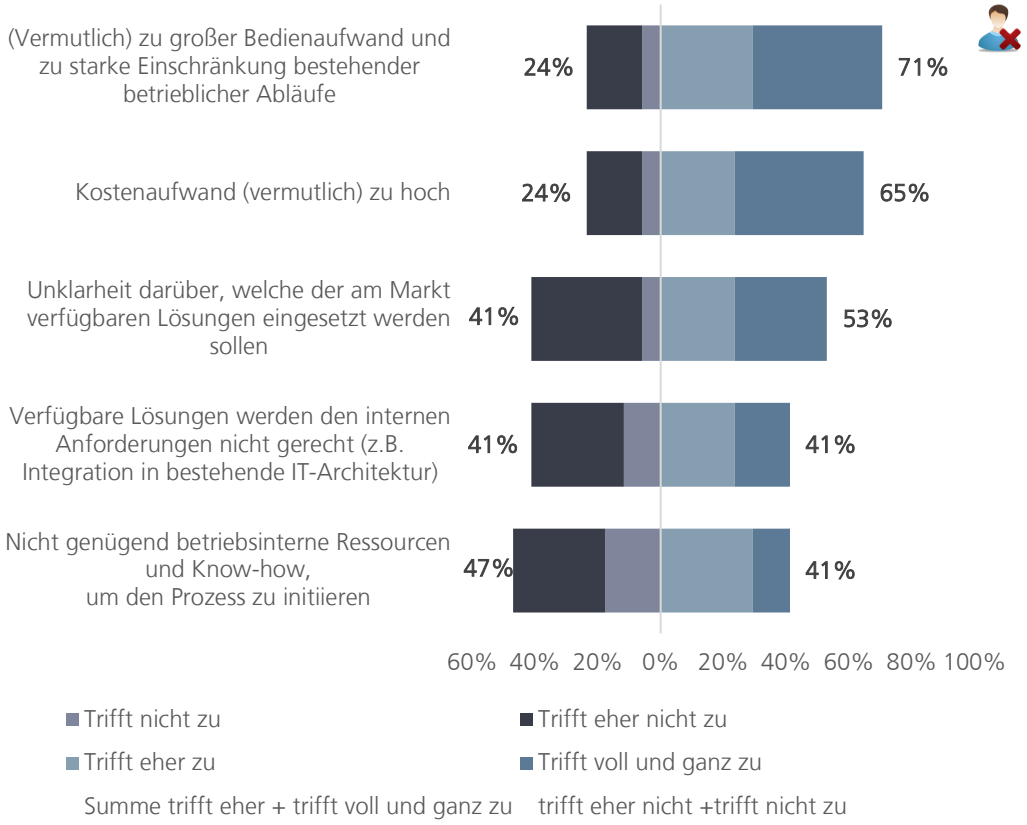
Insgesamt sehen die Unternehmen ein mangelndes Bewusstsein für IT-Sicherheit auf Anwender- und Entscheider-Ebenen und fehlende Kompetenz beim Umgang mit Verschlüsselungslösungen als die größten Hemmnisse für den Einsatz von Verschlüsselung an.

Für die folgende Analyse in Abb. 26 wurden nur KMU berücksichtigt, die sich mit der Verschlüsselungsthematik **bereits beschäftigt haben,[4] sich jedoch bewusst gegen einen Einsatz entschieden** haben. Es handelt sich in der folgenden Abbildung somit um die Angaben von **Nicht-Anwendern mit Kenntnissen zu bestehenden Marktlösungen.**

71 Prozent dieser Nicht-Anwender mit Kenntnissen zu bestehenden Marktlösungen führten vor allem einen zu großen Bedienungsaufwand und starke Einschränkungen bestehender betrieblicher Abläufe als Gründe an, welche gegen die Einführung von Verschlüsselung sprechen.

4 Z.B. indem sie bereits ein konkretes Angebot eingeholt haben.

Abb. 26 Gründe gegen den Einsatz von verschlüsselter Übertragung (Unternehmen, die sich mit der Thematik beschäftigt hatten)



Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=17.
Frage: Wie entscheidend sind darüber hinaus die folgenden Gründe gegen den Einsatz von Verschlüsselung?

Weiterhin gaben 65 Prozent der Nicht-Anwender mit Kenntnissen zu bestehenden Marktlösungen an, dass der Kostenaufwand für eine Einführung von Verschlüsselung (vermutlich) zu hoch ist.

Etwa die Hälfte der KMU, die sich bereits mit Verschlüsselungslösungen beschäftigt haben, benannte auch die fehlende Markttransparenz auf dem Markt für Verschlüsselungslösungen als hemmenden Faktor, sich bislang für keine Lösung entschieden zu haben.

4 Rechtliche Analyse

4.1 Einleitung

Eine Verschlüsselung von Daten wird regelmäßig im wirtschaftlichen Eigeninteresse von Unternehmen liegen. Jenseits eines solchen Eigeninteresses gibt es aber auch eine rechtliche Dimension. Diese wird im Folgenden analysiert.

4.1.1 Allgemeines

Rechtliche Vorgaben zur Verschlüsselung lassen sich grob in fünf Gruppen unterteilen:

1. ausdrückliche Verschlüsselungspflichten,
2. Verschlüsselungsobliegenheiten,
3. Generalklauseln,
4. behördliche Vorgaben,
5. Ausbildung.

In die erste Gruppe fallen alle gesetzlichen Vorgaben, die ausdrücklich eine Verschlüsselung von Daten fordern. Die zweite Gruppe erfasst gesetzlich Vorschriften, die zwar ausdrücklich Bezug auf Verschlüsselung nehmen, diese aber nicht zwingend vorschreiben. Die dritte Gruppe umfasst allgemeine rechtliche Verhaltensvorgaben, die durch eine Verschlüsselung von Daten befolgt werden können, ohne dass ausdrücklich eine Verschlüsselung verlangt wird – in diesem Kontext werden insbesondere Haftungsregeln betrachtet. Die vierte Fallgruppe umfasst behördliche Vorgaben mit Bezug auf Verschlüsselung. Schließlich regelt der Staat in verschiedenen Bereichen die Ausbildungsinhalte – diese können auch die Vermittlung von Kenntnissen über Verschlüsselung enthalten.

Im Fokus der rechtlichen Betrachtungen stehen *staatliche* Regelungen in Bezug auf Verschlüsselung. Nicht betrachtet wurden insoweit privatrechtliche Verschlüsselungspflichten, die auf Vereinbarungen zwischen Privaten beruhen. So existieren in einigen Branchen Standards, die u.a. eine Verschlüsselung von Daten vorsehen – beispielhaft sei hier der Payment Card Industry Data Security Standard (PCI-DSS) für die Speicherung und Verarbeitung von Kreditkartendaten genannt. In einem Exkurs wird allerdings am Ende der rechtlichen Betrachtungen kurz auf sogenannte „Cyberrisiko- oder Cyber-Versicherungen“ eingegangen.[5]

Betrachtet wurde nur das deutsche Recht und – soweit relevant – der unionsrechtliche Rahmen.[6] Die Untersuchung wurde zudem auf die Rechtsgebiete beschränkt, die regelmäßig für kleine und mittlere Unternehmen relevant sind.[7]

5 Unten, S. 90 ff. (unter 4.9).

6 Nicht betrachtet wurden demnach US-amerikanische Gesetze, wie etwa der Sarbanes-Oxley Act, auch wenn dieser für deutsche Unternehmen relevant sein mag, die etwa an einer US-amerikanischen Wertpapierbörse notiert sind. Ebenfalls nicht betrachtet wurden die Federal Rules of Civil Procedure.

7 Nicht untersucht wurde deshalb etwa das Finanzmarktrecht.

4.1.2 De-Mail-Gesetz

Nicht im Fokus der Studie stand das De-Mail-Gesetz. Hierüber hat der Bund die Grundlagen für eine elektronische Kommunikationsplattform geschaffen, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen soll.[8] Durch gesetzliche Vorgaben wird sichergestellt, dass sowohl die Kommunikation zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt[9] als auch zwischen den Dienstleistern[10]. Das De-Mail-Gesetz schreibt allerdings keine Ende-zu-Ende-Verschlüsselung vor.[11]

Eine rechtliche Verpflichtung zur Nutzung von De-Mail besteht nicht. Der Gesetzgeber hat in verschiedenen anderen Gesetzen Regelungen in Bezug auf den De-Mail-Dienst getroffen. Diese betreffen aber in erster Linie Fragen des Zugangs[12] bzw. des Beweiswerts entsprechender Nachrichten[13]. Soweit Fragen in Bezug auf eine Verschlüsselung adressiert werden, handelt es sich um Ausnahmen, wonach Daten, die ansonsten verschlüsselt übertragen werden müssen, bei der Nutzung von De-Mail auch ohne (zusätzliche) Ende-zu-Ende-Verschlüsselung übertragen werden dürfen.[14] Diese eher punktuellen Regelungen dürften jedoch nicht dahingehend verallgemeinerungsfähig sein, dass bei Nutzung eines (nicht Ende-zu-Ende-verschlüsselten) De-Mail-Dienstes grundsätzlich davon ausgegangen werden kann, dass geheimschutzrechtlichen Vorgaben genügt wurde.[15]

Es ist aber in Rechnung zu stellen, dass die De-Mail-Anbieter inzwischen Zusatzprogramme zur Verfügung stellen, über die Daten (unter Nutzung des PGP-Standards) Ende-zu-Ende-verschlüsselt übertragen werden können. Eine solche Übermittelung wird in aller Regel sowohl gesetzlichen Verschlüsselungsverpflichtungen genügen als auch sonstigen Schutzpflichten entsprechen (jedenfalls soweit es um die typischen Belange kleiner und mittlerer Unternehmen geht).[16] Allerdings unterscheidet sich eine derartige Datenübermittlung in Bezug auf die hier relevanten Fragestellungen nicht von jeder anderen verschlüsselten Datenübermittlung unter Nutzung eines entsprechenden Standards, weshalb keine gesonderte Betrachtung des De-Mail-Dienstes unter rechtlichen Gesichtspunkten erforderlich war.

4.1.3 Bestandsrecherche

Um die für das Gutachten relevanten gesetzlichen Vorschriften zu identifizieren, wurde zunächst in der Fachdatenbank juris recherchiert. Die Datenbank lieferte

8 § 1 De-Mail-Gesetz.

9 § 4 Abs. 3 De-Mail-Gesetz.

10 § 5 Abs. 3 De-Mail-Gesetz.

11 Vgl. § 5 Abs. 3 S. 2 De-Mail-Gesetz „Der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) bleibt hiervon unberührt."

12 Etwa § 5a VwZG, § 174 ZPO.

13 Etwa § 3a VwZG, § 371a ZPO.

14 Etwa § 30 Abs. 7 u. § 87a Abs. 1 Abgabenordnung; auch § 67 Abs. 6 Nr. 3 SGB X.

15 LDI Berlin, Jahresbericht 2014, S. 190 geht davon aus, dass De-Mail „ungeeignet für die Übermittlung von Gesundheits- und anderen vergleichbar sensitiven Daten" ist, vgl. ders., Jahresbericht 2012, S. 15. Auch BfDI, Tätigkeitsbericht 2009/2010, S. 38 geht davon aus, dass trotz Nutzung von De-Mail für „sensible Daten" eine Ende-zu-Ende-Verschlüsselung erforderlich ist.

16 Insoweit wird allerdings unterstellt, dass eine Verschlüsselung nach dem PGP-Standard dem Stand der Technik entspricht, vgl. hierzu unten, S. 31 ff. (unter 4.3).

173 Treffer im Bundesrecht mit Bezug auf Verschlüsselung[17] und zehn Treffer für Kryptographie[18]. Diese Trefferliste umfasst aber nicht nur die kryptographische Verschlüsselung von Daten, sondern auch die Verschlüsselung von Informationen durch vorgegebene Zeichenfolgen.[19] Ein großer Teil der relevanten Vorschriften betrifft zudem nicht die Privatwirtschaft, sondern adressiert Verpflichtungen der Verwaltung. Überwiegend handelt es sich dabei um Vorschriften, nach denen die Datenübermittlung zwischen Behörden verschlüsselt werden muss, wenn öffentliche Telekommunikationsnetze hierzu genutzt werden.[20]

Für das Landesrecht (aller Bundesländer) werden in juris insgesamt 295 Treffer erzielt.[21] Exemplarisch wurden die Bundesländer Berlin und Nordrhein-Westfalen näher untersucht. Die Datenbank mit dem Landesrecht Berlin[22] liefert 25 Treffer,[23] die jeweils Pflichten der öffentlichen Verwaltung (sowie von Krankenhäusern) adressieren und deshalb im Folgenden nicht weiter untersucht werden. Für Nordrhein-Westfalen weist juris 23 Treffer aus, die ebenfalls keinen Bezug zur Privatwirtschaft haben.

Im Unionsrecht werden in der Datenbank EUR-Lex 303 Treffer mit Bezug auf Verschlüsselung erzielt.[24] Für die Studie wurden nur die 113 Verordnungen weiter untersucht, weil nur diese in allen Mitgliedstaaten verbindlich sind und keiner nationalen Umsetzung bedürfen.[25] Weit überwiegend adressieren diese Verordnungen Pflichten staatlicher Stellen[26], betreffen die Verschlüsselung von Informationen durch vorgegebene Zeichenfolgen[27] oder betreffen Exportbeschränkungen[28].

17 Stand 2.8.2016 für den Suchbegriff „verschlüssel*" und mit den Einschränkungen auf „Gesetze/Verordnungen", „heute" und „Bund".

18 Stand 3.8.2016 für den Suchbegriff „kryptogr*" und mit den Einschränkungen auf „Gesetze/Verordnungen", „heute" und „Bund". Ein großer Teil dieser Vorschriften nimmt Bezug auf digitale Signaturen.

19 Etwa § 301 Abs. 2 S. 1 SGB V: „Die Diagnosen nach Absatz 1 Satz 1 Nr. 3 und 7 sind nach der Internationalen Klassifikation der Krankheiten in der jeweiligen vom Deutschen Institut für medizinische Dokumentation und Information im Auftrag des Bundesministeriums für Gesundheit herausgegebenen deutschen Fassung zu verschlüsseln." Vgl. weiter Anlage 9 zu § 25 Abs. 3 Fahrerlaubnis-Verordnung.

20 Etwa § 4 Abs. 2 S. 1 Verordnung über das Vermögensverzeichnis: „Werden zur Übermittlung der Daten öffentliche Telekommunikationsnetze genutzt, ist ein geeignetes Verschlüsselungsverfahren zu verwenden."

21 Stand 3.8.2016 für den Suchbegriff „verschlüssel*" und mit den Einschränkungen auf „Gesetze/Verordnungen", „heute" und „alle Bundesländer".

22 <http://gesetze.berlin.de/>.

23 Stand 3.8.2016 für den Suchbegriff „verschlüssel*", Suchsprache: Deutsch, Teilbereich: Rechtsvorschriften.

24 Stand 3.8.2016 für den Suchbegriff „verschlüssel*", Suchsprache: Deutsch, Teilbereich: Rechtsvorschriften.

25 Vgl. Art. 288 AEUV. Richtlinien wurden nicht betrachtet, weil diese einer Umsetzung in das nationale Recht bedürfen, so dass insoweit auf das nationale Recht abzustellen ist; Beschlüsse sind ebenso wie Verordnungen verbindlich, sie sind jedoch in der Praxis an bestimmte Adressaten gerichtet, so dass sie keine allgemeine Geltung beanspruchen.

26 Etwa Art. 34 Abs. 2 lit. j) Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

27 Etwa Art. 28 Verordnung (EU) Nr. 1272/2009 der Kommission vom 11. Dezember 2009 mit gemeinsamen Durchführungsbestimmungen zur Verordnung (EG) Nr. 1234/2007 des Rates hinsichtlich des An- und Verkaufs von landwirtschaftlichen Erzeugnissen im Rahmen der öffentlichen Intervention.

28 Z.B. Verordnung (EU) Nr. 961/2010 des Rates vom 25. Oktober 2010 über restriktive Maßnahmen gegen Iran und zur Aufhebung der Verordnung (EG) Nr. 423/2007.

Eine erste Grobsichtung der Rechercheergebnisse hat gezeigt, dass die ganz überwiegende Zahl der ermittelten gesetzlichen Regelungen dem allgemeinen und sektorspezifischen Datenschutzrecht sowie dem Abgabenrecht entstammt.

4.2 Exkurs: Verfassungsrechtliche Vorüberlegungen

4.2.1 Allgemeinwohlbezug

Verpflichtende staatliche Vorgaben zum Einsatz von Verschlüsselungsverfahren im Bereich der Privatwirtschaft sind zunächst am Maßstab der Berufsfreiheit aus Art. 12 Abs. 1 GG zu messen.

Werden Private verpflichtet, im beruflichen Umfeld Daten zu verschlüsseln, so stellt dies grundsätzlich einen Eingriff in die Freiheit der Berufsausübung dar. Solche Eingriffe sind nach ständiger Rechtsprechung des BVerfG nur zulässig, „soweit vernünftige Erwägungen des Gemeinwohls es zweckmäßig erscheinen lassen".[29] Jede gesetzliche Verpflichtung, Daten zu verschlüsseln, muss also einen Bezug zum Allgemeinwohl haben.

Ein solcher Allgemeinwohlbezug ist unschwer im Bereich des Datenschutzrechts gegeben, zielen doch diese Regelungen auf den Schutz des Rechts auf informationelle Selbstbestimmung ab. Stark vereinfacht schafft der Gesetzgeber in diesem Bereich einen Ausgleich zwischen dem Interesse an einer möglichst freien Gestaltung der Berufsausübung (bei der die Verschlüsselung von Daten hinderlich sein mag) und dem Interesse der Allgemeinheit am Schutz personenbezogener Daten (die eine Verschlüsselung besonders sensibler personenbezogener Daten erforderlich machen kann).

Dementsprechend ist der nach der Bestandsanalyse gegebene Befund, wonach der überwiegende Teil staatlicher Vorgaben in Bezug auf die Verschlüsselung dem Datenschutzrecht im weiteren Sinne entstammt, auch nicht weiter verwunderlich.

Ebenfalls unschwer begründbar ist ein Allgemeinwohlbezug, wenn es um den Schutz kritischer Infrastrukturen geht.[30] Schließlich kann ein Ausfall solcher Infrastrukturen – definitionsgemäß[31] – weitreichende gesellschaftliche Folgen haben.

4.2.2 Paternalistische Verschlüsselungspflichten

Ohne diese – deutlich außerhalb des Fokus der hiesigen Studie liegende – Frage vertieft zu analysieren, folgt aus dem verfassungsrechtlichen Gebot eines Allge-

29 So der Leitsatz 6. a) des grundlegenden Apothekenurteils (BVerfGE 7, 377 = Urt. v. 11.6.1958 – Az. 1 BvR 596/56).

30 Die Begründung zum Gesetzentwurf des IT-Sicherheitsgesetzes spricht ausdrücklich die „besondere Verantwortung [der Betreiber kritischer Infrastrukturen] für das Gemeinwohl" an, BT-Drs. 18/4096, 2.

31 Nach BMI, KRITIS-Strategie, S. 3 sind „[k]ritische Infrastrukturen ... Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." Vgl. auch § 2 Abs. 10 Nr. 2 BSIG: „Kritische Infrastrukturen ... sind Einrichtungen, Anlagen oder Teile davon, die ... von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

meinwohlbezugs, dass staatliche Verpflichtungen zur Verschlüsselung allein im *Eigeninteresse* der betroffenen Unternehmen unzulässig wären. So mag es etwa sinnvoll sein, Betriebs- und Geschäftsgeheimnisse nur verschlüsselt zu speichern oder zu übermitteln. Eine öffentlich-rechtliche Verpflichtung hierzu wäre aber verfassungsrechtlich grundsätzlich problematisch.[32]

Das Verbot solcher paternalistischen Verschlüsselungsverpflichtungen bedeutet jedoch nicht, dass der Staat keine Möglichkeiten hätte, auf einen verstärkten Einsatz von Verschlüsselung hinzuwirken. Solange hierdurch nicht in die Berufsausübung oder -wahl eingegriffen wird, bestehen jedenfalls mit Blick auf Art. 12 GG keine Hindernisse. Das betrifft insbesondere den Bereich der Informationspolitik oder die Förderung des Einsatzes von Verschlüsselungstechnologien.[33] Ebenfalls unproblematisch ist es, wenn im Rahmen der Berufsausbildung der Einsatz von Verschlüsselungstechniken gelehrt wird.[34]

4.2.3 Privatrechtliche Verschlüsselungspflichten

Von staatlichen Verschlüsselungspflichten deutlich zu unterscheiden sind privatrechtliche Pflichten und ihre staatliche Durchsetzung.

So mag sich die Geschäftsführung einer GmbH oder der Vorstand einer AG (grob) sorgfaltswidrig verhalten, wenn eine Datenbank mit Betriebs- und Geschäftsgeheimnissen ungesichert über das Internet zugänglich gemacht wird. Entsteht der Gesellschaft hierdurch ein Schaden, können Geschäftsführer oder Vorstand hierfür haften.[35] Ein entsprechender Schadenersatzanspruch könnte vor den staatlichen Zivilgerichten (und im Wege der staatlichen Zwangsvollstreckung) durchgesetzt werden.

In dieser Konstellation würde beispielsweise der Geschäftsführer jedoch nicht etwa gegen eine staatliche Verschlüsselungspflicht verstoßen, sondern er würde es schlicht an der Sorgfalt eines „ordentlichen Geschäftsmannes“[36] mangeln lassen. Die Haftung würde also nicht aus dem Verstoß gegen eine öffentlich-rechtliche Verpflichtung folgen, sondern aus der Verletzung einer Verpflichtung gegenüber der Gesellschaft (bzw. den Vermögensinteressen der Gesellschafter). Der Unterschied wird deutlicher, wenn statt eines GmbH-Geschäftsführers ein Einzelkaufmann sich entsprechend verhalten würde. Würde ein solcher seine Betriebs- und Geschäftsgeheimnisse nicht schützen, wäre dies allein sein Problem. Ein entsprechender Sorgfaltspflichtverstoß wäre (grundsätzlich) nicht rechtlich sanktionierbar.

Ob und wie weit es zu der Sorgfalt eines „gewissenhaften Geschäftsleiters“ oder „ordentlichen Geschäftsmannes“ zählt, für eine Verschlüsselung von Daten zu sorgen, wird unter 4.6.1 (S. 68 ff.) näher untersucht.

32 Das gilt jedenfalls, solange Aspekte wie Spionage im Bereich gemeinwohlrelevanter Technologien keine Rolle spielen.

33 Wobei hier freilich ggf. Gleichheitsaspekte (Art. 3 GG) zu berücksichtigen wären, wenn etwa bestimmte Produkte gefördert werden sollen.

34 Vgl. hierzu ausführlicher unten, S. 88 (unter 4.8).

35 Vgl. ausführlicher unten, S. 68 ff. (unter 4.6.1).

36 Vgl. § 43 Abs. 1 GmbHG.

4.3 Exkurs: Stand der Technik

Zahlreiche Normen, die auf eine Verschlüsselung Bezug nehmen, stellen darauf ab, dass diese dem „Stand der Technik entsprechen" muss. Es ist deshalb vorab zu klären, was hierunter im rechtlichen Kontext zu verstehen ist.[37]

Bei Begriffen wie „Stand der Technik" oder auch „Stand der Wissenschaft" handelt es sich um unbestimmte Rechtsbegriffe.[38] Solcher unbestimmten Rechtsbegriffe bedient sich der Gesetzgeber unter anderem in Gebieten, die einer raschen technischen Entwicklung unterworfen sind. Wollte der Gesetzgeber durch klar bestimmte Regelungen Schritt mit der Entwicklung halten, müsste er die gesetzlichen Vorschriften permanent anpassen.[39] Bezogen auf eine Datenverschlüsselung müsste der Gesetzgeber etwa ständig die verfügbaren Verschlüsselungsalgorithmen beurteilen und entscheiden, welche Schlüssellängen für welche Zwecke zulässig (bzw. ausreichend) wären. Um eine solche laufende Gesetzesanpassung zu vermeiden, darf der Gesetzgeber durch die Verwendung unbestimmter Rechtsbegriffe die verbindliche Konkretisierung – und damit die Anpassung an die wissenschaftliche und technische Entwicklung – „mehr oder weniger" auf die Verwaltung bzw. die Rechtsprechung verlagern.[40]

Soweit ein technischer Fortschritt adressiert werden soll, kann (u. a.) unterschieden werden zwischen den „allgemein anerkannten Regeln der Technik", dem „Stand der Technik" und dem „Stand der Wissenschaft".

Dabei versteht die Rechtsprechung unter

„allgemein anerkannten Regeln der Technik" die „herrschende Auffassung unter den technischen Praktikern". Der Begriff stellt demnach auf einen Status quo ab und ist durch tatsächliche Elemente geprägt. Insbesondere hinkt ein solcher Maßstab stets hinter einer weiterstrebenden technischen Entwicklung hinterher.[41]

„Stand der Technik" die „Front der technischen Entwicklung" (so die Formulierung des BVerfG). Es kommt also nicht darauf an, ob eine Technik allgemein anerkannt ist oder sich bereits in der Praxis bewährt hat.[42] Vielmehr kommt es darauf an, was nach dem (ggf. nicht einheitlichen) Meinungsstand der Techniker technisch notwendig, geeignet, angemessen und vermeidbar ist.[43]

„Stand der Wissenschaft" die Berücksichtigung der neuesten wissenschaftlichen Erkenntnisse. Soweit es um die Abwehr von Gefahren geht, ist insbesondere nicht

37 Etwa Anlage zu § 9 S. 2 BDSG, Anlage zu § 78 S. 2 SGB X, § 32 Datenschutz-Grundverordnung, § 13 TMG.

38 Allerdings finden sich auch Legaldefinitionen, die die Begriffe jedenfalls weiter präzisieren. Vgl. etwa § 3 Abs. 6 BImSchG: „Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung von Emissionen in Luft, Wasser und Boden, zur Gewährleistung der Anlagensicherheit, zur Gewährleistung einer umweltverträglichen Abfallentsorgung oder sonst zur Vermeidung oder Verminderung von Auswirkungen auf die Umwelt zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere die in der Anlage aufgeführten Kriterien zu berücksichtigen."

39 BVerfG, Beschl. v. 8.8.1978 – Az. 2 BvL 8/77, Rn. 105 (juris).

40 BVerfG, Beschl. v. 8.8.1978 – Az. 2 BvL 8/77, Rn. 106 (juris).

41 BVerfG, Beschl. v. 8.8.1978 – Az. 2 BvL 8/77, Rn. 107 (juris).

42 BVerwG, Beschl. v. 25.9.1992 – Az. 4 B 150.92, Rn. 4 (juris).

43 BVerfG, Beschl. v. 8.8.1978 – Az. 2 BvL 8/77, Rn. 108 (juris).

nur auf das technisch gegenwärtig Machbare abzustellen. Dabei müssen ggf. auch aktuell umstrittene Forschungsergebnisse berücksichtigt werden.[44]

Der „Stand der Technik" ist somit zwischen den „allgemein anerkannten Regeln der Technik" und dem „Stand der Wissenschaft" angesiedelt. Einerseits kommt es nicht darauf an, ob eine Technik bereits in der Praxis etabliert ist, anderseits ist auch nicht allein auf ggf. noch umstrittene wissenschaftliche Erkenntnisse abzustellen. Vielmehr kommt es darauf an, was nach dem Meinungstand der angewandten Wissenschaft geeignet und angemessen ist. Dabei ist grundsätzlich zu berücksichtigen, dass der Maßstab nicht statisch ist, sondern sich die Wissenschaft (und auch die Praxis) ständig verändern.[45] Das bedeutet insbesondere, dass (auch anerkannte) Standards oder Normen nicht unbedingt den Stand der Technik abbilden müssen,[46] sondern hinter diesem zurückbleiben können.

Was im Bereich der Verschlüsselung dem Stand der Technik entspricht, ist somit kein primär rechtswissenschaftliches Problem. Vielmehr ist insoweit auf den *Sachverstand* der jeweiligen Techniker abzustellen. Zu einem Problem für Juristen wird die Frage nach dem Stand der Technik erst, wenn es zu einem Streit hierüber kommt. Dies kann etwa der Fall sein, wenn eine Aufsichtsbehörde eine Aufsichtsmaßnahme anordnet, weil sie der Meinung ist, dass ein Unternehmen ein Verschlüsselungsverfahren eingesetzt hat, welches nicht dem Stand der Technik entspricht. Regelmäßig wird die Aufsichtsbehörde als Fachbehörde über einen entsprechenden Sachverstand verfügen. Wäre nun aber das Unternehmen der Meinung, die Behörde habe den Sachverhalt fehlerhaft beurteilt, könnte es Rechtsbehelfe gegen die behördliche Entscheidung einlegen und letztlich müsste ein Gericht entscheiden. Das Gericht – welches höchstwahrscheinlich – nicht über den entsprechenden Sachverstand verfügen würde,[47] müsste dann ein Sachverständigengutachten einholen und so ermitteln,[48] was dem Stand der Technik entspricht. Dabei wäre das Gericht allerdings nicht an das Sachverständigengutachten gebunden, sondern müsste dieses frei würdigen.[49]

Insoweit lassen sich aus rechtswissenschaftlicher Sicht in Bezug auf Verschlüsselungsverfahren allenfalls grobe Leitlinien festhalten: Soweit Verfahren gebrochen sind (und praktisch relevante Angriffe existieren), entsprechen diese auch dann

44 BVerfG, Beschl. v. 8.8.1978 – Az. 2 BvL 8/77, Rn. 109 f. (juris).

45 *Withus,* CCZ 2015, 139, 141.

46 BVerwG, Beschl. v. 30.9.1996 – Az. 4 B 175.96, Rn. 5 (juris) formuliert hierzu (allerdings in Bezug auf Regeln der Technik): „DIN-Vorschriften und sonstige technische Regelwerke kommen hierfür als geeignete Quellen in Betracht. Sie haben aber nicht schon kraft ihrer Existenz die Qualität von anerkannten Regeln der Technik und begründen auch keinen Ausschließlichkeitsanspruch. Als Ausdruck der fachlichen Mehrheitsmeinung sind sie nur dann zu werten, wenn sie sich mit der Praxis überwiegend angewandter Vollzugsweisen decken. Das wird häufig, muß aber nicht immer der Fall sein. Die Normausschüsse des Deutschen Instituts für Normung sind pluralistisch zusammengesetzt. Ihnen gehören auch Vertreter bestimmter Branchen und Unternehmen an, die ihre Eigeninteressen einbringen. Die verabschiedeten Normen sind nicht selten das Ergebnis eines Kompromisses der unterschiedlichen Zielvorstellungen, Meinungen und Standpunkt ... Sie begründen eine tatsächliche Vermutung dafür, daß sie als Regeln, die unter Beachtung bestimmter verfahrensrechtlicher Vorkehrungen zustande gekommen sind, sicherheitstechnische Festlegungen enthalten, die einer objektiven Kontrolle standhalten, sie schließen den Rückgriff auf weitere Erkenntnismittel aber keineswegs aus. Die Behörden, die im Rahmen des einschlägigen Rechts den Regeln der Technik Rechnung zu tragen haben, dürfen dabei auch aus Quellen schöpfen, die nicht in der gleichen Weise wie etwa die DIN-Normen kodifiziert sind."

47 BVerwG, Urt. v. 25.9.1992 – Az. 8 C 28.90, Rn. 10 (juris).

48 *Withus,* CCZ 2015, 139, 140 formuliert zutreffend: „Der Richter bestimmt nicht, was allgemein anerkannt ist, sondern er ermittelt es!".

49 Vgl. *Scherer/Fruth,* CCZ 2015, 9, 13; *Withus,* CCZ 2015, 139, 139.

nicht mehr dem Stand der Technik, wenn sie in der Praxis noch weit verbreitet sind.[50] Hingegen ist es irrelevant, wenn in der Forschung mögliche Angriffsszenarien diskutiert werden, deren Realisierung noch nicht abzusehen ist. Das mag etwa gelten für Angriffe auf asymmetrische Verschlüsselungsverfahren durch zukünftige Quantencomputer.[51]

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) existiert eine Bundesoberbehörde, zu deren Aufgaben unter anderem die Beurteilung der Sicherheit von Verschlüsselungsverfahren zählt[52] und die über einen entsprechenden personellen Sachverstand verfügt, um den aktuellen Stand der Technik und Wissenschaft zu beurteilen. Dementsprechend kommt den Empfehlungen des BSI zur Sicherheit von Verschlüsselungsverfahren und Schlüssellängen[53] eine besondere praktische Bedeutung zu.[54]

4.4 Verschlüsselungspflichten

Nur sehr wenige Vorschriften schreiben eine ausdrückliche Verschlüsselung von Daten vor. Alle diese Normen betreffen die Übermittlung von Daten über „allgemein zugängliche Netze", also insbesondere das Internet.

Diese gesetzlichen Regelungen lassen sich primär zwei Rechtsgebieten zuordnen:

1. dem Datenschutzrecht und

2. dem Abgaben- bzw. Steuerrecht.

4.4.1 Datenschutzrecht

Im sektorspezifischen Datenschutzrecht findet sich eine Reihe von Vorschriften, nach denen personenbezogene Daten nur verschlüsselt übermittelt werden dürfen. Diese lassen sich wiederum überwiegend dem Sozialrecht zuordnen.

4.4.1.1 Sozialrecht

Mehrere Vorschriften im Sozialrecht schreiben vor, dass Sozialdaten nur verschlüsselt übermittelt werden dürfen. Eine Besonderheit ist dabei, dass die Datenübertragung aus „systemgeprüften Programmen" erfolgen muss. [55] Dies ist etwa vorgesehen in:

§ 23c Abs. 2, Abs. 2a, Abs. 2b SGB IV,

§ 28 Abs. 4 SGB IV,

§ 28a SGB IV,

50 Vgl. die Beispiele bei *Bergt,* CR 2014, 726, 730.

51 Hierauf weist auch *Ernestus,* in: Simitis, § 9 Rn. 171 hin, der insoweit allerdings auf Aspekte einer wirtschaftlichen Machbarkeit abstellt.

52 Vgl. § 3 Abs. 12 Nr. 3, 7, 9 BSI-Gesetz.

53 Hierauf weisen auch *Bergt,* CR 2014, 726, 729; *Ernestus,* in: Simitis, § 9 Rn. 177 hin. Relevant ist insofern insbesondere die Technische Richtlinie des BSI, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1.

54 Ausführlich zu den kryptografischen Empfehlungen und Vorgaben durch das BSI: *Herchenbach-Canarius/Illies/Lochter/Sommer/Stein,* in: Kilian/Heussen, Teil 15. Datensicherheit – Kryptografie Rn. 56 ff.

55 Die Einführung dieser Melde- und Übermittlungsmöglichkeit zielte auf eine Beschleunigung der Arbeitsabläufe und die Erhöhung der Verfahrenssicherheit ab, vgl. BT-Drs. 15/4228, 21.

§ 202 Abs. 2 SGB V und

§ 196a SGB VI.[56]

Programme zur Lohn- und Gehaltsabrechnung oder zur Erstellung oder Annahme von Meldungen müssen vor ihrem Einsatz geprüft und zugelassen werden.[57] Die Zulassung erfolgt durch den Spitzenverband Bund der Krankenkassen.[58] Die Einzelheiten der Systemprüfung regeln der Spitzenverband Bund der Krankenkassen, die Deutsche Rentenversicherung Bund, die Deutsche Rentenversicherung Knappschaft-Bahn-See, die Deutsche Gesetzliche Unfallversicherung e. V. und die Bundesagentur für Arbeit einvernehmlich in sog. Gemeinsamen Grundsätzen.[59]

Allerdings schreiben die sozialgesetzlichen Vorschriften nicht zwingend die Nutzung systemgeprüfter Programme vor. Insbesondere für kleine Unternehmen[60] ist als Alternative die Datenübertragung mittels maschinell erstellter Ausfüllhilfen vorgesehen. Die Ausfüllhilfen werden kostenfrei in verschiedenen Formen über das Projekt sv.net[61] zur Verfügung gestellt. Verfügbar ist eine reine Online-Version, bei der die Daten über ein WWW-Formular verschlüsselt übermittelt werden können. Es existiert außerdem eine kostenfreie Windows-Einzelplatzanwendung, über die die Daten ebenfalls verschlüsselt über das Internet übertragen werden.[62]

Die entsprechenden sozialrechtlichen Vorschriften setzen also entweder den Einsatz eines systemgeprüften Programms oder von Ausfüllhilfen voraus. In sämtlichen Konstellationen erfolgt die Kommunikation verschlüsselt, ohne dass Unternehmen weitere Vorkehrungen treffen müssen.

Weitere Vorschriften im Sozialrecht verlangen die Nutzung von „Verschlüsselungsverfahren" bzw. „Verschlüsselungsverfahren, [die] dem jeweiligen Stand der Technik entsprechen [müssen]":

§ 5 Abs. 3 Unfallversicherungs-Anzeigeverordnung sowie

§ 4 Abs. 1 Verordnung zur Durchführung der steuerlichen Vorschriften des Einkommensteuergesetzes zur Altersvorsorge und zum Rentenbezugsmitteilungsverfahren sowie zum weiteren Datenaustausch mit der zentralen Stelle.

Jedenfalls im Bereich der Unfallmeldungen stellen verschiedene Versicherungsträger WWW-Schnittstellen zur Verfügung, über die Unfälle gemeldet werden können.[63] Nutzt der Meldende ein entsprechendes Portal, ist automatisch für eine Verschlüsselung gesorgt.

56 Vgl. außerdem § 18 Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung.

57 § 20 Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung.

58 § 21 Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung.

59 § 22 Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung.

60 Vgl. hierzu BT-Drs. 15/4228, 21.

61 „Sozialversicherung im Internet", weitere Informationen sind im Internet verfügbar unter <http://www.itsg.de/svnet_Startseite.html>.

62 Vgl. ITSG GmbH, Kurzanleitung zu sv.net, Stand: Mai 2012, im Internet abrufbar unter <https://download.gkvnet-ag.de/kurzanleitung.pdf>.

63 Etwa Unfallkasse NRW <https://extranet.unfallkasse-nrw.de/login/perl/login.pl> oder Gemeinde-Unfallversicherungsverband Hannover Landesunfallkasse Niedersachsen <http://lukn.de/service/extranet/>.

4.4.1.2 § 113d TKG

Eine gewisse Sonderstellung nimmt § 113d TKG ein. Hiernach müssen die im Rahmen der sog. Vorratsdatenspeicherung gespeicherten Daten durch „technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme und Verwendung geschützt werden". Insoweit handelt es sich um eine typische Generalklausel, wie sie in verschiedenen datenschutzrechtlichen Vorschriften zu finden ist. Allerdings werden die zu ergreifenden Maßnahmen weiter konkretisiert. So wird unter anderem der „Einsatz eines besonders sicheren Verschlüsselungsverfahrens" ausdrücklich benannt. Diese gesetzliche Regelung trägt der Kritik des BVerfG an der Ausgestaltung der Vorratsdatenspeicherung durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[64] Rechnung.[65]

§ 113d TKG wird durch § 113f TKG flankiert. Hiernach erstellt die Bundesnetzagentur im Benehmen mit dem BSI einen Anforderungskatalog. Dieser Katalog ist zwar nicht verbindlich, allerdings wird nach § 113f Abs. 1 S. 2 TKG vermutet, dass die zur Vorratsdatenspeicherung verpflichteten Betreiber öffentlich zugänglicher Telekommunikationsdienste für Endnutzer einen besonders hohen Standard der Datensicherheit gewährleisten, wenn sie die Anforderungen des Kataloges erfüllen.

Der Anforderungskatalog verpflichtet nicht zum Einsatz bestimmter Verschlüsselungsverfahren, sondern schreibt nur vor, dass die Datenspeicher „mit einem geeigneten Verschlüsselungsverfahren ... verschlüsselt werden".[66] In einem Klammerzusatz wird allerdings auf die Technische Richtlinie des BSI zu kryptographischen Verfahren (BSI-TR-02102-1) verwiesen.

4.4.1.3 Sonstiges sektorspezifisches Datenschutzrecht

Eine Verschlüsselung bei der „Nutzung allgemein zugänglicher Netze" wird auch in einer Reihe weiterer Vorschriften des sektorspezifischen Datenschutzrechts gefordert. Es handelt sich hierbei letztlich aber um einige sehr spezifische Regelungen, von denen nur Unternehmen in einzelnen Branchen betroffen sind. Hierbei handelt es sich um:

§ 7 S. 3 WpHG-Mitarbeiteranzeigeverordnung (Mitarbeiter in der Anlageberatung im Sinne des § 34d Absatz 1 des Wertpapierhandelsgesetzes),

§ 28 Abs. 6 S. 3 und § 43 Abs. 2 Röntgenverordnung (Menschen, die Röntgenstrahlung ausgesetzt sind),

§ 115 Abs. 2 Strahlenschutzverordnung (Menschen, die ionisierender Strahlung ausgesetzt sind),

§ 4 Abs. 3 S. 12 Fahrpersonalgesetz (Fahrpersonal von Kraftfahrzeugen sowie von Straßenbahnen) sowie

64 BGBl. 2007 I, 3198.

65 BT-Drs. 18/5088, 46. Vgl. zu den verfassungsgerichtlichen Ausführungen auch unten, S. 40 ff. (unter 4.5.1.1).

66 Ziffer 5.2.2. Anforderungskatalog nach § 113f TKG.

§ 2 Abs. 6 Fahrpersonalverordnung (Fahrer von [bestimmten] Fahrzeugen zur Güter- und Personenbeförderung).

Die entsprechenden Vorschriften zielen erkennbar auf den Schutz der Persönlichkeitsrechte der jeweils betroffenen Personen ab.

Ebenfalls dem Datenschutzrecht zuzuweisen ist § 19 Abs. 4 Messstellenbetriebsgesetz.[67] Hiernach müssen bei Strommessgeräten, die in irgendeiner Weise in allgemein zugängliche Kommunikationsnetze eingebunden sind, Verschlüsselungsverfahren angewendet werden. Die Vorschrift begründet insofern eine Pflicht gegenüber den Herstellern solcher Systeme und (insbesondere) Netzbetreibern bzw. Messstellenbetreibern, die solche Geräte einsetzen wollen.

Gleiches gilt für die Verordnung über ein Register für Anlagen zur Erzeugung von Strom aus erneuerbaren Energien und Grubengas (Anlagenregisterverordnung). Hiernach errichtet und betreibt die Bundesnetzagentur ein Anlagenregister (§ 1 Anlagenregisterverordnung). Für die Übermittlung von Daten darf die Bundesnetzagentur ein bestimmtes Format sowie ein etabliertes und dem Schutzbedarf angemessenes Verschlüsselungsverfahren vorgeben (§ 7 Abs. 3, § 9 Abs. 4 und § 12 Abs. 2 Anlagenregisterverordnung). Entsprechende Regelungen finden sich in § 28 Abs. 4 Freiflächenausschreibungsverordnung, § 30 Abs. 1 Grenzüberschreitende-Erneuerbare-Energien-Verordnung, § 3 Abs. 3 und § 22 Abs. 5 Herkunftsnachweis-Durchführungsverordnung.

Ebenfalls dem Datenschutzrecht zuzuordnen ist § 6 DIMDI[68]-Verordnung. Die Verordnung regelt die Übermittlung von Mitteilungen, welche die Inverkehrbringer (Hersteller, Importeure etc.) von Medizinprodukten an das Deutsche Institut für Medizinische Dokumentation und Information machen müssen.[69] Diese Meldungen umfassen auch personenbezogene Daten.[70] Die Meldungen erfolgen allerdings über ein zentrales Erfassungssystem,[71] so dass die Betroffenen lediglich das entsprechende System nutzen müssen, welches dann für eine verschlüsselte Übertragung sorgt. Weitere Vorkehrungen müssen nicht getroffen werden.

4.4.1.4 Zusammenfassung

Im (Sozial-) Datenschutzrecht sehen verschiedene Vorschriften eine Verschlüsselung personenbezogener Daten bei der Übermittlung vor. Allerdings ist bei den für die Mehrzahl von kleinen und mittleren Unternehmen relevanten Vorschriften vorgesehen, dass besondere Programme oder WWW-Seiten für die Übermittlung genutzt werden. Der Nutzer muss also nicht selbst für eine Verschlüsselungsinfrastruktur sorgen, sondern Verschlüsselung erfolgt über die ohnehin eingesetzten Programme oder WWW-Schnittstellen.

67 Nach BT-Drs. 18/7555, 82 dient die Vorschrift „zur Sicherstellung von Datenschutz und Datensicherheit".

68 Deutsches Institut für Medizinische Dokumentation und Information.

69 Vgl. § 1 und § 2 DIMDI-Verordnung i. V. m. § 25, § 30 Abs. 2 und § 5 Medizinproduktegesetz.

70 Hierauf stellt auch BR-Drs. 749/02, 41 entscheidend ab.

71 § 2 Abs. 1 DIMDI-Verordnung.

4.4.2 Abgaben- und Steuerrecht

In der Abgabenordnung regelt § 87a Abs. 1 die elektronische Kommunikation. Die Norm enthält allerdings nur eine Verpflichtung der Finanzbehörde, Daten, die dem Steuergeheimnis unterliegen, mit einem geeigneten Verfahren zu verschlüsseln. Eine entsprechende Pflicht auf Seiten von Unternehmen besteht nicht.

Eine weitere steuerrechtliche Vorschrift zur Verschlüsselung von Daten findet sich in § 1 Abs. 3 Steuerdaten-Übermittlungsverordnung. Hiernach sind „im Falle der Nutzung allgemein zugänglicher Netze ... Verschlüsselungsverfahren anzuwenden."

Die Begründung zur Steuerdaten-Übermittlungsverordnung führt hierzu aus, „dass die für die elektronische Übermittlung sensibler Daten erforderlichen Maßnahmen zu treffen sind".[72] Die Verordnung betrifft allerdings nicht die „normale" Kommunikation zwischen steuerpflichtigen Unternehmen und der Finanzverwaltung, sondern „die Übermittlung von für das Besteuerungsverfahren erforderlichen Daten" über bestimmte Schnittstellen.[73] Die Vorschriften zielen damit letztlich auf die Schaffung einer sicheren vom Staat zur Verfügung gestellten Kommunikationsinfrastruktur ab. Eine (relevante) *eigenständige* Belastung durch eine Verschlüsselungspflicht ist hiermit nicht verbunden.[74] Will der Steuerpflichtige elektronisch mit der Finanzverwaltung kommunizieren, muss er hierzu ohnehin die staatlicherseits vorgegebenen Schnittstellen nutzen.[75]

Die Steuerdaten-Übermittlungsverordnung betrifft damit die Kommunikation zwischen Steuerpflichtigen und der Finanzverwaltung mittels „Programme[n], die für die Verarbeitung von für das Besteuerungsverfahren erforderlichen Daten bestimmt sind".[76] Oder anders formuliert: Die Steuerdaten-Übermittlungsverordnung gestaltet das automatisierte Besteuerungsverfahren[77] näher aus, indem sie Anforderungen an die entsprechenden Programme[78] und die Prüfung dieser Programme[79] normiert.

Will (bzw. muss) ein Unternehmen am automatisierten Besteuerungsverfahren teilnehmen, ist es darauf angewiesen, ein entsprechendes Programm zu nutzen. Dieses Programm muss dann verschlüsselt kommunizieren können. Sobald Unternehmen entsprechende Programme einsetzen, übermitteln sie Daten verschlüsselt, ohne dass es weiterer Anstrengungen bedarf.

72 BR-Drs. 892/02, 11.

73 Vgl. § 1 Abs. 1 und § 2 Steuerdaten-Übermittlungsverordnung.

74 Vgl. allgemein zur Frage der Nutzung spezieller Programme zur Übermittlung von Daten an die Finanzverwaltung: FG Bremen, Urt. v. 26.6.2014 – Az. 2 K 12/14 (2), FG Neustadt, Urt. v. 15.7.2015 – Az. 1 K 2204/13; FG Stuttgart, Urt. v. 23.3.2016 – Az. 7 K 3192/15.

75 Abgesehen davon dürfte die ganz überwiegende Zahl der Steuerpflichtigen ein großes bis essentielles Interesse an einer sicheren und verschlüsselten Übermittlung haben, so dass pauschal eine kryptographische Absicherung vorgesehen werden darf.

76 Vgl. § 3 Abs. 1 Steuerdaten-Übermittlungsverordnung.

77 Vgl. etwa die Verordnungsermächtigung in § 150 Abs. 6 Abgabenordnung.

78 § 3 Steuerdaten-Übermittlungsverordnung.

79 § 4 Steuerdaten-Übermittlungsverordnung.

Entsprechende Regelungen finden sich in einer Reihe weiterer steuerrechtlicher Vorschriften, die einzelne Verbrauchsteuern regeln und die folglich nur sektorspezifisch relevant sind:

§ 46 Abs. 3 Biersteuerverordnung,

§ 61 Abs. 3 Branntweinsteuerverordnung,

§ 7 Abs. 4 Energiesteuer- und Stromsteuer-Transparenzverordnung,

§ 38 Abs. 3 Kaffeesteuerverordnung,

§ 4 Abs. 3 Luftverkehrsteuer-Durchführungsverordnung,

§ 42a Abs. 4 Schaumwein- und Zwischenerzeugnissteuerverordnung und

§ 54 Abs. 3 Tabaksteuerverordnung (wie Steuerdaten-Übermittlungsverordnung).

Im Abgabenrecht ist somit in verschiedenen Vorschriften die verschlüsselte Übertragung von steuerlich relevanten Daten vorgesehen. Letztlich bedeutet dies aber vor allem, dass staatliche Schnittstellen zur Datenübermittlung vorgegeben werden, die eine Verschlüsselung der übertragenen Daten vorsehen. Nutzt der Steuerpflichtige die entsprechenden Schnittstellen (oder Programme), werden die Daten automatisch verschlüsselt, ohne dass es hierfür weiterer Maßnahmen seitens des Steuerpflichtigen bedürfte.

4.4.2.1 Geheimschutz

Weitere rechtliche Verschlüsselungspflichten können sich im Bereich des staatlichen Geheimschutzes ergeben. Betroffen können hiervon Unternehmen sein, die mit staatlichen Verschlusssachen umgehen.

Der Umgang mit Verschlusssachen ist – soweit hier relevant – in den Verschlusssachenanweisungen der Länder und des Bundes geregelt. Bei der Verschlusssachenanweisung des Bundes (VS-Anweisung) handelt es sich um eine allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern. Solche Verwaltungsvorschriften erzeugen grundsätzlich nur eine verwaltungsinterne Wirkung. Nach § 1 Abs. 2 VS-Anweisung „richtet" sich die Vorschrift aber auch an Private, die Zugang zu Verschlusssachen erhalten. Nach § 21 Abs. 2 i. V. m. 40 VS-Anweisung sind Verschlusssachen bei der Übertragung über Telekommunikationsverbindungen mit einem für den betreffenden Geheimhaltungsgrad zugelassenen Kryptosystem zu verschlüsseln.

4.4.2.2 Zusammenfassung

Gesetzliche verpflichtende Vorgaben zur Verschlüsselung von Daten finden sich vor allem im Datenschutz- und Abgabenrecht. Diese Vorschriften betreffen sämtlich die Übermittlung von Daten über allgemein zugängliche Netze – also insbesondere das Internet. Weitergehende *ausdrückliche* Verschlüsselungspflichten, etwa bei der Speicherung von Daten durch Private, sehen die entsprechenden Gesetze nicht vor.

Im Bereich des Datenschutzrechts findet die Verschlüsselungspflicht ihre Begründung im Schutz personenbezogener Daten Dritter, die es beim Transport über unsichere Netzverbindungen zu schützen gilt. Allerdings entsteht durch die entsprechende Verpflichtung in den praktisch relevanten Konstellationen keine eigenständige Belastung, weil ohnehin spezielle Programme oder WWW-Schnittstellen genutzt werden müssen, die ihrerseits für eine (transparente) Verschlüsselung sorgen.

Letzteres trifft auch auf Verschlüsselungspflichten im Bereich des Abgabenrechts zu. Auch hier werden staatlicherseits elektronische Kommunikationsschnittstellen zur Verfügung gestellt, die eine transparente Verschlüsselung vorsehen.

Weitere Verschlüsselungspflichten können sich beim Umgang mit staatlichen Verschlusssachen durch Private ergeben.

4.5 Verschlüsselungsobliegenheiten und Hinweispflichten (sowie hiermit in Zusammenhang stehende Vorschriften)

Unter einer Obliegenheit versteht man ein Gebot, dessen Befolgung nicht erzwungen werden kann, sondern das im eigenen Interesse besteht und bei dessen Nichtbeachtung Rechtsnachteile drohen.[80] Unter einer Verschlüsselungsobliegenheit werden deshalb im Folgenden gesetzliche Regelungen verstanden, die zwar Bezug auf eine Verschlüsselung nehmen, eine solche aber nicht zwingend vorschreiben. Erfasst werden damit insbesondere auch Vorschriften, bei denen es sich streng genommen nicht um Obliegenheiten im eigentlichen Sinne handelt, weil sich im konkreten Einzelfall Hinweise auf Verschlüsselungsmöglichkeiten zu entsprechenden Pflichten verdichten können. Außerdem wird eine Reihe von Vorschriften betrachtet, die zwar eine Verschlüsselung nicht ausdrücklich erwähnen, die aber einen naheliegenden Bezug zu einer Verschlüsselung aufweisen.

80 *Musielak/Hau,* Grundkurs BGB, Rn. 629.

4.5.1 Datenschutzrecht[81]

4.5.1.1 § 9 BDSG[82] nebst Anlage

Technische und organisatorische Maßnahmen

Das BDSG enthält in § 9 eine Verpflichtung, „die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes ... zu gewährleisten." Erforderlich sind Maßnahmen aber nur dann, „wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht".[83]

Diese Vorschrift wird durch eine Anlage weiter konkretisiert. In der „Anlage zu § 9 S. 1" ist ein Katalog mit Maßnahmen enthalten, die „je nach der Art der zu schützenden personenbezogenen Daten geeignet sind" beispielsweise „zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können" (Nr. 2). Weitere Maßnahmen sind etwa eine Zugriffskontrolle (Nr. 3) oder eine Weitergabekontrolle (Nr. 4). S. 2 der Anlage zu § 9 S. 2 BDSG benennt als eine Maßnahme, die „insbesondere" geeignet ist, „die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren".

§ 9 BDSG adressiert zunächst Aspekte der Datensicherheit bzw. Datensicherung.[84] Erfasst werden dabei sowohl äußere Einflüsse als auch fehlerhafte oder missbräuchliche innere Abläufe.[85] Die Norm differenziert insoweit nicht danach, ob Gefahren für personenbezogene Daten durch betriebsfremde Dritte – etwa Hacker – drohen oder von Innentätern ausgehen.

In § 9 S. 1 BDSG wird generalklauselartig eine Verpflichtung auferlegt, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen. Bereits der Wortlaut – „*insbesondere* die in der Anlage zu diesem Gesetz genannten Anforderungen"[86]; „dabei sind *insbesondere* Maßnahmen zu treffen, die ..."[87] – macht deutlich, dass die im Gesetz benannten Maßnahmen *nicht abschließend* sind. Erfasst werden somit letztlich „alle denkbaren Mechanismen", die jeweils erforderlich sind.[88] Gleichzeitig verdeutlicht der Wortlaut, dass nicht in jedem Fall sämtliche der benannten Maßnahmen zu ergreifen sind, sondern stets nur die,

81 Die Abgrenzung erfolgt im Folgenden nicht ganz trennscharf, weil einige Normen neben datenschutzrechtlichen Aspekten auch weitere Gesichtspunkte wie etwa das Fernmeldegeheimnis (§ 109 TKG) oder die Systemsicherheit (§ 13 TMG) adressieren. Sie werden dennoch im datenschutzrechtlichen Kontext behandelt, weil die jeweiligen Anforderungen und Tatbestandsvoraussetzungen vergleichbar sind.

82 Am 25. Mai 2016 ist die Datenschutz-Grundverordnung in Kraft treten. Durch sie werden zahlreiche Vorschriften des BDSG ersetzt werden. Derzeit befindet sich ein ABDSG in der politischen Diskussion. Die im Folgenden relevanten Vorschriften dürften in weiten Teilen durch die Datenschutz-Grundverordnung hinfällig werde. Allerdings enthalten die ab dem 25. Mai 2018 geltenden Regelungen der Datenschutz-Grundverordnung – soweit sie hier relevant sind – zahlreiche Parallelen zum BDSG. Da zum BDSG bereits ein umfangreiches Schrifttum existiert, während eine solches zur Datenschutz-Grundverordnung erst im Entstehen ist, werden zunächst die BDSG-Vorschriften unter Auswertung des entsprechenden Schrifttums ausgewertet und es werden dann Parallelen bzw. Unterschiede zur Datenschutz-Grundverordnung benannt.

83 § 9 S. 2 BDSG.

84 *Gola/Schomerus,* § 9 Rn. 1; *Plath,* in: Plath, § 9 Rn. 1.

85 *Plath,* in: Plath, § 9 Rn. 1.

86 § 9 S. 1 BDSG (Hervorhebung nur hier).

87 S. 1 der Anlage zu § 9 S. 1 BDSG (Hervorhebung nur hier).

88 *Plath,* in: Plath, § 9 Rn. 11.

„die je nach der Art der zu schützenden personenbezogenen Daten ... geeignet[89] sind", das jeweilige Ziel zu erreichen. Welche konkreten Maßnahmen zu ergreifen sind, hängt also von den besonderen Umständen des jeweiligen Einzelfalls ab.[90] Die zu treffenden Maßnahmen können grundsätzlich etwa baulicher Art (Schlösser) oder personeller Natur (Datenschutzbeauftragter, besondere Schulung) sein, sie können durch IT-Verfahren umgesetzt oder durch betriebliche Abläufe geregelt werden.[91]

Weiter steht die Verpflichtung unter einem Verhältnismäßigkeitsvorbehalt.[92] Erforderlich sind hiernach nur Maßnahmen, deren Schutzwirkung in einem angemessenen Verhältnis zu dem Aufwand steht, den sie verursachen.[93] Es hat also eine Abwägung zwischen den beiden Bezugsgrößen Schutzzweck und Aufwand stattzufinden.[94] Dabei ist nach S. 1 der Anlage zu § 9 S. 1 BDSG insbesondere die „Art der zu schützenden personenbezogenen Daten" bei der Abwägung zu berücksichtigen. Je sensibler solche Daten sind, desto mehr Aufwand muss betrieben werden, um die Daten zu schützen. Auf der anderen Seite sind der finanzielle, zeitliche und organisatorische Aufwand bei der Abwägung zu berücksichtigen.[95] Allerdings folgt hieraus nicht, dass *erforderliche* Maßnahmen nicht erfolgen müssen, weil sie etwa zu teuer wären.[96] Kann ein bestimmter Schutzzweck nur auf *eine* Weise erreicht werden, so muss die entsprechende Maßnahme auch ergriffen werden.[97]

Es muss also grundsätzlich eine umfassende Risikoanalyse erfolgen.[98]

S. 3 der Anlage zu § 9 S. 1 BDSG benennt nun als eine mögliche Maßnahme für Zugangs-, Zugriffs- und Weitergabekontrolle (S. 2 Nr. 2 bis 4 der Anlage zu § 9 S. 1 BDSG) „insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren". Aus der Formulierung „insbesondere" folgt, dass Verschlüsselungsverfahren nicht zwingend vorgeschrieben werden, sondern die entsprechenden Maßnahmen auch auf anderem Weg umgesetzt werden können.[99]

Der Satz ist erst im Jahr 2009 in das BDSG eingefügt worden.[100] In der Beschlussempfehlung des Innenausschusses (u. a.) zu dem Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften heißt es hierzu:

---

89 Die Verwendung des Begriffs „geeignet" dürfte einer gesetzgeberischen Ungenauigkeit geschuldet sein; gemeint sein dürfte „erforderlich", vgl. *Plath,* in: Plath, § 9 Rn. 23.

90 *Conrad/Huppertz,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 173; *Gola/Schomerus,* § 9 Rn. 7; *Plath,* in: Plath, § 9 Rn. 11.

91 *Plath,* in: Plath, § 9 Rn. 12.

92 § 9 S. 2 BDSG.

93 *Gola/Schomerus,* § 9 Rn. 7 unter Verweis auf *Nungesser,* Hessisches Datenschutzgesetz, § 10 Rn. 8. Dies ergibt sich freilich bereits aus dem Wortlaut von § 9 S. 2 BDSG.

94 *Gola/Schomerus,* § 9 Rn. 9.

95 *Plath,* in: Plath, § 9 Rn. 15.

96 *Schultze-Melling,* in: Taeger/Gabel, § 9 Rn. 31.

97 *Plath,* in: Plath, § 9 Rn. 15.

98 *Gola/Schomerus*, § 9 Rn. 9.

99 *Ernestus,* in: Simitis, § 9 Rn. 173.

100 Art. 1 Nr. 19 Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.7.2009, BGBl. 2009 I, 2814.

„Verschlüsselungsverfahren gehören bereits jetzt zu den technischen und organisatorischen Maßnahmen zur Zugangs-, Zugriffs- und Weitergabekontrolle nach Satz 2 Nummer 2 bis 4 der Anlage zu § 9 Satz 1. Da Verschlüsselungsverfahren in der Praxis noch nicht im wünschenswerten Umfang eingesetzt werden, sollen sie im Gesetz ausdrücklich als geeignete Maßnahmen erwähnt werden. Die Formulierung ‚dem Stand der Technik entsprechende' bringt zum Ausdruck, dass fortschrittliche Verfahren gemeint sind, die sich in der Praxis bewährt haben und einen hohen Sicherheitsstandard gewährleisten."[101]

Der Innenausschuss ist also davon ausgegangen, dass bereits in der Vergangenheit der Einsatz von Verschlüsselungsverfahren als Schutzmaßnahme im Sinne des BDSG in Frage kam. Allerdings war der Ausschuss der Meinung, dass solche Verfahren in der Praxis nur unzureichend eingesetzt würden. Deshalb sollten sie im Gesetz ausdrücklich erwähnt werden.

Anders formuliert: S. 3 der Anlage zu § 9 S. 1 BDSG kommt die Funktion einer „Erinnerung" zu. Den verantwortlichen Stellen (sowie Auftragsdatenverarbeitern) sollte in Erinnerung gerufen werden, dass personenbezogene Daten „insbesondere" durch den Einsatz von Verschlüsselungsverfahren geschützt werden können. In der Literatur ist diese gesetzgeberische Vorgehensweise auch als „kreativ platzierter gesetzgeberischer Hinweis" gewertet worden.[102] Auch in der datenschutzrechtlichen Praxis und Literatur war schließlich schon früher anerkannt, dass Verschlüsselungsverfahren geeignete Maßnahmen zur Erreichung der entsprechenden Schutzziele darstellen.[103]

Zusammenfassend lässt sind insoweit zunächst festhalten, dass personenbezogene Daten geschützt werden müssen. Welche Maßnahmen hierzu *konkret* zu ergreifen sind, ist gesetzlich nicht geregelt, sondern eine Frage des jeweiligen Einzelfalls. Dies können reine organisatorische Maßnahmen sein – etwa in einem Kleinbetrieb das an die Mitarbeiter gerichtete Verbot, den Computer im (abschließbaren) Zimmer des Chefs zu nutzen, auf welchem die Kundendaten gespeichert sind. Dies können aber auch technische Maßnahmen wie eine Verschlüsselung sein. Der Einsatz solcher Verfahren ist – je nach Fallgestaltung mehr oder minder – naheliegend und wird deshalb vom Gesetz nur beispielhaft erwähnt bzw. anempfohlen. Eine grundsätzliche Verpflichtung, Verschlüsselungsverfahren einzusetzen, ist hiermit nicht verbunden.[104]

Pflicht zur Verschlüsselung

Auch wenn aus der Anlage zu § 9 S. 1 BDSG keine grundsätzliche Verschlüsselungspflicht folgt, ist dennoch fraglich, ob es Fallkonstellationen gibt, in denen sich der „gesetzgeberische Hinweis" bzw. die allgemeinen Regeln zu einer Pflicht verdichten. Dies scheint zunächst fernliegend, wenn man die gesetzliche Struktur be-

101 BT-Drs. 16/13657, 23. Dabei ist freilich anzumerken, dass dieses Begriffsverständnis tendenziell von dem des BVerfG abweicht, wonach es für den Stand der Technik nicht darauf ankommt, ob sich ein Verfahren bereits in der Praxis bewährt hat, sondern der Stand der Technik, die „Front der technischen Entwicklung" beschreibt.

102 *Plath,* in: Plath, § 9 Rn. 88.

103 *Conrad/Huppertz,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 193; *Plath,* in: Plath, § 9 Rn. 88.

104 *Ernestus,* in: Simitis, § 9 Rn. 174; vgl. auch VG Berlin, Urt. v. 24.5.2011 – Az. 1 K 133.10, Rn. 20 f. (juris).

rücksichtigt, die es letztlich der verantwortlichen Stelle überlässt, in einer *konkreten* Situation *konkrete* Schutzmaßnahmen zu ergreifen. Allerdings besteht nach § 9 BDSG – bzw. nach den sonstigen gesetzlichen Regelungen – grundsätzlich eine *Pflicht,* die „innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird".[105] Kann dieses Ziel in einer konkreten Situation *allein* durch eine Verschlüsselung von Daten erreicht werden, dann kann auch eine entsprechende *Pflicht* hierzu bestehen. Diese Pflicht würde dann aber auch ohne den „gesetzgeberischen Hinweis" bestehen und allein daraus folgen, dass nur eine Verschlüsselung von Daten ein geeignetes Mittel ist, um für einen entsprechenden Schutz personenbezogener Daten zu sorgen.

Exkurs: besonders hoher Sicherheitsstandard für besonders sensible Daten

Eine entsprechende Pflicht könnte zunächst für besonders sensible Daten bestehen. Mit dem Schutz solcher Daten hat sich das BVerfG u. a. in seinem Urteil zur Vorratsdatenspeicherung[106] befasst.

Ausgangspunkt der entsprechenden Überlegungen war allerdings nicht unmittelbar die hier interessierende Frage, welche Maßnahmen Dritte ergreifen müssen, wenn sie mit besonders sensiblen personenbezogenen Daten umgehen, sondern die Frage, welche Maßnahmen der Staat ergreifen muss, wenn er Private verpflichtet, solche Daten für staatliche Zwecke zu speichern.[107]

Das Urteil betraf die Speicherung von Telekommunikationsverkehrsdaten (also Informationen darüber, wer wann mit wem kommuniziert hat) für sechs Monate. Das Gericht ist davon ausgegangen, dass die „Aussagekraft" dieser Daten „weitreichend" ist, weil sie „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers" ermöglichen.[108] Dieser Ansatz dürfte sich über den konkreten Bezug zu Telekommunikationsverkehrsdaten auch auf sonstige besonders aussagekräftige Daten verallgemeinern lassen. Besonders schutzwürdig wären nach diesem Ansatz grundsätzlich Daten, die in besonderer Weise Rückschlüsse auf die Persönlichkeit zulassen. Das könnte etwa für Daten gelten, die detaillierte Rückschluss über das Kaufverhalten einer Person liefern und deshalb Rückschlüsse auf Interessen, politische Ausrichtung (etwa anhand des Leseverhaltens) oder sogar sexuelle Präferenzen zulassen.

Das BVerfG ist weiter davon ausgegangen, dass für solche besonders aussagekräftigen Daten ein „besonders hohe[r] Sicherheitsstandard[...]" gewährleistet werden muss.[109] Im Kontext der Vorratsdatenspeicherung kritisiert das Gericht dann zunächst, dass die existierenden gesetzlichen Regelungen – genannt werden u. a. § 109 TKG und § 9 BDSG[110] – Raum für Wirtschaftlichkeitserwägungen im Einzelfall ließen.[111] Der Gesetzgeber habe es insoweit unterlassen, die „als Kernelemente genannten Instrumente (getrennte Speicherung, asymmetrische Verschlüsselung,

105 So die Formulierung in S. 1 Anlage zu § 9 S. 1 BDSG.
106 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08.
107 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 271 ff.
108 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 211.
109 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 271.
110 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 274.
111 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 271.

Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokollierung von Zugriff und Löschung) durchsetzbar vor[zu]geben".[112] Insoweit ist zunächst in Rechnung zu stellen, dass das Urteil Regelungen betraf, wonach Private aufgrund staatlicher Vorgaben besonders aussagekräftige Daten für staatliche Zwecke speichern mussten. Es ist deshalb konsequent, dass in dieser Situation auch der Staat (konkrete) Vorgaben für die Absicherung dieser Daten machen musste. Das Gericht musste in der konkreten Verfahrenssituation einer Verfassungsbeschwerde nicht klären, welche Sicherungsmaßnahmen erforderlich sind. Vielmehr konnte es sich insoweit darauf beschränken, festzustellen, dass der Gesetzgeber überhaupt keine konkreten Sicherungsmaßnahmen vorgesehen hatte. Dennoch ist es bemerkenswert, dass das Gericht als Beispiel für ein „Kernelement" für die Sicherung entsprechender Daten eine „asymmetrische Verschlüsselung" angesehen hat. Das lässt immerhin den Schluss zu, dass das Gericht davon ausgegangen ist, dass solche Daten nicht unverschlüsselt übertragen[113] werden dürfen. Auch wenn sich das Gericht nicht ausdrücklich zur Speicherung der Daten geäußert hat, ist doch davon auszugehen, dass hierbei ebenfalls für einen entsprechenden Schutz durch Verschlüsselung gesorgt werden muss. Dieses Verständnis liegt auch der Neuregelung der Vorratsdatenspeicherung[114] zugrunde. § 113d S. 2 Nr. 1 TKG sieht nämlich vor, dass die Vorratsdaten insbesondere durch „den Einsatz eines besonders sicheren Verschlüsselungsverfahrens" geschützt werden müssen. Diese Regelung soll den entsprechenden Bedenken des BVerfG Rechnung tragen.[115]

Allerdings ist erneut in Rechnung zu stellen, dass das Urteil eine Konstellation betraf, in welcher ein staatlicher Eingriff in das Fernmeldegeheimnis (als besondere Ausprägung des Rechts auf informationelle Selbstbestimmung) zu beurteilen war. Weiter ist aber auch zu berücksichtigen, dass die hier interessierenden Aussagen nur einen Teilaspekt betreffen, nämlich die Frage der Absicherung von Daten. In diesem Kontext ist es aber irrelevant, ob Private Daten verarbeiten oder der Staat. Aus der Sicht des Betroffenen ist es nämlich unerheblich, bei wem ggf. besonders sensible Daten abhandenkommen können. Deshalb differenziert das Datenschutzrecht hinsichtlich der Datensicherheit auch nicht zwischen öffentlichen und nichtöffentlichen Stellen.[116] Folglich dürften die Ausführungen des BVerfG zu den Anforderungen an die Datensicherheit grundsätzlich auf Private übertragbar sein.

Das Urteil des BVerfG zur Vorratsdatenspeicherung lässt sich dahingehend verstehen, dass Daten, die besonders aussagekräftig hinsichtlich der Persönlichkeitsstruktur sind, unter Anwendung eines besonders hohen Sicherheitsstandards zu schützen sind. Hierfür sind Daten u. a. durch den Einsatz eines besonders sicheren Verschlüsselungsverfahrens zu sichern.

112 BVerfG, Urt. v. 2.3.2010 – Az. 1 BvR 256/08, Rn. 275.

113 Asymmetrische (bzw. hybride) Verschlüsselungsverfahren kommen in erster Linie bei der Übertragung von Daten zum Einsatz, während bei der Speicherung von Daten eher symmetrische Verfahren eingesetzt werden.

114 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, BGBl. 2015 I, 2218.

115 BT-Drs. 18/5088, 22.

116 § 9 BDSG findet sich im ersten Abschnitt „Allgemeine und gemeinsame Bestimmungen", der sowohl für öffentliche wie auch für nichtöffentliche Stellen gilt. Art. 32 Datenschutz-Grundverordnung differenziert ebenfalls nicht danach, ob eine Datenverarbeitung durch private oder staatliche Verantwortliche erfolgt.

Exkurs: Betrieb von E-Mail-Servern[117]

Grundsätzliche Probleme stellen sich im Zusammenhang mit E-Mail-Servern, da hierüber praktisch immer datenschutzrechtlich relevante Daten verarbeitet werden. Sowohl beim Versand von Nachrichten über SMPT wie auch beim Abruf von E-Mails über POP3 oder IMAP stehen verschlüsselte Protokollvarianten zur Verfügung. Anders als bei einer Ende-zu-Ende-Verschlüsselung, die die Nutzung entsprechender (derzeit noch wenig verbreiteter) Programme (bzw. Plug-ins) auf den Endgeräten voraussetzt, ist die Konfiguration eines E-Mail-Servers, so dass dieser nur noch verschlüsselt mit E-Mail-Programmen und anderen E-Mail-Servern kommuniziert, verhältnismäßig einfach[118] möglich. Weiter ist zu berücksichtigen, dass die Kommunikation zwischen dem E-Mail-Programm und dem E-Mail-Server in vielen Konstellationen relativ einfach abgehört werden kann. Das ist insbesondere der Fall, wenn ungesicherte öffentliche WLANs genutzt werden (müssen). Hier ist es mit trivialen Mitteln möglich, fremde Kommunikation mitzulesen.[119] Gleiches gilt letztlich für sämtliche Angriffe, die aus einem lokalen Netz heraus erfolgen. E-Mails sind also insbesondere auf dem Weg zum und vom eigenen E-Mail-Server einer besonderen Gefährdung durch Angreifer ausgesetzt. Diese Gefahren lassen sich in vielen Fällen auch nur sinnvoll durch eine Transportverschlüsselung abschirmen.[120]

In die Abwägung ist also einzustellen, dass personenbezogene Daten auf dem Weg zum und vom E-Mail-Server besonderen Gefahren ausgesetzt sind. Diese Gefahren können durch eine Transportverschlüsselung sicher abgewehrt werden. Gleichzeitig ist eine solche Transportverschlüsselung relativ einfach auf dem E-Mail-Server einzurichten.

Es spricht deshalb einiges dafür, dass E-Mail-Server auch so konfiguriert sein *müssen,* dass über sie verschlüsselt kommuniziert werden kann. Diese Sicht wird von verschiedenen datenschutzrechtlichen Aufsichtsbehörden geteilt,[121] die in der Vergangenheit auch entsprechende Kontrollen vorgenommen und Zwangsgelder jedenfalls angedroht haben.[122] Die allgemeine Pflicht zum Schutz personenbezogener Daten kann sich insofern zu einer Pflicht, eine Transportverschlüsselung bereitzustellen, verdichten.

117 Die Zuordnung der entsprechenden Problematik zu § 9 BDSG ist wegen der Subsidiarität des BDSG (§ 1 Abs. 3) nicht unproblematisch. Zudem handelt es sich beim E-Mail-Dienst um eine Materie, die im Grenzbereich zwischen Telekommunikations- und Telemedienrecht angesiedelt ist.

118 I. S. v.: Es müssen nur an einer Stelle von einem Administrator die entsprechenden Einstellungen vorgenommen werden, wohingegen praktisch alle gängigen E-Mail-Programme (-Clients) ohne größeren Konfigurationsaufwand eine SSL/TLS-Verschlüsselung nutzen können.

119 Das Programm Wireshark dürfte etwa zur Grundausstattung jedes Netzwerkadministrators zählen.

120 Vgl. *Koch,* Verschlüsselungspraxis, E-Mail -> Dichtung und Wahrheit -> Technik.

121 ULD Schleswig-Holstein, Tätigkeitsbericht 2015, S. 139 betrachtet die Verschlüsselung als „bereits seit Jahren Stand der Technik"; BayLDA, Tätigkeitsbericht 2015/2016, S. 140.

122 BayLDA, Pressemitteilung v. 9.9.2014 <https://www.lda.bayern.de/media/pm2014_12.pdf>; BayLDA, Tätigkeitsbericht 2015/2016, S. 140.

Exkurs: Versand von E-Mails

Hoch umstritten ist die Frage, ob E-Mails, die personenbezogene (oder unternehmensrelevante)[123] Daten enthalten, grundsätzlich mit einer Ende-zu-Ende-Verschlüsselung gesichert werden müssen. Zahlreiche Stimmen im rechtswissenschaftlichen Schrifttum nehmen das an. Diese Sicht wird auch von (einigen)[124] datenschutzrechtlichen Aufsichtsbehörden geteilt. So hat die BfDI etwa den Versand von „Willkommensbriefen" per E-Mail, in denen Name, Anschrift, Kundenkennwort und Bankverbindung genannt waren, als Verstoß gegen § 9 S. 1 BDSG gewertet. Die „Willkommensbriefe" sind in der Folge per Post verschickt worden.[125] Andere Datenschutzbehörden gehen jedenfalls für den öffentlichen Bereich davon aus, dass personenbezogene Daten grundsätzlich nur verschlüsselt gemailt werden dürfen.[126]

Allerdings würde eine derartige Sicht dazu führen, dass der E-Mail-Dienst im unternehmerischen Bereich derzeit praktisch nicht mehr nutzbar wäre. Letztlich dürften die meisten E-Mails nämlich irgendwelche Informationen mit Personenbezug enthalten. Zwar stehen verschiedene Möglichkeiten zur Verfügung, E-Mails Ende-zu-Ende-verschlüsselt zu verschicken. Keine dieser Lösungen hat sich bislang aber soweit durchgesetzt, dass von einer relevanten Marktdurchdringung ausgegangen werden könnte.[127] Praktisch würde das also bedeuten, dass entsprechende Informationen nicht mehr per E-Mail verschickt werden dürften. So stehen nach einem Bericht der Landesbeauftragten für den Datenschutz und Informationsfreiheit Nordrhein-Westfalen verschiedene Versicherungsunternehmen vor dem Problem, dass Versicherte zwar an einer Kommunikation per E-Mail interessiert, aber nicht bereit seien, Angebote für eine Ende-zu-Ende-Verschlüsselung (oder auch nur sichere WWW-Portale) zu nutzen. Erwartet werde vielmehr eine „zügige und unkomplizierte Korrespondenz ohne Verschlüsselung".[128]

Auch der BGH geht davon aus, dass der E-Mail-Dienst grundsätzlich unsicher ist. Ohne weitere Begründung hat er ausgeführt, dass es einem Unternehmen nicht zugemutet werden kann, Unternehmensinterna per E-Mail unverschlüsselt an eine Behörde zu übermitteln. Dabei hat der BGH ausdrücklich darauf abgestellt, dass es *nicht* darauf ankommt, ob die zu übermittelnden Daten Betriebs- oder Geschäftsgeheimnisse enthalten.[129]

Ohne dies hier abschließend klären zu können, bestehen aber durchaus Zweifel, ob eine Übermittlung über das Internet zwischen den E-Mail-Servern (es geht insoweit also nicht um den Transport zwischen dem E-Mail-Programm und dem E-

123 Das gleiche Problem stellt sich unter „Compliance"-Gesichtspunkten mit Blick auf unternehmensbezogene E-Mails, so dass der Exkurs auch insoweit relevant ist.

124 Es ist nur eine stichprobenartige Auswertung erfolgt, weshalb hier keine Verallgemeinerung vorgenommen werden soll.

125 BfDI, Tätigkeitsbericht 2013/2014, S. 157.

126 LDI Berlin, Jahresbericht 2014, S. 21.

127 ULD Schleswig-Holstein, Tätigkeitsbericht 2017, S. 95 weist darauf hin, dass „Ende-zu-Ende-Verschlüsselung ... längst noch kein Standard in der E-Mail-Kommunikation" ist.

128 LDI NRW, Bericht 2017, S. 143; vgl. auch LDI Berlin, Jahresbericht 2016, wonach davon auszugehen sei, dass die E-Mail-Kommunikation zwischen den Berliner Schulen und Schulämtern – trotz entsprechender Hinweise und Aufforderungen – unverschlüsselt erfolge.

129 BGH, Beschl. 26.2.2013 – Az. KVZ 57/12, Rn. 2 (juris).

Mail-Server) tatsächlich deutlich unsicherer ist als etwa ein Telefongespräch, ein Fax oder ein Brief.[130]

Letztlich dürfte jedoch in Rechnung zu stellen sein, dass jedenfalls derzeit kein System für eine Ende-zu-Ende-Verschlüsselung verfügbar ist, welches eine praktisch relevante Markdurchdringung vorzuweisen hätte. Die Alternative zu einer unverschlüsselten Übertragung per E-Mail wäre deshalb regelmäßig der *vollständige Verzicht* auf eine elektronische Übermittlung. Es bestehen deshalb erhebliche Bedenken, ob der hiermit verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck (vgl. § 9 S. 2 BDSG) steht.[131] Das dürfte jedenfalls bei Daten gelten, die nur mäßig sensibel sind (weil sie etwa die rein berufliche Sphäre betreffen). Geht es dagegen um den Versand besonders sensibler Daten, dürfte von einer Pflicht zur Verschlüsselung oder zur Wahl einer alternativen Transportmethode auszugehen sein.[132] Das bayerische Landesamt für Datenschutzaufsicht geht inzwischen davon aus, dass bei Daten mit erhöhtem Schutzbedarf – wie etwa Gesundheitsdaten – sowohl eine Transport- als auch eine Inhaltsverschlüsselung als Stand der Technik anzusehen sind.[133]

Jedenfalls soweit nicht besonders sensible (personenbezogene) Daten betroffen sind, spricht vieles dafür, dass eine unverschlüsselte Nutzung des E-Mail-Dienstes nicht grundsätzlich ausgeschlossen ist. Einige Aufsichtsbehörden scheinen insoweit aber einer restriktiveren Sicht zuzuneigen. Hingegen dürfte sich bei besonders sensiblen Daten die allgemeine Schutzpflicht zu einer Verschlüsselungspflicht verdichten.

Sonstige Fälle einer „Ermessensreduzierung auf null"

Über die diskutierten Beispiele hinaus dürfte es weitere Fallkonstellationen geben, in denen eine Verschlüsselung die einzige angemessene technische und organisatorische Maßnahme ist, um personenbezogene Daten zu schützen. Das ULD Schleswig-Holstein berichtet von einem Fall, in welchem einem Kinderarzt ein Laptop mit Patientendaten gestohlen wurde.[134] Der Arzt hatte nach Einschätzung der Polizei „ausreichende Schutzmaßnahmen gegen Einbruch" getroffen. Das ULD Schleswig-Holstein ging deshalb davon aus, dass der Kinderarztpraxis kein Verstoß gegen datenschutzrechtliche Bestimmungen vorgeworfen werden konnte. Dennoch hat es den Arzt aufgefordert, Patientendaten zukünftig verschlüsselt zu speichern.[135] Welche Rechtsqualität diese „Aufforderung" hatte, wird nicht mitgeteilt. Insoweit ist zunächst anzumerken, dass offensichtlich auch das ULD (zunächst?)

130 Vgl. ausführlicher *Koch,* DuD 2014, 691, 691, 694.

131 So auch VG Berlin, Urt. v. 24.5.2011 – Az. 1 K 133.10, Rn. 20 (juris). Ausführlicher zu dem Urteil unter Abschnitt 4.6.2.1.

132 BfDI, Tätigkeitsbericht 2009/2010, S. 38 stellt darauf ab, dass „besonders schützenswerte" oder „sensible Daten wie beispielsweise Gesundheitsdaten" grundsätzlich nur Ende-zu-Ende-verschlüsselt übertragen werden dürfen.

133 BayLDA, Tätigkeitsbericht 2015/2016, S. 62.

134 ULD Schleswig-Holstein, Tätigkeitsbericht 2011, S. 61 f.; ULD Schleswig-Holstein, Tätigkeitsbericht 2017, S. 49 berichtet von einem vergleichbaren Fall, in welchem in eine Gemeinschaftspraxis für Neurologie, Psychiatrie, Psychosomatik und Psychotherapie eingebrochen wurde.

135 ULD Schleswig-Holstein, Tätigkeitsbericht 2011, S. 61 f.

davon ausging, dass eine physische Absicherung der Praxis gegen Einbruch ausreichend ist, um den datenschutzrechtlichen Schutzanforderungen nachzukommen. Demgegenüber kann die spätere „Aufforderung" allerdings auch darauf hindeuten, dass eine solche Einbruchssicherung (letztlich doch) nicht ausreichend ist, wenn es um den Schutz *besonders sensibler* Patientendaten geht.

Dabei dürfte zunächst zu bedenken sein, dass sich Einbrüche praktisch nicht vermeiden lassen und dass Laptops besonders einfach zu stehlen sind. Darüber hinaus ging es nicht um den Schutz irgendwelcher Daten mit Personenbezug, sonders es ging um besonders sensible Gesundheitsdaten von Kindern. In einer solchen Konstellation ist es jedenfalls nicht fernliegend, von einer Verdichtung der allgemeinen Sicherungspflicht hin zu einer Verschlüsselungspflicht auszugehen. Zudem dürfte zu berücksichtigen sein, dass eine Vollverschlüsselung von Laptops relativ einfach einzurichten ist, weil alle gängigen Betriebssysteme (jedenfalls in den Versionen für berufliche Anwender) entsprechende Möglichkeiten bereitstellen.

Dieser Ansatz dürfte dahingehend zu verallgemeinern sein, dass besonders sensible personenbezogene Daten,[136] die auf tragbaren Geräten gespeichert werden, verschlüsselt werden müssen.[137] Das wird jedenfalls dann gelten, wenn ein Verlust durch Diebstahl oder Unaufmerksamkeit nicht mit hinreichender Sicherheit ausgeschlossen werden kann.[138]

In der Unternehmensbefragung hat sich gezeigt, dass in 36 Prozent der befragten KMU Laptops/Notebooks grundsätzlich verschlüsselt werden.[139]

Geht man davon aus, dass im Einzelfall eine Verpflichtung zur Verschlüsselung bestehen kann, so ist weiter fraglich, welche Folgen ein Verstoß hiergegen haben kann.

Nach § 38 Abs. 5 BDSG kann die Aufsichtsbehörde Maßnahmen anordnen, die zur Beseitigung festgestellter Verstöße erforderlich sind.[140] Auch wenn im Beispiel des ULD Schleswig-Holstein nicht mitgeteilt ist, ob eine entsprechende hoheitliche Aufforderung erteilt wurde, ist eine solche doch grundsätzlich denkbar.

Eine ordnungswidrigkeiten- oder strafrechtliche Sanktionierbarkeit ist nicht vorgesehen.[141]

136 Also insbesondere Arten personenbezogener Daten i. S. v. § 3 Abs. 9 BDSG, aber auch sonstige besonders schützenswerten Daten, wie etwa Passwörter.

137 So auch ausdrücklich Bayerischer Landesbeauftragter für den Datenschutz, Tätigkeitsbericht 2009/2010, S. 97. Vgl. auch

138 Insoweit wäre der Fall im Beispiel ggf. anders zu lösen, wenn der Laptop nachts zusätzlich in einem Tresor verwahrt worden wäre.

139 Vgl. S. 20 (unter 3.5).

140 Vgl. hierzu *Bergt,* CR 2014, 726, 731.

141 *Plath,* in: Plath, § 9 Rn. 19. Allerdings kann ein Verstoß gegen § 9 BDSG gleichzeitig ein Verstoß gegen eine weitere Vorschrift des BDSG darstellen, der dann seinerseits bußgeldbewehrt sein kann. In diesem Sinne dürfte es zu verstehen sein, wenn *von Holleben/Menz,* CR 2010, 63, 68 auf die Gefahr von Bußgeldern bis 300.000 € hinweisen.

Zusammenfassung

Das BDSG sieht keine Pflicht zur Verschlüsselung personenbezogener Daten vor. Allerdings enthält die Anlage zu § 9 S. 1 BDSG einen Hinweis auf die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Zudem können sich die allgemeinen Pflichten zur Sicherung personenbezogener Daten im Einzelfall zu einer Verschlüsselungspflicht verdichten. Das kann insbesondere der Fall sein bei Daten, die besonders sensibel sind, weil sie eine hohe Aussagekraft über die Persönlichkeitsstruktur der Betroffenen aufweisen.

Weiter spricht vieles dafür, dass E-Mail-Server grundsätzlich eine Transportverschlüsselung zur Verfügung stellen müssen. Die Zulässigkeit eines unverschlüsselten Versands personenbezogener oder unternehmensrelevanter Daten per E-Mail ist in der rechtswissenschaftlichen Literatur umstritten. Letztlich dürfen hier aber die gewichtigeren Argumente gegen eine grundsätzliche Pflicht zu einer Ende-zu-Ende-Verschlüsselung sprechen. Allerdings neigen einige Aufsichtsbehörden zu einer deutlich restriktiveren Sicht.

4.5.1.2 § 78a SGB X nebst Anlage

Für den Bereich des Sozialdatenschutzes enthält § 78a SGB X eine § 9 BDSG entsprechende Vorschrift, die durch eine Anlage konkretisiert wird, welche ebenfalls der Anlage zu § 9 BDSG entspricht.

4.5.1.3 Art. 32 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung enthält in Art. 32 eine Vorschrift zur Datensicherheit. Hiernach müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Vorschrift entspricht in ihrer Grundkonzeption § 9 BDSG,[142] so dass zunächst auf die obigen Ausführungen[143] verwiesen werden kann.

Als Abwägungsgesichtspunkte werden der Stand der Technik, die Implementierungskosten, Art und Umfang, die Umstände und der Zweck der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere der mit der Verarbeitung verbundenen Risiken benannt.[144] Stärker als das BDSG wird insoweit der Kostenfaktor von Schutzmaßnahmen betont. Hieraus darf aber nicht geschlossen werden, dass nach der Datenschutz-Grundverordnung auf *erforderliche* Schutzmaßnahmen aus Kostengründen verzichtet werden dürfte.[145] Auch nach der Datenschutz-Grundverordnung hat also eine umfassende und auf die Besonderheiten des Einzelfalls zugeschnittene Abwägung zu erfolgen, welche Maßnahmen konkret ergriffen werden müssen.

Die Norm benennt – wie auch das BDSG – verschiedene Maßnahmen. Diese Maßnahmen „schließen unter anderem … die … Verschlüsselung personenbezogener

142 So auch *Grages,* in: Plath, Art. 32 DSGVO Rn. 1, 9.

143 Unter 4.5.1.1.

144 Art. 32 Abs. 1 Datenschutz-Grundverordnung.

145 *Grages,* in: Plath, Art. 32 DSGVO Rn. 3.

Daten"[146] ein. Eine Verschlüsselung wird also auch durch die Datenschutz-Grundverordnung nicht verpflichtend vorgeschrieben. Allerdings wird eine solche ausdrücklich als Schutzmaßnahme erwähnt. Eine gewisse Betonung gegenüber anderen Schutzmaßnahmen erfährt die Verschlüsselung durch Erwägungsgrund 83 Datenschutz-Grundverordnung. Hierin wird die Verschlüsselung als *einziges Beispiel* für die Eindämmung von Risiken genannt.

Mithin schreibt auch die Datenschutz-Grundverordnung eine Verschlüsselung von Daten nicht ausdrücklich oder zwingend vor. Allerdings verfolgt die Datenschutz-Grundverordnung einen Ansatz, der stärker als das BDSG auf einen Datenschutz durch Technik („data protection by design") abstellt. [147] So sind nach Art. 25 Abs. 1 Datenschutz-Grundverordnung bereits im „Zeitpunkt der Festlegung der Mittel für die Verarbeitung" technische Schutzmaßnahmen vorzusehen.

Wie bereits nach dem BDSG kann es Fallkonstellationen geben, in denen die in Art. 32 Abs. 1 Datenschutz-Grundverordnung vorgesehene Abwägung dazu führt, dass den Datenschutzgrundsätzen allein durch eine Verschlüsselung von Daten genügt werden kann. Das würde insbesondere bei der Übertragung sensibler personenbezogener Daten über unsichere Netzwerke gelten.

4.5.1.4 § 109 TKG

Nach § 109 TKG müssen Diensteanbieter die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen Verletzungen des Schutzes personenbezogener Daten treffen.[148]

Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste müssen zudem ein Sicherheitskonzept erstellen.[149] Dieses Konzept muss von Betreibern öffentlicher Telekommunikationsnetze der Bundesnetzagentur vorgelegt werden und kann von der Bundesnetzagentur von Betreibern öffentlich zugänglicher Telekommunikationsdienste angefordert werden.[150] Die Umsetzung des Sicherheitskonzepts wird regelmäßig (mindestens alle zwei Jahre) von der Bundesnetzagentur überprüft.[151] Als Grundlage für die Sicherheitskonzepte wird von der Bundesnetzagentur im Einvernehmen mit dem BSI und der BfDI ein Katalog von Sicherheitsanforderungen erstellt und veröffentlicht.[152]

Das TKG enthält insoweit keine konkreten Vorgaben für die Sicherheitskonzepte. Insbesondere wird nicht der Einsatz von Verschlüsselungstechniken vorgeschrieben.

146 Art. 32 Abs. 1 lit. a) Datenschutz-Grundverordnung.
147 Hierauf stellt Erwägungsgrund 78 ausdrücklich ab.
148 § 109 Abs. 1 TKG.
149 § 109 Abs. 4 S. 1 TKG.
150 § 109 Abs. 4 S. 2, 3 TKG.
151 § 109 Abs. 4 S. 6, 7 TKG.
152 § 109 Abs. 6 TKG.

Der derzeit geltende Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG[153] benennt an mehreren Stellen Verschlüsselungstechniken als mögliche Maßnahmen. Er schreibt den Einsatz aber nicht vor.

Allerdings macht der Katalog von Sicherheitsanforderungen sehr deutlich, dass der Einsatz von Verschlüsselungstechniken sinnvoll ist, um ein Sicherheitskonzept im Sinne von § 109 TKG zu erstellen und umzusetzen.

Insofern verpflichten weder § 109 TKG noch der auf dieser Grundlage veröffentlichte Sicherheitskatalog zum Einsatz von Verschlüsselungstechniken. Der Einsatz von Verschlüsselungstechniken erleichtert allerdings die Umsetzung der Pflichten nach § 109 TKG.

4.5.1.5 § 13 Abs. 7 TMG

Nach § 13 Abs. 7 TMG müssen (geschäftsmäßige Telemedien-) Diensteanbieter durch technische und organisatorische Vorkehrungen sicherstellen, dass keine unerlaubten Zugriffe auf ihre Infrastruktur erfolgten und ihre Einrichtungen gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen – einschließlich äußerer Angriffe – gesichert sind. Der Stand der Technik muss also in die Auswahl und Bewertung der zu ergreifenden Maßnahmen eingestellt werden, er muss aber nicht in jedem Fall umgesetzt werden.[154] Die entsprechenden Maßnahmen müssen den Stand der Technik berücksichtigen. Als eine mögliche Maßnahme benennt die Norm „die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens".[155]

Die Norm ist von ihrer Zielrichtung deutlich breiter aufgestellt als § 9 BDSG. Neben dem Schutz personenbezogener Daten zielt die Vorschrift auf die Verhinderung eines Missbrauchs von Telemediendiensten etwa zur Verbreitung von Schadsoftware.[156]

Die Norm schreibt den Einsatz von Verschlüsselungsverfahren nicht vor, sondern benennt diese lediglich beispielhaft. Anders gefasst: Der Diensteanbieter muss Daten nicht verschlüsseln, der Einsatz von Verschlüsselungsverfahren ist jedoch ein geeignetes – und vom Gesetzgeber empfohlenes – Mittel, die Pflichten nach § 13 Abs. 7 TMG zu erfüllen.

Allerdings ist es auch insoweit denkbar, dass sich in einem konkreten Anwendungsfall die *allgemeine* Pflicht zur Verhinderung unerlaubter Zugriffe *konkret* zu einer Verschlüsselungspflicht *verdichtet.* Das wird teilweise angenommen, wenn (personenbezogene) Daten über ein WWW-Formular eingegeben und über das Internet übertragen werden sollen. (Jedenfalls) einige datenschutzrechtliche Aufsichtsbehörden gehen davon aus, dass in diesem Fall für eine Verschlüsselung über

153 Version 1.1, Stand 7.1.2016, ABl. BNetzA 2016, 248. Der Katalog ist im Internet abrufbar unter < https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Katalog-Sicherheitsanforderungen.pdf?__blob=publicationFile&v=6>.

154 *Gerlach,* CR 2015, 581, 588.

155 § 13 Abs. 7 S. 2 TMG.

156 BT-Drs. 18/4096, 34. Vgl. außerdem *Gerlach,* CR 2015, 581, 584.

HTTPS gesorgt werden muss.[157] Gleiches dürfte gelten, wenn besonders sensible Daten wie etwa Passwörter übertragen (und gespeichert) werden.[158] Auch hier wird (etwa vom BSI) angenommen, dass eine Transportverschlüsselung implementiert werden muss.[159] Deutlich weiter geht das bayerische Landesamt für Datenschutzaufsicht. Dieses geht davon aus, dass bei besonders sensiblen Gesundheitsdaten – wie sie etwa über Kontaktformulare von Ärzten oder Apotheken übermittelt werden – zusätzlich für eine Ende-zu-Ende-Verschlüsselung („z. B. PGP mit 4096-Bit ... [etwa] durch eine Verschlüsselung innerhalb des Browsers (mittels Javascript)") gesorgt werden muss.[160]

4.5.1.6 § 13 Abs. 4 Nr. 3 TMG

Nach § 13 Abs. 4 Nr. 3 TMG müssen Diensteanbieter „durch technische und organisatorische Vorkehrungen sicherstellen, dass ... der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann". Die Norm knüpft an § 4 Abs. 2 Nr. 3 TDG an. In der Begründung zum Entwurf des TDG wird darauf abgestellt, dass hierdurch „das Fernmeldegeheimnis im Bereich der Teledienste zusätzlich abgesichert" werden sollte.[161] Das könnte darauf hindeuten, dass der Diensteanbieter grundsätzlich für eine Verschlüsselung von Daten während des Transports sorgen muss. Das würde konkret bedeuten, dass WWW-Seiten nur über das Hypertext Text Protocol Secure (HTTPS) ausgeliefert werden dürften.[162] Allerdings ist insoweit in Rechnung zu stellen, dass das TDG aus dem Jahr 1997 stammt. Seinerzeit war HTTPS zwar bereits „standardisiert", aber (sehr) weit davon entfernt, als Standard für die Übertragung von WWW-Seiten zu dienen.

Den Gesetzgebungsmaterialien ist insoweit auch nichts dafür zu entnehmen, dass beabsichtigt gewesen sein könnte, Diensteanbieter zu verpflichten, statt des (überaus) weit verbreiteten Hypertext Text Protocol (HTTP) nur noch die Secure-Variante (HTTPS) einzusetzen. Es ist deshalb näherliegend anzunehmen, dass der Gesetzgeber insoweit lediglich eine allgemeine datenschutzrechtliche Verpflichtung vorsehen wollte, für eine Zugangs- und Zugriffskontrolle zu sorgen, wie sie etwa in Nr. 2 und 3 der Anlage zu § 9 BDSG vorgesehen ist.[163]

Unter systematischen Gesichtspunkten spricht für eine solche Sicht auch, dass § 13 Abs. 4 Nr. 3 TMG anders als § 13 Abs. 7 TMG nicht ausdrücklich Bezug auf Verschlüsselung nimmt. Das wäre aber äußerst naheliegend gewesen, wenn die Norm darauf abzielen würde, eine verschlüsselte Übermittlung nach dem Hypertext Text

157 Vgl. etwa BayLDA, Tätigkeitsbericht 2015/2016, S. 142; LfD Bayern, Tätigkeitsbericht 2013/2014, S. 50; ders., Tätigkeitsbericht 2011/2012, S. 26; BfDI, Tätigkeitsbericht 2011/2012, S. 74 f. für das vergleichbare Problem bei Bundesbehörden. Nach ULD Schleswig-Holstein, Tätigkeitsbericht 2017, S. 122 „müssen" Webserver auf HTTPS umgestellt werden. Allerdings ist nicht klar, ob hiermit tatsächlich eine rechtlich durch das ULD durchsetzbare Pflicht gemeint ist oder ob es sich eher um eine Empfehlung handelt.

158 Vgl. *Djeffal,* MMR 2015, 716, 721; vgl. außerdem für Gesundheitsdaten: BayLDA, Tätigkeitsbericht 2015/2016, S. 99.

159 Vgl. etwa BSI, Diskussionspapier, S. 6.

160 BayLDA, Tätigkeitsbericht 2015/2016, S. 99.

161 BT-Drs. 13/7385, 23. Allerdings ist ohnehin fraglich, ob dieser Hinweis auf das Fernmeldegeheimnis überhaupt sinnvoll ist. Das Teledienste-/-medienrecht regelt schließlich die Diensteebene und gerade nicht die Transportebene. Das Fernmeldegeheimnis betrifft aber (ganz primär) die Transportebene (und wird durch § 88 TKG einfachgesetzlich abgesichert).

162 In diesem Sinne wohl grundsätzlich (wenn auch ohne Anbindung an das TMG) LDI Berlin, Jahresbericht 2014, S. 26.

163 *Hullen/Roggenkamp,* in: Plath, § 13 TMG. I. d. S. auch *Conrad,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 215; *Moos,* in: Taeger/Gabel. § 13 Rn. 40.

Protocol Secure zu erreichen.[164] Schließlich würde es zu Wertungswidersprüchen führen, wenn nach § 13 Abs. 4 Nr. 3 TMG grundsätzlich eine Datenverschlüsselung für öffentlich zugängliche WWW-Seiten erforderlich wäre, während eine solche im Bereich des allgemeinen Datenschutzrechts nicht einmal für den Schutz besonders sensibler personenbezogener Daten verpflichtend vorgesehen ist.[165]

Geht man davon aus, dass § 13 Abs. 4 Nr. 3 TMG lediglich eine allgemeine Pflicht zur Absicherung gegen eine Kenntnisnahme Dritter vorsieht, so stellt sich erneut die Frage, wie eine solche umgesetzt werden kann. Eine Verschlüsselung von Daten wäre jedenfalls eine geeignete Maßnahme.[166] Erneut gilt insoweit, dass der Gesetzgeber zwar nicht ausdrücklich eine Verschlüsselungspflicht vorschreibt, die Verschlüsselung von Daten aber eine geeignete Maßnahme ist, um der allgemeinen gesetzlichen Schutzplicht nachzukommen.

4.5.1.7 § 8a BSIG (IT-Sicherheitsgesetz)

Schließlich sind nach § 8a Abs. 1 BSIG die Betreiber kritischer Infrastrukturen verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden."

§ 8a BSIG verpflichtet ebenfalls nicht ausdrücklich zur Verschlüsselung von Daten. Aber auch in diesem Kontext kann eine Datenverschlüsselung eine geeignete Maßnahme sein. Da der Schutz kritischer Infrastrukturen außerhalb des Fokus dieser auf kleine und mittlere Unternehmen ausgerichteten Studie liegt, sollen die entsprechenden Fragestellungen hier nicht weiter vertieft werden.

4.5.1.8 Zusammenfassung

Verschiedene (primär oder auch) datenschutzrechtliche Vorschriften schreiben einen Schutz personenbezogener Daten (bzw. kritischer Infrastrukturen) vor. Diese Vorschriften erwähnen den Einsatz von Verschlüsselungstechniken als eine *mögliche* Maßnahme. Durch die jeweils prominente Hervorhebung von Verschlüsselungstechniken macht der Gesetzgeber deutlich, dass solche Maßnahmen *besonderes* geeignet sind, die jeweiligen Schutzziele zu erreichen. Verpflichtend ist der Einsatz grundsätzlich nicht. Allerdings kann es Einzelfälle geben, in denen die gesetzlich vorgegebenen Schutzziele allein durch den Einsatz von Verschlüsselungsverfahren erreicht werden können – etwa beim Versand personenbezogener Daten über ein ungesichertes Netzwerk. In diesen Fällen besteht eine Pflicht zur Verschlüsselung. Diese folgt allerdings nicht aus der gesetzlichen Erwähnung von Verschlüsselung, sondern aus der allgemeinen Pflicht, Schutzmaßnahmen zu ergreifen. Kann ein Schutzziel nur durch *eine* Maßnahme (z. B eine Verschlüsselung) erreicht werden, muss diese auch ergriffen werden.

164 Allerdings wäre insoweit auch in Rechnung zu stellen, dass der Absatz 7 erst 2015 eingefügt worden ist.

165 *Bergt,* CR 2014, 726, 729.

166 Colorandi causa ist anzumerken, dass *Conrad,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 216, als geeignete Maßnahme nicht etwa die Datenverschlüsselung nennt, sondern den Einsatz eines Virenschutzprogramms.

Grundsätzlich steht es den Unternehmen frei, auf Verschlüsselungsverfahren zurückzugreifen oder auch nicht. Kommt es allerdings zu einem Sicherheitsvorfall und Daten waren nicht verschlüsselt, wird sich nur schwer begründen lassen, warum das Unternehmen diesen nicht zu vertreten hat.[167] Das Unternehmen müsste sich dann nämlich nicht nur vorwerfen lassen, eine möglicherweise naheliegende Schutzmaßnahme nicht ergriffen zu haben. Vielmehr dürfte der Vorwurf (grob) fahrlässigen Verhaltens relativ leicht zu begründen sein, weil eine sogar vom Gesetzgeber empfohlene Schutzmaßnahme nicht ergriffen wurde.

Wenn es zu einem Sicherheitsvorfall gekommen ist und ([sensible] personenbezogen) Daten waren – entgegen der gesetzgeberischen Empfehlung – nicht verschlüsselt und sind hierdurch Dritten zugänglich geworden, werden deshalb bußgeldrechtliche Sanktionen sowie Schadensersatzansprüche sehr naheliegend sein.

Schon allein mit Blick auf solche Folgen sollte ein unternehmerisches Eigeninteresse bestehen, die entsprechenden Daten zu verschlüsseln, um im Schadensfall nicht auch noch mit rechtlichen Sanktionen konfrontiert zu sein.

4.5.2 Benachrichtigungs- und Meldepflichten

4.5.2.1 § 42a BDSG

Nach § 42a BDSG besteht eine Informationspflicht bei einer unrechtmäßigen Kenntniserlangung Dritter von personenbezogenen Daten.

Hiernach müssen die zuständigen Aufsichtsbehörden und die Betroffenen[168] informiert werden, wenn (im Gesetz näher benannte)[169] besonders sensible personenbezogene Daten unrechtmäßig an Dritte übermittelt wurden oder sie Dritten auf sonstige Weise zur Kenntnis gelangt sind und hierdurch schutzwürdige Interessen schwerwiegend beeinträchtigt werden.[170]

Soweit eine Information aller Betroffenen nur mit unverhältnismäßigem Aufwand möglich wäre, kann auch eine öffentliche Information über Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder eine Maßnahme mit einer vergleichbaren Wirkung erfolgen.[171]

Erfasst werden hiervon insbesondere Fälle, in denen sich Angreifer („Hacker") Zugang zu entsprechenden Daten verschafft haben, aber auch Fälle, in denen etwa Datenträger verloren wurden, Daten ungesichert über das Internet einsehbar waren oder Daten an den falschen Empfänger gesendet wurden.[172] Der Wortlaut der Norm setzt voraus, dass die Daten Dritten zur Kenntnis gelangt sind. Das wird sich

167 Vgl. zu Schadensersatzansprüchen unten, S. 82 (unter 4.6.6).

168 ULD Schleswig-Holstein, Tätigkeitsbericht 2017, S. 49 berichtet von einem Fall, in welchem in eine Gemeinschaftspraxis für Neurologie, Psychiatrie, Psychosomatik und Psychotherapie eingebrochen wurde und Datenträger mit Patientendaten entwendet wurden. Es mussten daraufhin über 40.000 Briefe verschickt werden.

169 § 42a BDSG nennt: „1. besondere Arten personenbezogener Daten (§ 3 Absatz 9), 2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen, 3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder 4. personenbezogene Daten zu Bank- oder Kreditkartenkonten".

170 Die Unbestimmtheit des Tatbestands ist im Gesetzgebungsverfahren kritisiert worden, vgl. *Grentzenberg/Schreibauer/Schuppert,* K&R 2009, 368, 374.

171 § 42a S. 5 BDSG.

172 *Dix,* in: Simitis, § 42a Rn. 8; *Gola/Schomerus,* § 42a Rn. 4; *Herbst,* in: Auernhammer, § 42a Rn. 1.

häufig nicht nachweisen lassen, weil allenfalls bekannt ist, dass ein Einbruch in ein System stattgefunden hat, nicht aber, ob die Angreifer auch tatsächlich alle Daten zur Kenntnis genommen haben. Das datenschutzrechtliche Schrifttum geht deshalb überwiegend davon aus, dass eine Kenntnisnahme nicht sicher feststehen muss, sondern eine hohe Wahrscheinlichkeit hierfür ausreichend ist.[173] Teilweise wird sogar davon ausgegangen, dass im „Zweifelsfall" von einer Kenntnis auszugehen ist.[174]

Kann hingegen ausgeschlossen werden, dass Dritte sich Kenntnis vom Inhalt erbeuteter oder auch gefundener Daten verschaffen können, greift auch die Informationspflicht nicht.[175] Das ist insbesondere der Fall, wenn Daten verschlüsselt waren[176] und sichergestellt ist, dass der Schlüssel nicht kompromittiert wurde[177].

Welche Anforderungen an eine Verschlüsselung zu stellen sind, lässt sich der Norm nicht unmittelbar entnehmen. In der datenschutzrechtlichen Literatur finden sich Formulierungen wie „hinreichend verschlüsselt",[178] „hinreichend sichere[...] Verschlüsselung",[179] „wirksame Verschlüsselung",[180] „(hinreichend wirksam) verschlüsselte[...] Form"[181] oder „dem Stand der Technik entsprechend stark verschlüsselt"[182]. Stellt man auf den Zweck der Norm ab, wonach die Aufsichtsbehörden und die Betroffenen darüber informiert werden sollen, dass Dritte (potentiell) Kenntnis von besonders sensiblen Daten erlangt haben, dann kann es nicht darauf ankommen, dass Daten *irgendwie* verschlüsselt waren. Vielmehr kann eine Kenntnis nur ausgeschlossen werden, wenn sichergestellt ist, dass Dritte die Daten auch tatsächlich nicht entschlüsseln können. Dabei dürfte es auf die Besonderheiten des jeweiligen Sachverhalts ankommen.[183] Jedenfalls wenn Dritte zielgerichtet Zugriff auf Daten genommen haben, muss regelmäßig davon ausgegangen werden, dass auch ein gesteigertes Interesse daran bestehen wird, die Daten zu entschlüsseln. Deshalb dürften schwache oder gar gebrochene Verschlüsselungsverfahren nicht ausreichend sein, um eine Kenntnisnahme auszuschließen. Das wird auch dann gelten, wenn solche Verfahren noch verbreitet sind. Letztlich spricht deshalb vieles dafür, dass auf den jeweiligen Stand der Technik abzustellen ist.[184]

Allerdings kommt es nicht nur darauf an, dass ein sicheres Verschlüsselungsverfahren eingesetzt wird, dieses muss selbstverständlich auch so genutzt werden, dass

173 *Dix,* in: Simitis, § 42a Rn. 8; *Gola/Schomerus,* § 42a Rn. 4; *Herbst,* in: Auernhammer, § 42a Rn. 18. Anderer Ansicht aber *Grentzenberg/Schreibauer/Schuppert,* K&R 2009, 368, 374.

174 *Hullen,* in: Plath, § 42 Rn. 7 – diese Sicht steht jedoch in einem gewissen Spannungsverhältnis zu den unmittelbar vorhergehenden Ausführungen, wonach „tatsächliche Anhaltspunkte auf eine hohe Wahrscheinlichkeit" schließen lassen müssen.

175 BayLDA, Tätigkeitsbericht 2015/2016, S. 136, geht davon aus, dass eine Meldung [nur] erfolgen muss, wenn Daten nicht ausreichend kryptographisch gesichert waren.

176 *Dix,* in: Simitis, § 42a Rn. 8; *Gabel*, in: Taeger/Gabel, § 42a Rn. 17; *Gola/Schomerus,* § 42a Rn. 4; *Herbst,* in: Auernhammer, § 42a Rn. 17; *Hullen,* in: Plath, § 42 Rn. 7. Kritisch *Grentzenberg/Schreibauer/Schuppert,* K&R 2009, 368, 374. Allgemein zum Personenbezug verschlüsselter Daten für Dritte, die nicht über den Schlüssel verfügen, *Stiemerling/Hartung,* CR 2012, 60, 67.

177 Hierauf weist auch *Marschall,* DuD 2015, 183, 189 im Kontext der Datenschutz-Grundverordnung hin.

178 *Dix,* in: Simitis, § 42a Rn. 8.

179 *Gabel,* in: Taeger/Gabel, § 42a Rn. 17.

180 *Gola/Schomerus,* § 42a Rn. 4.

181 *Herbst,* in: Auernhammer, § 42a Rn. 17.

182 *Hullen,* in: Plath, § 42 Rn. 7; ebenso *Franck,* ZD 2016, 324, 325.

183 Vgl. insoweit auch Arbeitskreise Technik und Medien, Orientierungshilfe – Cloud Computing, S. 12 f.

184 Vgl. zu diesem Maßstab bereits oben (unter 4.3).

das hohe Schutzniveau eines sicheren Verschlüsselungsverfahrens nicht durch eine falsche Bedienung ausgehöhlt wird. So bietet selbst eine Verschlüsselung mit AES 256 kaum Schutz, wenn etwa durch Bequemlichkeit ein zu kurzes Passwort verwendet wird. Bei der Vollverschlüsselung von Laptops ist weiter zu berücksichtigen, dass der Schutz nur wirksam ist, wenn der Computer heruntergefahren wurde.[185]

Eine (richtig eingesetzte) Verschlüsselung von Daten nach dem Stand der Technik führt also dazu, dass in Fällen, in denen beispielsweise (Hacker-) Angriffe stattgefunden haben, Datenträger verloren wurden oder versehentlich (öffentlich) zugänglich waren, keine Information an die Aufsichtsbehörde, die Betroffenen oder gar die Öffentlichkeit erfolgen muss. § 42a BDSG schreibt insoweit zwar keine Verschlüsselung von personenbezogenen Daten vor; werden Daten aber wirksam verschlüsselt, dann führt ein Verlust derart verschlüsselter Daten dazu, dass weder gegenüber der (datenschutzrechtlichen) Aufsichtsbehörde noch der Öffentlichkeit eingestanden werden muss, dass es zu einem Sicherheitsvorfall gekommen ist.[186] Insoweit ist die typische Konstellation einer Obliegenheit gegeben. Es besteht zwar keine Pflicht zur Verschlüsselung, eine Verschlüsselung bringt aber einen rechtlichen – und vor allem tatsächlichen – Vorteil. Insoweit geht von § 42a BDSG jedenfalls ein wirtschaftlicher Anreiz aus, Datensicherheitsmaßnahmen zu ergreifen, weil sich meldepflichtige Datenpannen praktisch immer wirtschaftlich nachteilig auf ein Unternehmen auswirken werden.[187] Dabei dürften die Kosten für die Information nach am geringsten wiegen. Viel gewichtiger wird der Reputationsschaden sein, den ein Unternehmen hinzunehmen hat, wenn es ggf. gar öffentlich darüber informieren muss, sensible personenbezogen Daten nicht ordnungsgemäß geschützt zu haben. Ein Teil des datenschutzrechtlichen Schrifttums geht davon aus, dass ein solcher indirekter Anreiz, Maßnahmen zur Verhinderung meldepflichtiger Ereignisse zu ergreifen, durchaus vom Gesetzgeber intendiert war.[188]

Verstöße gegen § 42a BDSG – also ein Unterlassen der Meldung an die Aufsichtsbehörde und die Betroffenen (bzw. die Öffentlichkeit) – sind nach § 43 Abs. 2 Nr. 7 BDSG bußgeldbewehrt.

§ 42a BDSG enthält somit eine Verschlüsselungsobliegenheit. Grundsätzlich verpflichtet die Norm bei Hacker-Angriffen, dem Verlust von Datenträgern etc. zu einer Meldung an die Aufsichtsbehörden, die Betroffenen bzw. auch die Öffentlichkeit, wenn besonders sensible personenbezogene Daten betroffen sind. Hiermit einhergehen werden regelmäßig wirtschaftliche Verluste und insbesondere Reputationsschäden. Sind die Daten hingegen mit einem dem Stand der Technik entsprechenden Verschlüsselungsverfahren gesichert (und ist der Schlüssel nicht kom-

185 LDI Berlin, Jahresbericht 2012, S. 154 berichtet von einem Fall, in welchem ein Laptop mit ärztlichen Stellungnahmen aus dem PKW entwendet wurde. Das Gerät verfügte zwar über eine Festplattenverschlüsselung, das verwendete Passwort bestand allerdings nur aus acht Zeichen.

186 Meldepflichten können sich aber aus anderen Rechtsgrundlagen ergeben. Für Betreiber kritischer Infrastrukturen wäre insoweit insbesondere § 8b Abs. 4 BSIG relevant.

187 *Herbst,* in: Auernhammer, § 42 Rn. 2.

188 *Gola/Schomerus,* § 42a Rn. 1; *Hullen,* in: Plath, § 42 Rn. 2. Allerdings finden sich in den Gesetzesmaterialien (insb. BT-Drs. 16/12011 u. 16/13657) keine Hinweise auf eine solche ausdrückliche Absicht des Gesetzgebers.

promittiert), können Angreifer und sonstige Dritte keinen Zugriff auf die abhandengekommenen Daten nehmen. Es muss deshalb auch keine Meldung (nach dem BDSG)[189] erfolgen.

4.5.2.2 Art. 33, 34 Datenschutz-Grundverordnung

In der Datenschutz-Grundverordnung sind in den Art. 33 und 34 mit § 42a BDSG vergleichbare Meldepflichten vorgesehen.

Nach Art. 33 Abs. 1 Datenschutz-Grundverordnung muss bei jeder Verletzung des Schutzes personenbezogener Daten eine Meldung an die zuständige Aufsichtsbehörde erfolgen. Die Norm ist allerdings deutlich weiter gefasst als § 42a BDSG.[190] Anders als nach dem BDSG ist die Vorschrift nämlich nicht auf besonders sensible personenbezogene Daten beschränkt, sondern es werden alle Formen von Datenpannen und Datenlecks erfasst, die personenbezogene Daten betreffen.[191] Außerdem sieht die Datenschutz-Grundverordnung vor, dass die Meldung binnen 72 Stunden erfolgen und jede Verzögerung begründet werden muss.[192]

Die Meldung darf unterbleiben, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt."[193] Insoweit ist fraglich, ob eine Meldung unterbleiben darf, wenn Daten (sicher) verschlüsselt waren. Hiergegen könnte sprechen, dass Art. 34 Abs. 3 Datenschutz-Grundverordnung eine ausdrückliche Regelung für den Fall enthält, dass Daten durch geeignete technische Schutzmaßnahmen – „etwa durch Verschlüsselung" – gesichert waren. In diesem Fall brauchen die betroffenen Personen nicht benachrichtigt zu werden. Eine vergleichbare ausdrückliche Regelung in Bezug auf verschlüsselte Daten fehlt hinsichtlich der Meldung an die Aufsichtsbehörde. Das könnte unter systematischen Gesichtspunkten dagegen sprechen, dass eine Meldung an die Aufsichtsbehörde grundsätzlich unterbleiben kann, wenn Daten (sicher) verschlüsselt waren. Allerdings würde ein solches (systematisches) Verständnis ausblenden, dass nach dem Stand der Technik verschlüsselte Daten für Dritte schlicht unbrauchbar sind (solange der Schlüssel nicht ebenfalls kompromittiert wurde). Selbst wenn solche Daten Dritten zugänglich werden, können diese hiermit nichts anfangen. Folglich bestehen dann auch keine Risiken für die Rechte der betroffenen Personen. Es spricht somit – vor allem unter teleologischen Gesichtspunkten – vieles dafür, dass im Falle verschlüsselter Daten auch keine Meldung an die Aufsichtsbehörden erfolgen muss.[194]

Art. 34 Datenschutz-Grundverordnung sieht eine Benachrichtigung an die Betroffenen vor. Eine solche muss allerdings nur erfolgen, wenn „ein hohes Risiko

189 Meldepflichten können sich aber aus anderen Rechtsgrundlagen ergeben. Für Betreiber kritischer Infrastrukturen wäre insoweit insbesondere § 8b Abs. 4 BSIG relevant.

190 So auch *Grages,* in: Plath, Art. 33 DSGVO Rn. 1.

191 *Marschall,* DuD 2015, 183, 184.

192 Art. 33 Abs. 1 S. 1 u. 2. Datenschutz-Grundverordnung.

193 Art. 33 Abs. 1 S. 1 a. E. Datenschutz-Grundverordnung.

194 Zu eng dürfte es allerdings sein, wenn *Marschall,* DuD 2015, 183, 189 darauf abstellt, dass dies (also die Befreiung von der Pflicht zur Mitteilung an die Aufsichtsbehörde) „(nur)" der Fall ist, wenn die Daten verschlüsselt waren.

für die persönlichen Rechte und Freiheiten" der Betroffenen besteht.[195] Erwägungsgrund 85 Datenschutz-Grundverordnung zählt als mögliche Risiken auf: „Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile". Anders als nach Art. 33 Abs. 1 Datenschutz-Grundverordnung (Meldung an die Aufsichtsbehörde) muss also nicht bei jeder (relevanten) Datenpanne oder jedem Datenleck eine Information an die Betroffenen erfolgen. Allerdings ist die Norm auch nicht wie § 42a BDSG auf besonders sensible Daten beschränkt.

Art. 34 Abs. 3 lit. a) Datenschutz-Grundverordnung sieht vor, dass die Benachrichtigung (an die betroffenen Personen) unterbleiben kann, wenn der Verantwortliche technische Sicherheitsvorkehrungen getroffen hat. Die Verschlüsselung wird in diesem Kontext ausdrücklich genannt.

Die Datenschutz-Grundverordnung konkretisiert nicht weiter, welche Anforderungen an eine Verschlüsselung zu stellen sind. Die Vorschrift knüpft aber an Art. 4 Abs. 3 E-Datenschutzrichtlinie 2002/58/EG an.[196] Zu dieser Richtlinie hat die Kommission die Verordnung (EU) Nr. 611/2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten erlassen. Dort ist geregelt, dass keine Benachrichtigung erfolgen muss, wenn die Daten für Dritte „unverständlich sind". Das ist nach der Verordnung der Fall, wenn die Daten „auf sichere Weise mit einem Standardalgorithmus verschlüsselt worden sind, der zur Entschlüsselung verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zur Entschlüsselung verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann, oder ... sie durch ihren mit einer kryptografischen verschlüsselten Standard-Hash-Funktion berechneten Hash-Wert ersetzt worden sind, der zum Daten-Hashing verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt ist und der zum Daten-Hashing verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann."[197] Die Verordnung sieht weiter vor, dass die Kommission eine vorläufige Auflistung geeigneter technischer Schutzmaßnahmen veröffentlichen kann.[198]

Verschlüsselungsverfahren sind hiernach jedenfalls dann als geeignet anzusehen, wenn die Kommission sie in eine entsprechende Auflistung aufgenommen hat. Ansonsten muss das Verschlüsselungsverfahren so ausgestaltet sein, dass der Schlüssel mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann. Es muss – mit anderen Worten – dem Stand der Technik entsprechen. Dass nicht jedes Verschlüsselungs- (oder Hash-) Verfahren ausreichend ist, wird zudem durch

195 Art. 34 Abs. 1 Datenschutz-Grundverordnung.

196 In diesem Sinne auch *Marschall,* DuD 2015, 183, 183.

197 Art. 4 Abs. 2 lit. a) und b) Verordnung (EU) Nr. 611/2013.

198 Art. 4 Abs. 3 Verordnung (EU) Nr. 611/2013.

Erwägungsgrund 17 Verordnung (EU) Nr. 611/2013 klargestellt. Hiernach soll allein „die Anwendung von Verschlüsselung oder Streuspeicherung (Hashing) ... nicht als ausreichend" dafür angesehen werden, dass der Betreiber seinen Schutzpflichten nachgekommen ist.

Verstöße gegen die Meldepflichten können nach Art. 83 Abs. 4 lit. a) Datenschutz-Grundverordnung mit Geldbußen bis zu 10.000.000 € oder 2 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden.

4.5.2.3 § 109a TKG

§ 109a TKG enthält für den Bereich des Telekommunikationsrechts eine § 42a BDSG vergleichbare Regelung für Anbieter öffentlich zugänglicher Telekommunikationsdienste.

Hiernach muss eine Verletzung des Schutzes personenbezogener Daten[199] unverzüglich an die Bundesnetzagentur und die BfDI gemeldet werden. Anders als nach § 42a BDSG ist die Meldepflicht nicht auf besonders sensible personenbezogene Daten beschränkt.[200]

Ist anzunehmen, dass es zu schwerwiegenden Beeinträchtigungen der Betroffenen kommt, müssen diese ebenfalls informiert werden.

Die Benachrichtigung der Betroffenen kann unterbleiben, wenn in einem Sicherheitskonzept nachgewiesen wurde, dass die Daten durch geeignete technische Vorkehrungen gesichert waren. Dabei wird die „Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens" ausdrücklich als Beispiel genannt.

Schließlich sieht § 109a Abs. 1 S. 4 TKG eine Rückausnahme vor. Hiernach kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten in jedem Fall zu einer Benachrichtigung der Betroffenen verpflichten. Waren Daten mit einem dem Stand der Technik entsprechenden Verschlüsselungsverfahren gesichert (und wurde der Schlüssel nicht kompromittiert), dürften solche Auswirkungen allerdings ausgeschlossen werden können.

In der Literatur wird teilweise angenommen, es komme für die Informationspflicht allein darauf an, ob ein Sicherheitskonzept nachgewiesen wurde, nicht aber darauf, ob es auch im Einzelfall angewandt wurde.[201] Eine solche Sicht ist zunächst nur schwer mit dem intendierten Zweck der Regelung in Einklang zu bringen, die

199 Die „Verletzung des Schutzes personenbezogener Daten" wird in § 3 Nr. 30a TKG als „eine Verletzung der Datensicherheit, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden sowie der unrechtmäßige Zugang zu diesen" legaldefiniert.

200 *Jenny,* in: Plath, § 109a TKG Rn. 7; vgl. auch, *Mozek,* in: Säcker, § 109a Rn. 2.

201 *Graulich,* in: Arndt/Fetzer, § 109a Rn. 17, 19.

Betroffenen auf drohende Risiken hinzuweisen,[202] wenn sie betreffende personenbezogene Daten abhandengekommen sind.[203] Insoweit kann es allein darauf ankommen, ob die Daten im Einzelfall – etwa durch Verschlüsselung – gesichert waren[204] und nicht darauf, ob der Diensteanbieter eine solche Sicherung zwar vorgesehen, aber nicht umgesetzt hat. Letztlich kommt es hierauf aber im hiesigen Rahmen nicht entscheidend an, weil die Bundesnetzagentur in einer dieser Konstellationen nach § 109a Abs. 1 S. 4 TKG eine Benachrichtigung anordnen könnte.[205]

Auch in Bezug auf die Meldepflichten nach dem TKG ist damit keine Verschlüsselung von Gesetzes wegen vorgeschrieben. Die (wirksame) Implementierung von Verschlüsselungssystemen führt aber dazu, dass Benachrichtigungspflichten an die Betroffenen – und damit potentiell erhebliche Reputationsschäden – vermieden werden können.

Verstöße gegen die Meldepflichten sind nach § 149 Abs. 1 Nr. 21b TKG bußgeldbewehrt.

4.5.2.4 § 15a TMG

§ 15a TMG enthält eine Rechtsfolgenverweisung auf § 42a BDSG. Die Informationspflicht wird ausgelöst, wenn der Diensteanbieter feststellt, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers drohen.

Es wird insoweit auf die Ausführungen zu § 42a BDSG verwiesen.[206]

Anders als bei § 42a BDSG und § 109a TKG ist ein Verstoß gegen § 15a TMG nicht bußgeldbewehrt. In der Literatur wird angenommen, dass es sich hierbei um ein gesetzgeberisches Versehen handelt.[207]

4.5.2.5 Zusammenfassung

Verschiedene (primär datenschutz-) rechtliche Regeln sehen eine Meldepflicht für datensicherheitsrelevante Vorfälle vor. Erfasst werden hiervon insbesondere Fälle, in denen es Hackern gelingt, Daten zu entwenden, in denen Datenträger verloren werden oder in denen Daten versehentlich an den falschen Empfänger versandt wurden.

Neben einer Meldepflicht an die zuständigen Aufsichtsbehörden sehen die Vorschriften auch eine Information der Betroffenen vor. Das kann im schlimmsten Fall

202 Vgl. zum Regelungszweck *Eckhardt,* in: Beck'scher TKG-Kommentar, § 109a Rn. 7.

203 Kritisch zu Recht *Eckhardt*, in: Beck'scher TKG-Kommentar, § 109a Rn. 18, 29.

204 So auch *Jenny*, in: Plath, § 109a TKG Rn. 10.

205 Richtigerweise ist davon auszugehen, dass nach § 109a Abs. 1 S. 3 TKG auch dann eine Benachrichtigung erfolgen muss, wenn das Sicherheitskonzept zwar geeignete technische Vorkehrungen vorsieht, solche aber nicht erfolgt sind. Der TK-Diensteanbieter muss dann allerdings in jedem Fall zunächst einschätzen, ob das Sicherheitskonzept angesichts des spezifischen Angriffs wirksam war oder nicht. Insoweit kann es zu Einschätzungsdifferenzen zwischen dem TK-Diensteanbieter und der Bundesnetzagentur kommen. So verstanden, würde § 109a Abs. 1 S. 4 TKG der Bundesnetzagentur ein Ermessen eröffnen, eine „Fehleinschätzung" des TK-Diensteanbieters zu korrigieren, in diesem Sinne auch *Jenny,* in: Plath, § 109a TKG Rn. 11 u. *Mozek,* in: Säcker, § 109a Rn. 13.

206 Vgl. oben, S. 54 ff. (unter 4.5.2.1).

207 *Hullen/Roggenkamp,* in: Plath, § 15a TMG Rn. 9.

den gesamten Kundenstamm betreffen. Das betroffene Unternehmen muss also ggf. gegenüber all seinen Kunden eingestehen, ggf. sehr sensible Daten nicht ordnungsgemäß geschützt zu haben. In der Literatur wird darauf hingewiesen, dass es hierdurch zu messbaren Effekten auf den Börsenkurs von Unternehmen kommen kann.[208] Gerade bei kleinen und mittleren Unternehmen dürften die möglichen Folgen besonders gravierend sein, wenn ein möglicherweise kleiner, aber sensibler Kundenkreis das Vertrauen in ein Unternehmen verloren hat.[209]

Die Meldung an die Betroffenen (und teilweise auch an die datenschutzrechtlich zuständige Aufsichtsbehörde) kann jeweils unterbleiben, wenn ausgeschlossen werden kann, dass Dritte mit den Daten etwas anfangen können, weil diese (dem Stand der Technik entsprechend) verschlüsselt waren.

Gerade mit Blick auf die massiven Gefahren, Opfer eines (ggf. nicht einmal gezielten) Hacker-Angriffs zu werden, bei welchem personenbezogene Daten entwendet werden, und auf den hiermit einhergehenden Reputationsschaden, wenn sämtliche Kunden hierüber informiert werden müssen, sollte ein massives wirtschaftliches und unternehmerisches Eigeninteresse bestehen, Verschlüsselungsverfahren einzusetzen.

4.5.3 Urheberrecht

Werke einer bestimmten Schöpfungshöhe genießen grundsätzlich urheberrechtlichen Schutz. Hierfür kommt es nicht darauf an, ob sie durch eine Schutzmaßnahme wie eine Verschlüsselung gesichert sind. Allerdings enthält § 95a UrhG eine Regelung, wonach wirksame technische Maßnahmen zum Schutz eines Werkes nicht umgangen werden dürfen.[210] Hierdurch wird insbesondere das Recht auf „Privatkopie" nach § 53 Abs. 1 UrhG beschränkt. Rechteinhaber können also durch eine Verschlüsselung einen gesteigerten urheberrechtlichen Schutz erreichen und erhalten insbesondere einen erweiterten rechtlichen Schutz gegen andernfalls legale Vervielfältigungshandlungen. Technische Schutzmaßnahmen gelten u. a. als wirksam, soweit durch sie die Nutzung eines geschützten Werkes von dem Rechteinhaber durch einen Schutzmechanismus wie Verschlüsselung unter Kontrolle gehalten wird.[211]

Welche konkreten Anforderungen an eine derartige Verschlüsselung zu stellen sind, ist in der Literatur umstritten. Teilweise wird auf den gegenwärtigen Stand der Technik abgestellt,[212] teilweise wird darauf abgestellt, ob die Umgehung einem Durchschnittsnutzer möglich ist[213]. Einigkeit besteht jedoch, dass der Umstand, dass ein Schutzmechanismus tatsächlich umgangen werden kann, nicht die Wirksamkeit i. S. d. § 95a UrhG in Frage stellt. Andernfalls wäre das Umgehungsverbot nämlich nicht erforderlich.[214] Die Rechtsprechung hat beispielsweise das Real-Time

208 *Hornung,* NJW 2010, 1841, 1842.

209 Vgl. zu existenzgefährdenden Risiken im Kontext schlecht abgesicherter WWW-Seiten *Lurz/Scheben/Dolle,* BB 2015, 2755, 2761.

210 § 95a Abs. 1 UrhG.

211 § 95a Abs. 2 S. 2 UrhG.

212 *Schmidl,* in: Büscher/Dittmer/Schiwy, § 95a UrhG Rn. 8.

213 LG Hamburg, Urt. v. 29.11.2013 – Az. 310 O 144/13, Rn. 34 (juris); *Spindler,* in: Spindler/Schuster, § 95a UrhG Rn. 11.

214 BT-Drs. 15/38, 26.

Messaging Protocol (RTMPE) zum Schutz von Videostreams als wirksamen Schutz angesehen,[215] obwohl der Schlüssel bei diesem Verfahren mit einfachen Mitteln bestimmt werden kann[216].

Für eine wirksame Verschlüsselung nach § 95a UrhG kommt es demnach nicht darauf an, ob auszuschließen ist, dass Dritte die Daten entschlüsseln können. Es kommt auch nicht darauf an, ob ggf. ein geheimer Schlüssel kompromittiert wurde. Vielmehr ist darauf abzustellen, ob der Schutz durch Verschlüsselung gegenüber einem Durchschnittsnutzer (der sich keiner speziellen Hilfsmittel bedient) wirksam ist.

Setzt der urheberrechtlich Berechtigte einen solchen Schutz ein – etwa bei CDs, DVDs, Blu-ray-Discs, eBooks, Videostreams etc. –, so darf ein solcher Schutz nicht umgangen werden. Verstöße gegen dieses Verbot sind unter den Voraussetzungen des § 108b UrhG strafbewehrt. § 95a UrhG beschränkt insoweit das Recht auf „Privatkopie" nach § 53 Abs. 1 UrhG.

4.5.4 Schutz von Betriebs- und Geschäftsgeheimnissen

Fraglich ist weiter, ob insbesondere aus lauterkeitsrechtlichen Vorschriften eine Verschlüsselungsobliegenheit abgeleitet werden kann. Eine solche könnte insbesondere aus den Regeln über den Schutz von Betriebs- und Geschäftsgeheimnissen[217] folgen.

4.5.4.1 § 17 UWG

Im deutschen Recht erfolgt ein (mittelbarer) Schutz von Betriebs- und Geschäftsgeheimnissen vor allem durch § 17 UWG. Hierbei handelt es sich um eine Strafvorschrift, die den Verrat von Betriebs- und Geschäftsgeheimnissen pönalisiert.

Erfasst wird hiervon zunächst die Mitteilung von Betriebs- und Geschäftsgeheimnissen durch eine im Unternehmen beschäftigte Person an Dritte (aus Eigennutz oder in Schädigungsabsicht).[218]

Betriebsfremde können den Tatbestand erfüllen, wenn sie sich ein Betriebs- und Geschäftsgeheimnis etwa durch Anwendung technischer Mittel verschaffen.[219]

Der Begriff des Betriebs- und Geschäftsgeheimnisses ist im UWG nicht legaldefiniert. Rechtsprechung und Literatur verstehen hierunter „alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge …, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat."[220]

215 LG Hamburg, Urt. v. 29.11.2013 – Az. 310 O 144/13, Rn. 34 (juris).

216 Vgl. hierzu *Heinemeyer/Kreitlow,* MMR 2013, 623, 625 f.

217 Die Terminologie ist uneinheitlich. Geschäftsgeheimnisse sollen sich auf den kaufmännischen Geschäftsbetrieb beziehen, Betriebsgeheimnisse auf den technischen Betriebsablauf. Teilweise wird auch von Unternehmens- oder Wirtschaftsgeheimnissen gesprochen. Vgl. *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 4a; *Lehmler,* in: Büscher/Dittmer/Schiwy, § 17 UWG Rn. 9.

218 § 17 Abs. 1 UWG.

219 § 17 Abs. 2 Nr. 1 lit. a) UWG.

220 BVerfG, Beschl. v. 14.3.2006 – Az. 1 BvR 2087/03, 1 BvR 2111/03, Rn. 87; BGH, Urt. v. 9.12.2015 – Az. IV ZR 272/15, Rn. 14; *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 4; *Lehmler,* in: Büscher/Dittmer/Schiwy, § 17 UWG Rn. 9.

Voraussetzung für das Vorliegen eines Betriebs- und Geschäftsgeheimnisses ist also (nur), dass die Tatsachen

1. nicht offenkundig sind,

2. nur einem begrenzten Personenkreis zugänglich sind und

3. der Rechtsträger an der Nichtverbreitung ein berechtigtes Interesse hat.

Offenkundigkeit ist hiernach gegeben, wenn Informationen allgemein bekannt sind, weil sie etwa in allgemein zugänglichen Medien veröffentlicht wurden.[221]

Offenkundigkeit ist hingegen nicht gegeben, wenn die Informationen nur einem begrenzten Personenkreis zugänglich sind. Das gilt insbesondere, wenn dieser Personenkreis vertraglich oder gesetzlich zur Verschwiegenheit verpflichtet ist. Erfasst werden hiervon vor allem Betriebsangehörige, aber auch Dritte, denen eine Geheimhaltungspflicht auferlegt wurde. Eine Geheimhaltungspflicht muss dabei nicht ausdrücklich vereinbart werden, sondern kann sich auch aus den Umständen ergeben.[222]

Für das Vorliegen von Betriebs- und Geschäftsgeheimnissen ist es also zunächst unerheblich, ob ein ggf. auch sehr großer Personenkreis hiervon Kenntnis hat, solange dieser Personenkreis zur Geheimhaltung verpflichtet ist. Ein Betriebs- und Geschäftsgeheimnis kann also insbesondere auch dann vorliegen, wenn es *allen* Beschäftigten bekannt ist. Betriebs- und Geschäftsgeheimnisse müssen folglich nicht vor den eigenen Beschäftigten geheim gehalten werden. Es ist deshalb für eine Qualifikation als Betriebs- und Geschäftsgeheimnis auch nicht erforderlich, dass betriebsintern besondere Vorkehrungen getroffen werden, damit etwa nur bestimmte Personen Kenntnis von einem bestimmten Wissen erlangen können.

Einer Offenkundigkeit steht es gleich, wenn das betreffende Wissen leicht zugänglich ist. Dem Begriff des Geheimnisses ist insoweit immanent, dass es nicht ohne weiteres verfügbar ist.[223] Das ist aber nur der Fall, wenn Dritte sich das Wissen ohne größere Schwierigkeiten mit lauteren Mitteln verschaffen können.[224] Ein Überwinden einer *besonderen* Zugangssicherung wird dabei von § 17 UWG nicht gefordert.[225]

Auch gegenüber Dritten ist es somit ausreichend, dass Sicherungen bestehen, die einen Zugang auf einfachem Wege ausschließen. Muss sich der Dritte erst unlauterer Mittel bedienen, um auf die betreffende Information zuzugreifen, führt dies nicht zu deren Offenkundigkeit. Insoweit ist es für den Begriff des Betriebs- und Geschäftsgeheimnisses nicht erforderlich, dass *besondere* Schutzmaßnahmen, wie etwa eine Datenverschlüsselung, ergriffen wurden.

Schließlich muss ein Geheimhaltungsinteresse bestehen. Das wird für alle Informationen angenommen, die für die Wettbewerbsfähigkeit eines Unternehmens relevant sind.[226] Der Unternehmensinhaber muss ferner einen Geheimhaltungswillen

221 *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 7; *Lehmler,* in: Büscher/Dittmer/Schiwy, § 17 UWG Rn. 11.

222 *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 7a.

223 *Koch,* RTkom 2001, 217, 223; ders. Angriff und Verteidigung, S. 223.

224 *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 8; *Lehmler,* in: Büscher/Dittmer/Schiwy, § 17 UWG Rn. 11.

225 *Koch,* RTkom 2001, 217, 223; ders. Angriff und Verteidigung, S. 223.

226 *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 9.

haben. Dieser muss nicht ausdrücklich erklärt werden, aber erkennbar sein und kann sich aus der Natur der geheim gehaltenen Tatsache ergeben. Ein allgemeiner Geheimhaltungswille genügt.[227] Erforderlich ist nicht, dass dieser durch *besondere* Maßnahmen dokumentiert wird.

Für eine Qualifizierung als Betriebs- und Geschäftsgeheimnis ist es folglich nicht erforderlich, dass Daten verschlüsselt werden.

Allerdings ist das Vorliegen eines Betriebs- und Geschäftsgeheimnisses zu verneinen, wenn Informationen für Dritte ohne weiteres zugänglich sind. Das kann etwa der Fall sein, wenn geheimhaltungsbedürftige Informationen längere Zeit versehentlich über die WWW-Seite eines Unternehmens öffentlich einsehbar sind. Insofern hat die Qualifikation als Geheimnis eine objektive Seite, wonach der Geschäftsherr wenigstens basale Sicherungsmaßnahmen zu treffen hat. Die rein subjektive Schutzbedürftigkeit einer Information ist deshalb nicht ausreichend.

Zudem mag es in der Praxis zu Beweisproblemen kommen, wenn Informationen einem großen Personenkreis zugänglich waren und keine ausdrückliche Geheimhaltungspflicht auferlegt wurde. Ein Geheimhaltungswille wird in solchen Fällen schwer nachzuweisen sein.[228] Solche praktischen Schwierigkeiten können umgangen werden, wenn geheimhaltungsbedürftige Informationen im Unternehmen verschlüsselt sind.

4.5.4.2 Richtlinie (EU) 2016/943

Auf Unionsebene wird der Geheim- und Know-how-Schutz durch die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung adressiert.

Die Richtlinie gilt – wie alle Richtlinien – nicht unmittelbar, sondern muss von den Mitgliedstaaten umgesetzt werden.[229]

Sie enthält in Art. 2 Nr. 1 eine Legaldefinition des Begriffs „Geschäftsgeheimnis". Hierunter versteht die Richtlinie „Informationen, die alle nachstehenden Kriterien erfüllen:

a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind;

b) sie sind von kommerziellem Wert, weil sie geheim sind;

c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt".

227 *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 10.

228 Allerdings wird regelmäßig der Verletze beweisen müssen, dass kein Geheimhaltungswille vorlag, *Köhler,* in: Köhler/Bornkamm, § 17 UWG Rn. 10.

229 Art. 288 UAbs. 3 AEUV.

Diese Legaldefinition unterscheidet sich dem Wortlaut nach von der Definition, die von Rechtsprechung und Schrifttum für den Begriff „Betriebs- und Geschäftsgeheimnis" nach deutschem Recht gefunden wurden. Zum einen fehlen subjektive Elemente („Geheimhaltungswille"), zum anderen wird deutlich stärker das Erfordernis von „angemessenen Geheimhaltungsmaßnahmen" betont.

Im vorliegenden Kontext ist insbesondere Letzteres von Interesse, schließlich könnte eine Umsetzung der Richtlinie bedeuten, dass zukünftig wesentlich strengere Anforderungen erfüllt sein müssen, damit Betriebs- und Geschäftsgeheimnissen einen gesetzlichen Schutz erfahren. Im Schrifttum ist sogar diskutiert worden, insoweit auf die Anforderungen nach der Anlage 1 zu § 9 BDSG zurückzugreifen.[230] Andere Stimmen gehen davon aus, dass zukünftig der Geheimnisträger wird nachweisen müssen, dass er in adäquater Weise technische, physische und vertragliche Maßnahmen zur Geheimhaltung getroffen hat.[231]

Würde sich ein solches Verständnis durchsetzen, müssten zukünftig deutlich umfangreichere Maßnahmen getroffen werden, um Geschäftsgeheimnisse zu sichern. Es wären dann sogar Konstellationen denkbar, in denen der Umstand, dass Informationen nicht verschlüsselt waren, dazu führt, dass ein gesetzlicher Schutz verweigert wird. Das gilt insbesondere, wenn man unterstellt, dass der Geheimnisträger den vollen Beweis dafür erbringen müsste, geeignete Schutzmaßnahmen ergriffen zu haben. In einer solchen Situation ist es durchaus vorstellbar, dass ein Gericht aus dem Verzicht auf eine Verschlüsselung – als sehr naheliegende Schutzmaßnahme – schließen könnte, dass kein Geschäftsgeheimnis gegeben war. Bei einem solchen Verständnis würde also ein deutlicher Druck bestehen, aktive Sicherungsmaßnahmen, wie die Verschlüsselung von Daten, zu ergreifen, um entsprechende Prozessrisiken abzuwehren.

Ohne dies hier zu vertiefen, sind aber Zweifel an einer solchen Sicht angezeigt. Zunächst ist daran zu erinnern, dass es sich um eine Richtlinie handelt, die einer Umsetzung in das nationale Recht bedarf. Anders als etwa die Datenschutz-Grundverordnung gilt die Richtlinie also nicht unmittelbar, so dass auch die Begriffsbestimmung nicht unmittelbar gilt. Zudem ist fraglich, ob mit der Richtlinie eine Vollharmonisierung des Geheimschutzes beabsichtigt wird, der die Mitgliedstaaten zwingt, ggf. ihr bisheriges Schutzniveau deutlich *abzusenken.* Hiergegen spricht, dass die Erwägungsgründe die Bedeutung von Geschäftsgeheimnissen gerade für kleine und mittlere Unternehmen ausdrücklich betonen.[232] Zudem stellt die Richtlinie darauf ab, dass in Mitgliedstaaten, in denen ein vergleichsweise geringes Schutzniveau für Geschäftsgeheimnisse besteht, ein höheres Geschäftsrisiko gegeben ist, weil die Gefahr größer ist, dass Geschäftsgeheimnisse auf unrechtmäßige Weise erworben werden. *Hierin* wird eine Gefahr für den Binnenmarkt gesehen.[233] Vor diesem Hintergrund wäre es widersinnig anzunehmen, die Richtlinie könnte darauf abzielen, dass Mitgliedstaaten ein vergleichsweise *hohes* Schutzniveau *absenken* müssten und damit Unternehmen einem *höheren* Risiko eines Verlusts von Geschäftsgeheimnissen ausgesetzt wären. Ein solches Verständnis würde der

230 Vgl. zu solchen Ansätzen *Koós,* MMR 2016, 224, 225.

231 *Hauck,* NJW 2016, 2218, 2220.

232 Erwägungsgründe 2 ff. Richtlinie (EU) 2016/943.

233 Erwägungsgrund 9 Richtlinie (EU) 2016/943.

Union unterstellen, dass sie versuchte, den Binnenmarkt zu stärken, indem sie dafür sorgte, dass in Ländern mit einem *hohen* Schutzniveau Geschäftsgeheimnisse *leichter unrechtmäßig* erworben werden könnten und Betriebs- und Industriespionage *vereinfacht* würde. So gesehen spricht einiges dafür, dass über die Richtlinie eine Mindestharmonisierung erstrebt wird, nicht aber eine Vollharmonisierung, die zu einer Absenkung des Schutzniveaus führt. Auch Art. 1 Abs. 1 UAbs. 2 der Richtlinie streitet für ein solches Verständnis. Letztlich kann dies an dieser Stelle nicht vertieft werden und es bleibt abzuwarten, ob der deutsche Gesetzgeber Handlungsbedarf sehen wird und welcher dies ggf. sein wird.

Selbst wenn man annähme, dass eine Vollharmonisierung erstrebt wird, ist es aber keineswegs zwingend anzunehmen, dass dies zu einer Verschärfung der Anforderungen an den Geheimschutz führen wird. Schon nach der bislang in Deutschland geltenden Rechtslage ist schließlich erforderlich, dass das Geheimnis nicht allgemein bekannt ist. Dem ist immanent, dass *gewisse* Schutzmaßnahmen ergriffen werden. Insoweit scheint es durchaus vertretbar, dass unter „angemessenen Geheimhaltungsmaßnahmen" auch eine – ggf. sogar schlüssige – Verpflichtung von Mitarbeitern und Dritten auf einen Geheimschutz verstanden wird.

Unabhängig davon, wie letztlich die Richtlinie in das deutsche Recht umgesetzt werden wird, ist die Verschlüsselung von Betriebs- und Geschäftsgeheimnissen aber in jeden Fall eine sinnvolle Schutzmaßnahme, welche die rechtliche Zweifelsfrage, ob tatsächlich ein Betriebs- und Geschäftsgeheimnis vorliegt, in aller Regel beseitigen wird.

4.5.4.3 § 202a StGB

Der Vollständigkeit halber ist darauf hinzuweisen, dass § 202a StGB das Ausspähen von Daten unter Strafe stelle. Erfasst werden hiervon aber nur Daten, die gegen unberechtigten Zugang besonders gesichert sind. Das heißt, der Betroffene muss durch Sicherungsmaßnahmen ein Geheimhaltungsinteresse manifestieren.[234] Grundsätzlich stellt die Verschlüsselung von Daten eine entsprechende Zugangssicherung dar. Allerdings werden an die Zugangssicherung keine besonders hohen Anforderungen gestellt.[235] Solange überhaupt eine wirksame Zugangssicherung vorhanden ist, kann der Tatbestand erfüllt werden.

§ 202a StGB erfasst insoweit zwar grundsätzlich Daten, die (nicht völlig trivial) verschlüsselt sind. Eine Verschlüsselung wird vom Tatbestand aber nicht vorausgesetzt.

Insoweit gilt jedoch, dass die Verschlüsselung von Daten – und zwar unabhängig davon, ob es sich um Geheimnisse handelt – dazu führt, dass diese von § 202a StGB erfasst werden und insoweit ein (mittelbarer) strafrechtlicher Schutz erfolgt.

234 *Koch,* Angriff und Verteidigung, S. 47 f.

235 *Koch,* Angriff und Verteidigung, S. 101 f.

4.5.4.4 Vergaberecht

Eine weitere höchst mittelbare Regelung in Bezug auf eine Verschlüsselung von Daten durch kleine und mittlere Unternehmen findet sich in § 11 Abs. 3 Nr. 3 Vergabeverordnung und § 9 Abs. 3 Nr. 3 Konzessionsvergabeverordnung. Hiernach müssen öffentliche Auftraggeber (bzw. Konzessionsgeber) allen interessierten Unternehmen die notwendigen Informationen zur Teilnahme an einem Vergabeverfahren zur Verfügung stellen. Diese Daten umfassen u. a. Angaben zu verwendeten Verschlüsselungsverfahren. Die Begründung zum Gesetzentwurf macht hierzu keine Ausführungen und verweist lediglich auf die praktisch wortgleichen Vorgaben im Unionsrecht.[236] Die Vorschrift dürfte jedoch dahingehend zu verstehen sein, dass öffentliche Auftraggeber grundsätzlich im Rahmen von Vergabeverfahren eine verschlüsselte Datenübermittlung vorsehen dürfen.[237] Unternehmen, die sich an einem Vergabeverfahren beteiligen wollen, wären dann faktisch gezwungen, entsprechende Verschlüsselungsverfahren zu nutzen.

4.5.4.5 Zusammenfassung

In verschiedenen primär datenschutzrechtlichen Regelungen wird eine Verschlüsselung ausdrücklich als Maßnahme zur Sicherung von Daten genannt. Den Regelungen kommt allerdings letztlich nur die Bedeutung einer gesetzgeberischen Empfehlung zu. Eine (ggf. immense) Bedeutung kann das allerdings bei der Bestimmung von Sorgfaltspflichten haben.

Zudem sieht das allgemeine und sektorspezifische Datenschutzrecht Informationspflichten bei Sicherheitsvorfällen vor. Diese können dazu führen, dass ggf. sogar öffentlich über entsprechende Vorfälle informiert werden muss. Hiermit wird praktisch immer ein (ggf. erheblicher) Reputationsschaden verbunden sein. Die Informationspflicht (gegenüber den Betroffenen) besteht hingegen nicht, wenn die Daten (sicher) verschlüsselt waren.

Eine Verschlüsselung von Daten wird zudem regelmäßig eine wirksame technische Schutzmaßnahme i. S. d. § 95a UrhG darstellen, die nicht umgangen werden darf.

Schließlich kann die Verschlüsselung von Daten eine Maßnahme darstellen, die ein Geheimhaltungsinteresse im Sinne des Lauterkeitsrechts verdeutlicht, so dass im Zweifel von einem Betriebs- und Geschäftsgeheimnis ausgegangen werden kann, das strafrechtlich vor unberechtigter Verbreitung geschützt ist.

236 BT-Drs. 18/7318, 155, 215 unter Bezugnahme auf die Richtlinien 2014/24/EU und 2014/25/EU.

237 Wobei allerdings weiter zu beachten wäre, dass diese nach § 11 Abs. 1 S. 1 Vergabeverordnung „allgemein verfügbar, nichtdiskriminierend und mit allgemein verbreiteten Geräten und Programmen der Informations- und Kommunikationstechnologie kompatibel sein“ müssen. § 12 Vergabeverordnung sieht Ausnahmen von diesem Grundsatz vor.

4.6 Generalklauseln

Unter einer Generalklausel wird in der Rechtswissenschaft eine Vorschrift verstanden, deren Tatbestand sehr weit gefasst ist und verschiedene Verhaltenspflichten (oder Eingriffsbefugnisse) umfasst. Im Folgenden werden dementsprechend Vorschriften betrachtet, die keinen Bezug auf IT-Sicherheit oder sogar eine Verschlüsselung nehmen, aus denen im Wege der Auslegung aber möglicherweise eine Verpflichtung zur Verschlüsselung entnommen werden kann.

4.6.1 § 93 AktG (Sorgfaltsmaßstab)

Nach § 93 Abs. 1 S. 1 AktG[238] haben „Vorstandsmitglieder ... bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden." Hierunter ist die Sorgfalt zu verstehen, die ein Geschäftsleiter in einem Unternehmen von bestimmter Art und Größe anzuwenden hat.[239] Als Maßstabsfigur soll dabei auf einen professionellen und hauptamtlichen Geschäftsleiter abgestellt werden, der die für seine Tätigkeit erforderlichen Fähigkeiten und Kenntnisse besitzt.[240]

Diese Definitionen zeigen das Grundproblem von Generalklauseln auf: Der genaue Inhalt des Sorgfaltsmaßstabes lässt sich abstrakt praktisch nicht bestimmen. Vielmehr verdeutlichen die Definitionen, dass es auf eine Vielzahl von Einzelaspekten ankommt, aus denen sich dann eine bestimmte Verhaltenspflicht ergeben kann, aber nicht muss.[241] Zu berücksichtigen sind insoweit zunächst Gesichtspunkte wie die Art des Unternehmens, seine Größe, die wirtschaftliche und finanzielle Lage, die Bedeutung einer Maßnahme für das Unternehmen etc.[242]

Dabei dürfte im Grundsatz anerkannt sein, dass Fragen der IT-Sicherheit zum Pflichtenkreis der Geschäftsleitung zählen.[243]

Der Sorgfaltsmaßstab in Bezug auf Verschlüsselung kann aber bei einem international tätigen Hightech-Unternehmen, welches einer Bedrohung durch Industriespionage ausgesetzt ist, anders aussehen als bei einem kunsthandwerklichen Betrieb, in dem lediglich das Rechnungswesen EDV-gestützt abgewickelt wird.

Anerkannt ist auch, dass der Sorgfaltsmaßstab normativ zu bestimmen ist. Es wird also auf einen in gewisser Weise idealisierten – eben „ordentlichen und gewissenhaften" – Geschäftsleiter abgestellt. Das heißt, es ist für den Sorgfaltsmaßstab unerheblich, ob in einer Branche eine abweichende tatsächliche Übung existiert bzw. bestimmte Nachlässigkeiten weit verbreitet oder gar üblich sind.[244] Auch kommt

238 § 93 AktG entspricht weitgehend § 43 GmbHG. Es wird deshalb in den Fußnoten auch aus der GmbH-rechtlichen Literatur zitiert. Siehe hierzu auch unter 4.6.3 und Fn. 317.

239 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 25.

240 *Fleischer,* in: Spindler/Stilz, § 93 Rn. 41.

241 Vgl. zu diesem Problem auch *Fleischer,* in: Spindler/Stilz, § 93 Rn. 41: „Die Sorgfaltsanforderungen ... variierten von Situation zu Situation".

242 *Zöllner/Noack,* in: Baumbach/Hueck, § 43 Rn. 9; *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn. 58; *Oetker,* in: Henssler/Strohn, § 43 GmbHG Rn. 14; *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 25; *Fleischer,* in: Spindler/Stilz, § 93 Rn. 41.

243 *Zöllner/Noack,* in: Baumbach/Hueck, § 43 Rn. 19; *Conrad/Huppertz,* in: Auer-Reinsdorf/Conrad, § 33 Rn. 2, 4; *von Holleben/Menz,* CR 2010, 63, 63; *Röhrborn/Lang,* BB, 2015, 2357, 2357; *Trappehl/Schmidl,* NZA 2009, 985, 985. Vgl. auch *Schuppenhauer,* GoDV-Handbuch, B Rn. 60, wonach die Geschäftsführung für eine interne Revision zu sorgen hat, über welche ggf. IT-Sicherheitsprobleme identifiziert werden können.

244 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 25; *Fleischer,* in: Spindler/Stilz, § 93 Rn. 41.

es nicht darauf an, wie bestimmte Fragen in vergleichbaren Unternehmen gehandhabt werden.[245]

Insoweit kann jedenfalls abstrakt festgestellt werden, dass der Umstand, dass in einer Branche auch sensible Kommunikation unverschlüsselt erfolgt oder unternehmenskritische Information unverschlüsselt gespeichert werden, nicht zu einer grundsätzlichen Entlastung der jeweiligen Geschäftsleiter führt.

4.6.1.1 Legalitätspflicht

Die wohl herrschende Ansicht in der Rechtswissenschaft geht davon aus, dass die Geschäftsleitung eine Einhaltung der gesetzlichen Vorgaben sicherstellen muss.[246] Das gilt auch dann, wenn sich Gesetzesverstöße als „nützlich" erweisen würden und das Unternehmen hiervon profitieren würde.[247]

Soweit von Gesetzes wegen der Schutz bestimmter – insbesondere personenbezogener – Daten vorgeschrieben ist, muss diesen Vorgaben selbst dann nachgekommen werden, wenn ein Verzicht hierauf wirtschaftlich sinnvoller wäre. Deshalb dürfen solche Kosten auch nicht in eine Kosten-Nutzen-Betrachtung eingestellt werden, bei der nicht die Gefahren für die jeweiligen (personenbezogenen) Daten eingestellt werden, sondern ein Entdeckungsrisiko durch die jeweilige Aufsichtsbehörde.

4.6.1.2 (Allgemeine) Betriebswirtschaftliche Standards

Teilweise wird bei der Bestimmung des Sorgfaltsmaßstabs auf in der Betriebswirtschaftslehre anerkannte „Grundsätze ordnungsgemäßer Unternehmensführung" abgestellt.[248] Teilweise wird demgegenüber bestritten, dass es solche Grundsätze überhaupt gibt.[249]

Dabei ist grundsätzlich in Rechnung zu stellen, dass all diese Standards gerade keine Rechtsqualität besitzen und betriebswirtschaftliche Praktikabilitätserwägungen im Vordergrund stehen.[250] Das heißt, es besteht weder eine rechtliche Verpflichtung, einem bestimmten Managementsystem zu folgen, noch kann die Befolgung eines solchen (Compliance-) Systems von der Haftung nach § 93 Abs. 2 AktG befreien.[251] Teilweise wird davon ausgegangen, dass der Befolgung eines Management- oder Compliance-Systems und der Zertifizierung einer Organisation – etwa nach einem ISO-Standard – nicht einmal eine Vermutungswirkung hinsichtlich der Einhaltung des Sorgfaltsmaßstabs des § 93 Abs. 1 S. 1 AktG zukommt.[252] Allerdings dürften die entsprechenden Regeln grundsätzlich heranzuziehen sein, um den Verhaltensmaßstab der gesetzlichen Generalklausel zu konkretisieren.[253]

245 *Dauner-Lieb,* in: Henssler/Strohn, § 93 AktG Rn. 7.

246 *Haas/Ziemons,* in: Michalski, § 43 Rn. 49a.

247 *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn. 61; *Koch,* in: Hüffer/Koch, § 43 Rn. 6; *Haas/Ziemons,* in: Michalski, § 43 Rn. 51; *Fleischer,* in: Spindler/Stilz, § 93 Rn. 36.

248 Für das GmbHG, *Zöllner/Noack,* in: Baumbach/Hueck, § 43 Rn. 19.

249 Vgl. die Nachweise bei *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 30 Fn. 115.

250 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 30.

251 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 30.

252 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 30.

253 *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn. 52, 96; *Haas/Ziemons,* in: Michalski, § 43 Rn. 47, 65.

Unabhängig davon ist aber ohnehin zu bedenken, dass solche *allgemeinen* Grundsätze kaum in der Lage sein werden, zu bestimmen, welche konkreten Daten in welcher konkreten Situation wie zu verschlüsseln sind.

4.6.1.3 Deutscher Corporate Governance Kodex

Eine gewisse Sonderstellung bei den betriebswirtschaftlichen Standards nimmt der Deutsche Corporate Governance Kodex ein. Dieser Verhaltenskodex wird von der Regierungskommission Deutscher Corporate Governance Kodex formuliert. In der Regierungskommission sind Vertreter von Unternehmen, der Wissenschaft, der Gewerkschaften sowie Wirtschaftsprüfer vertreten.[254] Die Mitglieder werden im Einvernehmen mit dem Bundeskanzleramt vom Bundesministerium für Justiz und für den Verbraucherschutz berufen.[255]

Der Kodex richtet sich in erster Linie an börsennotierte Unternehmen. Nicht kapitalmarktorientierten Gesellschaften wird die Beachtung des Kodex allerdings empfohlen.[256]

Der Deutsche Corporate Governance Kodex ist *nicht* verbindlich.[257] Börsennotierte Unternehmen müssen allerdings nach § 161 Abs. 1 AktG einmal jährlich erklären, ob sie ihm entsprechen. Wird der Deutsche Corporate Governance Kodex nicht befolgt, muss begründet werden, welche Empfehlungen nicht angewendet werden.[258] Hieraus wird teilweise geschlossen, dass dem Kodex „implizite Bedeutung für die Konkretisierung der Sorgfaltspflichten" zukommt. Teilweise wird der Umstand, dass § 161 AktG ausdrücklich ein Abweichen von dem Kodex zulässt, aber auch als Hinweis auf die Unverbindlichkeit des Kodex gewertet.[259]

Letztlich kann diese Frage aber offenbleiben. Soweit es um Fragen der IT-Sicherheit im Allgemeinen und der Verschlüsselung von Daten im Speziellen geht, enthält der Deutsche Corporate Governance Kodex nämlich ohnehin keine konkreten Verpflichtungen. Vielmehr finden sich dort erneut *Generalklauseln*, die im Sinne einer Verschlüsselung verstanden werden *können*.

So heißt es etwa in Ziffer 3.5:[260]

„Gute Unternehmensführung setzt eine offene Diskussion zwischen Vorstand und Aufsichtsrat sowie in Vorstand und Aufsichtsrat voraus. Die umfassende Wahrung der Vertraulichkeit ist dafür von entscheidender Bedeutung."

Ein Mittel zur Wahrung der Vertraulichkeit *kann* die Verschlüsselung der (E-Mail-) Kommunikation zwischen Vorstand und Aufsichtsrat sein. Es sind aber zahlreiche andere Mittel denkbar.

254 Ziffer 1.2 UAbs. 1 Geschäftsordnung der Regierungskommission Deutscher Corporate Governance Kodex.

255 Ziffer 1.2 UAbs. 2 Geschäftsordnung der Regierungskommission Deutscher Corporate Governance Kodex.

256 Ziffer 1 UAbs. 12 Geschäftsordnung der Regierungskommission Deutscher Corporate Governance Kodex.

257 Vgl. BT-Drs. 14/8769, 21: „Da der Kodex, soweit er nicht ohnedies zwingendes Recht nur wiedergibt, *unverbindliche* Verhaltensempfehlungen enthält, ist er wesentlich flexibler als eine zwingende und damit möglicherweise in vielen Fällen zu rigide gesetzliche Lösung." (Hervorhebung nur hier).

258 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 31.

259 *Fleischer,* in: Spindler/Stilz, § 93 Rn. 46.

260 Sämtliche Zitate beziehen sich auf die zum Zeitpunkt der Abfassung aktuelle Fassung vom 5. Mai 2015.

Nach Ziffer 4.1.4 sorgt der Vorstand „für ein angemessenes Risikomanagement ... im Unternehmen". Hierunter *kann* die Sicherung unternehmenskritischer Informationen durch Verschlüsselung fallen.

4.6.1.4 Grundsätze ordnungsgemäßer/ordnungsmäßiger Datenverarbeitung

Soweit in der juristischen Kommentarliteratur[261] im Zusammenhang mit dem allgemeinen Sorgfaltsmaßstab für Geschäftsleiter auf Sonderprobleme der IT-Sicherheit eingegangen wird, finden sich allenfalls Verweise auf die „Grundsätze ordnungsgemäßer Datenverarbeitung".[262] Soweit ersichtlich, ist bislang eine Konkretisierung dieses Begriffs durch die Rechtsprechung nicht erfolgt.[263] In der Literatur werden hierunter die Grundsätze verstanden, nach denen eine Datenverarbeitung zu organisieren, dokumentieren und überwachen ist.[264] Diese Grundsätze sollen sich aus dem Gesetz „legitimieren".[265] Der Schwerpunkt liegt insoweit zunächst auf Vorschriften über die ordnungsgemäße Führung von (Geschäfts-) Büchern und ihre EDV-technische Umsetzung.[266]

Allerdings dürfte insoweit dem Umstand, dass der Gesetzgeber in verschiedenen Vorschriften eine Verschlüsselung ausdrücklich empfiehlt, besondere Bedeutung zukommen. Wenn schon der Gesetzgeber eine konkrete Maßnahme zur Sicherung von Daten für sinnvoll erklärt, wird es im konkreten Einzelfall jedenfalls mit einigem Argumentationsaufwand verbunden sein, zu begründen, weshalb die entsprechende Maßnahme nicht umgesetzt wurde.

Eine weitere Konkretisierung dieser allgemeinen Grundsätze ordnungsgemäßer Datenverarbeitung kann sich aus behördlichen Vorgaben und Empfehlungen ergeben. Relevant sind insofern insbesondere die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" sowie der „IT-Grundschutz-Katalog".

Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[267] sind eine Verwaltungsanweisung des Bundesministeriums an die obersten Finanzbehörden der Länder. Die GoBD stellen also weder eine gesetzliche Regelung dar, noch richten sie sich an Unternehmen. Faktische Bedeutung erlangen

261 Soweit diese vorliegend ausgewertet wurde.

262 *Zöllner/Noack,* in: Baumbach/Hueck, § 43 Rn. 19.

263 Die Fachdatenbank juris liefert fünf Treffer in der Rechtsprechung (Stand 17.11.2016). Keine der gefundenen Entscheidungen setzt sich inhaltlich mit dem Begriff auseinander.

264 *Schuppenhauer,* A Rn. 76.

265 *Schuppenhauer,* a. a. O.

266 Das gilt jedenfalls für *Schuppenhauer,* X. Das Handbuch – vom Verlag als „Der De-facto-Standard der DV-Prüfung" bezeichnet – behandelt die Verschlüsselung von Daten allenfalls am Rande. Im Stichwortverzeichnis kommen die Begriffe „Verschlüsselung" oder „Kryptographie" überhaupt nicht vor. Das mag allerdings auch darauf zurückzuführen sein, dass die aktuelle 6. Auflage aus dem Jahr 2007 stammt.

267 Sämtliche Zitate beziehen sich auf die bei Abfassung aktuelle Fassung vom 14. November 2014.

die GoBD aber dadurch, dass die Finanzverwaltung diese anwendet und dementsprechend die betroffenen Unternehmen diese praktisch ebenfalls umsetzen müssen, wollen sie keinen Konflikt mit der Finanzverwaltung riskieren.

Die GoBD schreiben keine Verschlüsselung von Daten vor. Sie verbieten eine Datenverschlüsselung aber auch nicht. Allerdings ist beim „Einsatz von Kryptografietechniken ... sicherzustellen, dass die verschlüsselten Unterlagen im DV-System in entschlüsselter Form zur Verfügung stehen."[268]

Dabei ist aber die Zielrichtung der GoBD zu berücksichtigen: Die Regeln sollen der Finanzverwaltung einen möglichst einfachen Zugriff auf digital gespeicherte Finanzdaten ermöglichen. Unter *diesem* Blickwinkel erschwert die Verschlüsselung von Daten den Finanzbehörden einen Zugriff. Die GoBD adressieren also ein Interesse der Finanzverwaltung an einem Zugriff auf Daten und nicht etwa Unternehmens- oder Gemeinwohlinteressen an einem Schutz von Finanzdaten gegen Zugriffe von Dritten. Deshalb ist es in diesem Kontext verständlich, dass nicht etwa eine Verschlüsselung von Daten gefordert oder auch nur empfohlen wird. Die entsprechenden Sicherheitsinteressen stehen schlicht außerhalb des Fokus der GoBD. Andererseits verbieten die GoBD auch nicht die Verschlüsselung, wenn sichergestellt ist, dass die Unterlagen jederzeit entschlüsselt werden können.

Da die Zielrichtung der GoBD nicht auf den Schutz von (Finanz-) Daten gegenüber Dritten gerichtet ist, sondern gerade einen ungehinderten Zugriff der Finanzverwaltung im Blick hat, lässt sich hieraus wenig für die Frage nach einer Verschlüsselung von unternehmenskritischen (und sonstigen) Daten ableiten. Allenfalls ist festzustellen, dass auch die GoBD davon ausgehen, dass ein dem Zugriffsinteresse der Finanzverwaltung tendenziell entgegenstehendes Sicherheitsbedürfnis besteht, welchem durch die Verschlüsselung von Finanzdaten entsprochen werden kann. Diese Interessen erkennen die GoBD ausdrücklich an und schreiben lediglich vor, dass Daten ggf. für die Finanzverwaltung entschlüsselt werden müssen.

IT-Grundschutz-Katalog

Der IT-Grundschutz-Katalog[269] des BSI zielt auf einen angemessenen Schutz aller Informationen einer Institution.[270] Er beschreibt entsprechende Gefahren und beinhaltet u. a. eine Sammlung von IT-Sicherheitsmaßnahmen. Er richtet sich an Behörden und Unternehmen.

Der IT-Grundschutz-Katalog empfiehlt an zahlreichen Stellen den Einsatz von Verschlüsselungsverfahren und beschreibt abstrakte[271] und konkrete Einsatzmöglichkeiten[272] (einschließlich der Nutzung bestimmter Verschlüsselungsprodukte[273]), weist aber auch auf Probleme beim unsachgemäßen Umgang mit Verschlüsselungsprogrammen hin[274].

268 Rn. 134 GoBD.

269 Sämtliche Zitate beziehen sich auf die bei Abfassung aktuelle Fassung mit Stand der 15. Ergänzungslieferung 2016.

270 IT-Grundschutz-Katalog, S. 69.

271 Z. B. M 2.161 „Entwicklung eines Kryptokonzepts".

272 Z. B. M 4.29 „Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme".

273 Z. B. M 4.372 „Einsatz von FileVault unter Mac OS X".

274 Z. B. G 3.109 „Unsachgemäßer Umgang mit FileVault-Verschlüsselung".

Die Bedeutung, die der IT-Grundschutz-Katalog der Verschlüsselung bzw. Kryptographie beimisst, wird allein durch die Häufigkeit entsprechender Bezugnahmen belegt. So kommt der Begriff „Verschlüsselung" (mindestens) 1 228 Mal vor und „krypto" 1 091 Mal.

Kein verpflichtender Charakter

Der IT-Grundschutz-Katalog hat keinen verpflichtenden Charakter.[275] Die Umsetzung der enthaltenen Konzepte und Maßnahmen ist (jedenfalls in Bezug auf Unternehmen) freiwillig. Fraglich ist deshalb, ob eine Nichtberücksichtigung des IT-Grundschutz-Katalogs gleichzeitig auf eine Nichtberücksichtigung der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters schließen lässt. Insoweit ist zunächst in Rechnung zu stellen, dass grundsätzlich keine Verpflichtung des Vorstandes besteht, staatlichen *Empfehlungen* Folge zu leisten.[276] Beschränkt sich der Staat darauf, bestimmte Verhaltensweisen lediglich zu empfehlen, aber gerade nicht hoheitlich vorzuschreiben, so erlangen diese Empfehlungen keinen verpflichtenden Charakter, weil Vorstände aus Sorgfaltsgründen gehalten wären, diese einzuhalten.

Allerdings ist der Sorgfaltsmaßstab der Geschäftsleitung ein normativer. Letztlich wird also ein idealisierter Geschäftsführer betrachtet, der die Interessen seines Unternehmens verfolgt und alle erforderlichen und angemessenen Maßnahmen ergreift, um Schaden von ihm abzuwenden.

IT-Grundschutz-Katalog in der Rechtsprechung

Fraglich ist in diesem Kontext vor allem, welche Bedeutung die Rechtsprechung dem IT-Grundschutz-Katalog beimisst.

Zwar findet sich eine Reihe von Entscheidungen, die auf den IT-Grundschutz-Katalog Bezug nehmen. Diese sind allerdings alle nicht zum Sorgfaltsmaßstab des AktG ergangen. Es lassen sich deshalb allenfalls Tendenzen ausmachen, die Hinweise darauf liefern können, welche Bedeutung die Rechtsprechung dem IT-Grundschutz-Katalog möglicherweise auch im Rahmen der Bestimmung eines Sorgfaltsmaßstabes beimessen würde.

AG Reutlingen, Beschluss vom 5. Dezember 2011 – Az. 5 Gs 363/11, hat ohne weitere Begründung das Unterlassen einer Datensicherung unter Verweis auf „BSI IT-Grundschutz Empfehlungen, M 6.32, G 5.22 etc." als „offensichtlich in grob fahrlässiger Weise" erfolgtes Verhalten gewertet.[277] Hierbei handelt es sich allerdings um ein obiter dictum (die Ausführungen waren für das Urteil also nicht entscheidungserheblich). Das Gericht hatte darüber zu entscheiden, ob von der Finanzverwaltung beschlagnahmte Festplatten herauszugeben waren. In diesem Kontext wollte das Gericht offensichtlich dem Beschuldigten vorhalten, nicht für eine Sicherheitskopie gesorgt zu haben (gleichwohl hat das Gericht eine Herausgabe der Festplatten angeordnet).

---

275 Allerdings sollen einige Datenschutzbehörden davon ausgehen, dass der Grundschutzbaustein „Datenschutz" als verbindlicher Mindeststandard zur Erfüllung von § 9 BDSG anzusehen ist, vgl. *Conrad,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 243.

276 *Fleischer,* in: Spindler/Stilz, § 93 Rn. 45.

277 AG Reutlingen, Beschl. v. 5.12.2011 – Az. 5 Gs 363/11, Rn. 6 (juris).

Demgegenüber ist das *VG Berlin, Urteil vom 24. Mai 2011 – Az. 1 K 133.10,* davon ausgegangen, dass keine Verpflichtung besteht, personenbezogene Daten, die ein Arbeitsvermittler an potentielle Arbeitgeber verschickt, bei der Übermittlung per E-Mail zu verschlüsseln. Dem Fall lag eine Anordnung der datenschutzrechtlichen Aufsichtsbehörde zu Grunde, für eine solche Verschlüsselung zu sorgen. Die Aufsichtsbehörde hatte hierbei ausdrücklich Bezug auf den IT-Grundschutz-Katalog genommen und ausgeführt, dass der Sicherheitsstandard nach Baustein B 5.3 zu bestimmen sei und Maßnahmen nach M 5.108 zu ergreifen seien.[278] Dem ist das Verwaltungsgericht nicht gefolgt. Vielmehr hat es unter Verhältnismäßigkeitsgesichtspunkten darauf abgestellt, dass im vorliegenden Fall nicht für eine E-Mailverschlüsselung zu sorgen sei. Dabei kam es (wohl) entscheidend darauf an, dass die Empfänger der E-Mails in der Lage sein müssten, die E-Mails zu entschlüsseln, wovon nicht auszugehen sei. Zudem hatten die Betroffenen in eine unverschlüsselte Übermittlung eingewilligt.[279]

Das Gericht hatte allerdings die Berufung wegen grundsätzlicher Bedeutung der Rechtssache zugelassen. Während des Berufungsverfahrens hat der Arbeitsvermittler seine Tätigkeit eingestellt, weshalb der Rechtsstreit für erledigt erklärt wurde. Das Oberverwaltungsgericht hat die Verfahrenskosten den Beteiligten jeweils zur Hälfte auferlegt, weil es den Ausgang des Verfahrens für offen gehalten hat.[280]

FG Nürnberg, Beschluss vom 5. August 2014 – Az. 2 V 676/14, und *FG Baden-Württemberg, Urteil vom 23. März 2016 – Az. 7 K 3192/15,* betrafen Verfahren, in denen es um die elektronische Übermittlung von Umsatzsteuervoranmeldungen bzw. Einkommensteuererklärungen ging. Streitig war jeweils die Sicherheit der entsprechenden Verfahren. Die Gerichte haben in diesem Kontext darauf abgestellt, dass die für die Kommunikationsplattformen zuständigen Behörden auf der Basis des IT-Grundschutz-Katalogs zertifiziert seien; dies stelle den „De-Facto-Standard für IT-Sicherheit" dar.[281]

Insgesamt vier Entscheidungen, die Bezug auf den IT-Grundschutz-Katalog nehmen,[282] sind letztlich eine *deutlich* zu kleine Anzahl, um hieraus allgemeine Tendenzen in der Rechtsprechung abzuleiten. Zudem handelt es sich jeweils um Entscheidungen der Eingangsinstanzen.

Versucht man trotz dieser großen Unsicherheiten[283] und unter Berücksichtigung allgemeiner Tendenzen in der Rechtsprechung eine Verallgemeinerung, so lässt sich feststellen, dass die Einhaltung der Grundsätze des IT-Grundschutz-Katalogs und insbesondere eine Zertifizierung hiernach es dem erkennenden Gericht sehr

278 VG Berlin, Urt. v. 24.5.2011 – Az. 1 K 133.10, Rn. 14 (juris).

279 VG Berlin, Urt. v. 24.5.2011 – Az. 1 K 133.10, Rn. 20 (juris).

280 LDI Berlin, Jahresbericht 2013, S. 162.

281 FG Nürnberg, Beschl. v. 5.8.2014 – Az. 2 V 676/14, Rn. 27 (juris); FG Baden-Württemberg, Urt. v. 23.3.2016 – Az. 7 K 3192/15, Rn. 17 (juris).

282 Die Fachdatenbank juris liefert insgesamt 58 Treffer für „Grundschutz" in der Rechtsprechung (Stand 17.11.2016). Hiervon beziehen sich aber viele Entscheidungen auf einen „Basisschutz" oder einen „Bodenschutz". Soweit in den Entscheidungen ein IT-Grundschutz adressiert wird, bezieht sich ein großer Teil auf Verfahren, in denen es um Ausschreibungen ging, die Bezug auf den IT-Grundschutz-Katalog nahmen, ohne dass in der Entscheidung entsprechende Probleme adressiert wurden.

283 Die Studie der Kommission Arbeitsschutz und Normung, Rechtsprechung zu technischen Normen und normenähnlichen Dokumenten hinsichtlich ihrer Bedeutung für Sicherheit und Gesundheitsschutz, S. 58 kommt bei einer Untersuchung der Rechtsprechung zu technischen Normen zu dem Ergebnis, dass „eine Systematik ... für die Geeignetheit" der Heranziehung einer Norm nicht erkennbar sei.

erleichtert, von der Sicherheit entsprechender Verfahren auszugehen. Es spricht deshalb einiges dafür, dass bei Einhaltung der Grundsätze des IT-Grundschutz-Katalogs eine Pflichtverletzung abgelehnt werden würde.

Ebenfalls verallgemeinern lassen dürfte sich der Gedanke, dass der IT-Grundschutz-Katalog nicht in jedem Fall umgesetzt werden muss, sondern es gute Gründe geben kann, hiervon abzuweichen. Relevant dürfte insoweit auch die Überlegung sein, dass eine verschlüsselte Übertragung an sich schützenswerter Informationen daran scheitern kann, dass der Kommunikationspartner nicht in der Lage ist, diese zu entschlüsseln. Letztlich entspricht das diesbezügliche Urteil der Sichtweise der Literatur, wonach unverbindliche Handlungsempfehlungen gerade nicht generell umgesetzt werden müssen.

In einem gewissen Widerspruch zu dieser Rechtsprechung steht hingegen eine Rechtsprechung, wonach eine Nichtberücksichtigung des IT-Grundschutz-Katalogs ein grob fahrlässiges Verhalten nahelegt. Hier mögen die Besonderheiten des Einzelfalls eine Rolle gespielt haben.[284] Allerdings zeigt die Entscheidung eine durchaus relevante Gefahr: Werden Sicherungsmaßnahmen unterlassen und es kommt zu einem Schaden, dann kann der Vorwurf eines pflichtwidrigen Verhaltens ohne großen Argumentationsaufwand darauf gestützt werden, dass entsprechende Handlungsempfehlungen – etwa nach „BSI IT-Grundschutz Empfehlungen, M 6.32, G 5.22 etc." – nicht umgesetzt wurden. Der Umstand, dass bestimmte Verhaltensweisen „amtlich empfohlen" wurden, führt also jedenfalls implizit dazu, dass dem Betroffenen vorgehalten werden kann, er hätte es besser wissen können.

Sonstige IT-Sicherheitsstandards

Für sonstige IT-Sicherheitsstandards[285] gilt letztlich das zum IT-Grundschutz-Katalog Gesagte entsprechend. Diese Standards sind weder verpflichtend, noch kann pauschal gefolgert werden, dass die Einhaltung eines Sicherheitsstandards einer Pflichtverletzung zwingend entgegensteht.[286]

Zusammenfassung

Der Sorgfaltsmaßstab des § 93 Abs. 1 AktG zwingt nicht zur Einhaltung eines bestimmten IT-Sicherheitsstandards. Es sind lediglich allgemein die Grundsätze ordnungsgemäßer Datenverarbeitung einzuhalten. Welche Pflichten hieraus folgen, ist letztlich eine Frage des Einzelfalls und lässt sich nicht abstrakt beantworten.

Grundsätzlich führt die Einhaltung eines IT-Sicherheitsstandards oder die Zertifizierung nach einem solchen Standard nicht dazu, dass eine Pflichtverletzung ausgeschlossen ist. Allerdings dürfte in der gerichtlichen Praxis sehr viel dafürsprechen, dass bei Befolgung eines anerkannten IT-Sicherheitsstandards – insbesondere des IT-Grundschutz-Katalogs – eine Pflichtverletzung verneint würde. In jedem Fall müsste das Gericht nämlich ermitteln, welche Anforderungen in Bezug auf IT-Sicherheit an einen ordentlichen und gewissenhaften Geschäftsleiter zu stellen sind.

284 Der Beschuldigte, der offensichtlich keine Sicherheitskopie gefertigt hatte, war ein „EDV-Berater", wobei sich die Anführungszeichen auch im Urteil finden.

285 Eine Recherche bei Juris hat zu ISO/IEC 27001, ISO/IEC 27002 (bzw. ISO/IEC 17799), CoBIT, Common Criteria, ITIL und ITSEC/CC keine relevanten Treffer in der Rechtsprechung ergeben (Stand 17.11.2016).

286 So auch ausdrücklich *von Holleben/Menz,* CR 2010, 63, 65.

Bei der Ausfüllung dieser Pflichten ist es jedenfalls naheliegend, anerkannte Standards heranzuziehen. Insoweit zeigt die hier analysierte Rechtsprechung – auch wenn diese zahlenmäßig sehr klein ist –, dass bei Befolgung oder Nichtbefolgung des IT-Grundschutz-Katalogs neben einem kurzen Hinweis auf jene Regeln aus gerichtlicher Sicht keine weiteren Ermittlungen oder Ausführungen für erforderlich gehalten wurden (wenn nicht gute Gründe vorlagen, hiervon abzuweichen).

4.6.2 § 91 Abs. 2 AktG (KonTraG)

Nach § 91 Abs. 2 AktG hat der Vorstand „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Die Norm ist durch Art. 1 Nr. 7 des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in das AktG eingeführt worden.

Die Begründung zum Gesetzentwurf ging davon aus, dass entsprechende Pflichten ohnehin bestünden. Sie sollten lediglich „verdeutlicht werden".[287] Die Begründung nennt als gefährdende Entwicklungen „risikobehaftete Geschäfte, Unrichtigkeiten der Rechnungslegung und Verstöße gegen gesetzliche Vorschriften, die sich auf die Vermögens-, Finanz- und Ertragslage der Gesellschaft oder des Konzerns wesentlich auswirken."[288] Verbreitet wird davon ausgegangen, dass nur solche Entwicklungen erfasst werden, die ein Insolvenzrisiko begründen oder wesentlich steigern.[289] Bloß nachteilige Entwicklungen werden nicht adressiert.[290]

Die Vorschrift erfasst somit jedenfalls existenzgefährdende Entwicklungen im Bereich der IT-Sicherheit. In der rechtswissenschaftlichen Literatur wird mitunter aus § 91 Abs. 2 AktG aber auch eine allgemeine Pflicht zur Wahrung der IT-Sicherheit abgeleitet.[291] Ob das angesichts des klar auf „den Fortbestand der Gesellschaft gefährdende Entwicklungen" bezogenen Wortlauts der Vorschrift zutreffend ist, ist durchaus zweifelhaft.[292]

Auf den hiesigen Kontext bezogen kann somit aber festgestellt werden, dass in Unternehmen, deren Fortbestand von der Wahrung bestimmter Geschäfts- und Betriebsgeheimnisse abhängt, eine Pflicht besteht, entsprechende Risiken hierfür zu erkennen und zu überwachen. Dazu kann eine Pflicht gehören, dafür Sorge zu tragen, dass entsprechende Geheimnisse verschlüsselt gespeichert und übermittelt werden, und die Einhaltung entsprechender Verpflichtungen auch zu überwachen. Ein Beispiel hierfür mag die Sicherung von Quellcodes bei Unternehmen sein, die (Closed-Source-) Software entwickeln.[293]

Letztlich kommt es hierauf aber auch nicht an. IT-gestützte Systeme dürften heute in praktisch allen Branchen eine bedeutende (bis unternehmenskritische) Rolle

287 BT-Drs. 13/9712, 15.

288 *Von Holleben/Menz,* CR 2010, 63, 63 f.; *Müller-Michaels,* in: Hölters, § 90 Rn. 6; *Koch,* in: Hüffer/Koch, § 91 Rn. 6; *Trappehl/Schmidl,* NZA 2009, 985, 985 f.

289 BT-Drs. 13/9712, 15.

290 *Dauner-Lieb*, in: Henssler/Strohn, § 91 AktG Rn. 7.

291 *Röhrborn/Lang,* BB 2015, 2357, 2357 f.; wohl auch *von Holleben/Menz,* 2010, 63, 64; *Trappehl/Schmidl,* NZA 2009, 985, 986.

292 Kritisch auch *Conrad/Huppertz,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 32.

293 Vgl. hierzu: *Conrad/Huppertz,* in: Auer-Reinsdorff/Conrad, § 33 Rn. 82.

spielen. Fragen der IT-Sicherheit zählen deshalb grundsätzlich zum Kernbestand eines unternehmensinternen Risikomanagements[294] und gehören unmittelbar zu den Geschäftsleitungsaufgaben[295]. Werden die entsprechenden Aufgaben delegiert – was selbstverständlich möglich ist –, muss jedoch wenigstens eine regelmäßige Kontrolle durch die Geschäftsleitung erfolgen.[296]

4.6.2.1 Unternehmerisches Ermessen

Den Geschäftsleiter trifft keine Erfolgshaftung.[297] Jede unternehmerische Entscheidung birgt schließlich die Gefahr einer Fehleinschätzung und kann sich im Nachhinein als ungünstig herausstellen. Zudem ist unternehmerisches Verhalten praktisch immer durch Unwägbarkeiten gekennzeichnet.[298] Es ist deshalb anerkannt, dass der Geschäftsleitung ein unternehmerisches Ermessen zukommt.[299] Der BGH formuliert insoweit:

„[Eine Schadensersatzpflicht des Vorstandes] kann erst in Betracht kommen, wenn die Grenzen, in denen sich ein von Verantwortungsbewusstsein getragenes, ausschließlich am Unternehmenswohl orientiertes, auf sorgfältiger Ermittlung der Entscheidungsgrundlagen beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, die Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt worden ist oder das Verhalten des Vorstands aus anderen Gründen als pflichtwidrig gelten muss."[300]

Es sind also zwei Ebenen zu unterscheiden: Auf der Ebene der Vorbereitung und Durchführung einer unternehmerischen Entscheidung ist ein strenger – und auch kontrollierbarer – Maßstab anzulegen. Hingegen wird dem Geschäftsleiter bei den hieraus zu ziehenden Schlussfolgerungen ein weites unternehmerisches Ermessen zugebilligt.[301]

Maßgeblich ist immer die Sicht ex ante.[302] Für die Haftung ist es also insoweit grundsätzlich nicht entscheidend, *dass* es zu einem Schadereignis gekommen ist, sondern ob der Geschäftsleiter die Entscheidungsgrundlage sorgfältig ermittelt und hieraus vertretbare Schlüsse gezogen hat. Insoweit bezieht sich der Sorgfaltsmaßstab vor allem darauf, ob im *Vorfeld* einer Entscheidung alle maßgeblichen Informationen berücksichtigt wurden.[303]

Bezogen auf die Verschlüsselung von Daten bedeutet dies, dass der Geschäftsleiter alle für und gegen eine Verschlüsselung sprechende Gesichtspunkte sorgfältig ermitteln muss. Bei den hieraus zu ziehenden Schlüssen kommt ihm dann allerdings ein weites Ermessen zu.

294 *Conrad/Huppertz,* in: Auer-Reinsdorf/Conrad, § 33 Rn. 2.

295 *Conrad/Huppertz,* in: Auer-Reinsdorf/Conrad, § 33 Rn. 4.

296 *Zöllner/Noack,* in: Baumbach/Hueck, § 43 Rn. 19; *Hölters,* in: Hölters, § 93 Rn. 87; *Conrad/Huppertz,* in: Auer-Reinsdorf/Conrad, § 33 Rn. 4.

297 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 5, 26; *Haas/Ziemons,* in: Michalski, § 43 Rn. 66d.

298 *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn. 102.1.

299 Vgl. statt aller: BGH, Urt. v. 21.4.1997 – Az. II ZR 175/95, Rn. 22 (juris); *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn.102 ff.; *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 54.

300 BGH, Urt. v. 21.4.1997 – Az. II ZR 175/95, Rn. 22 (juris).

301 *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43 Rn. 103.

302 *Haas/Ziemons,* in: Michalski, § 43 Rn. 66d.

303 *Haas/Ziemons,* in: Michalski, § 43 Rn. 66d; *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 48.

Das mag folgendes Beispiel veranschaulichen: Müssen sensible Daten für einen Geschäftsabschluss kurzfristig an einen Geschäftspartner übermittelt werden, der seinerseits nicht in der Lage ist, Daten zu entschlüsseln, so wäre in die Entscheidung einzustellen, wie unternehmenskritisch die Daten sind (bzw. ob es sich um besonders sensible personenbezogene Daten handelt etc.), wie groß das Risiko eines Zugriffs durch Dritte ist und wie bedeutsam der Geschäftsabschluss ist. In solcher Situation *kann* es zu verantworten sein, eine unverschlüsselte Übermittlung per E-Mail trotz der hiermit verbundenen Risiken zu veranlassen.[304] Selbst wenn die Daten nun durch den Fehler eines ansonsten zuverlässigen Mitarbeiters an den falschen Empfänger übermittelt würden, läge kein Pflichtverstoß der Geschäftsleitung vor. Die Sicht würde sich allerdings ändern, wenn die Daten unternehmenskritisch wären, mit Industriespionage durch ausländische Geheimdienste gerechnet werden müsste und die Übermittlung von einem öffentlichen WLAN in einem Hotel erfolgte.

4.6.2.2 Tun und Unterlassen

Grundsätzlich kann ein Pflichtverstoß in einem Tun oder einem Unterlassen bestehen.[305] Insbesondere wird die Geschäftsleitung auch eine Sonderverantwortlichkeit treffen, das Unternehmen gegen IT-bezogene Gefahren abzuschirmen,[306] aus der sich somit grundsätzlich die Verantwortung für ein Unterlassen entsprechender Maßnahmen ergibt.

Insoweit kommt es in Bezug auf die Verschlüsselung von Daten nicht darauf an, ob eine ausdrückliche Entscheidung getroffen wird, Daten nicht zu verschlüsseln, oder ob es unterlassen wurde, überhaupt dafür zu sorgen, dass Daten ggf. verschlüsselt werden.

4.6.2.3 Verschulden

Grundsätzlich haften Vorstände schon für leichte Fahrlässigkeit.[307] Fachliche Unkenntnis oder persönliches Unvermögen wirken sich grundsätzlich nicht entlastend aus.[308] Es kommt folglich nicht darauf an, ob ein Geschäftsleiter persönlich für IT-relevante Risiken sensibilisiert ist oder um die Einsatzmöglichkeiten von Verschlüsselungstechniken weiß.

Anerkannt ist schließlich, dass die für Arbeitnehmer entwickelten Haftungserleichterungen nicht auf Geschäftsleiter übertragbar sind.[309]

---

304 Vgl. hierzu – wenn auch unter öffentlich-rechtlichen Gesichtspunkten – VG Berlin, Urt. v. 24.5.2011 – Az. 1 K 133.10, Rn. 20 (juris). Zu eng *Klett/Lee,* CR 2008, 644, 645 die davon ausgehen, dass Betriebs- und Geschäftsgeheimnisse grundsätzlich nur verschlüsselt versendet werden dürfen. Differenzierter *Backu,* ITRB 2003, 251, 252, der davon ausgeht, dass mit „zunehmender Sensibilität ... ein unverschlüsselter Versand nicht mehr zulässig sein" wird.

305 *Haas/Ziemons,* in: Beck'scher Online-Kommentar zum GmbHG, § 43; *Hüffer,* in: Hüffer, § 43 Rn. 53; *Haas/Ziemons,* in: Michalski, § 43 Rn. 174; *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 147.

306 Vgl. grundsätzlich zur Sonderverantwortlichkeit (allerdings in Bezug auf einen „Compliance Officer" in Bezug auf eine Beihilfe zum Betrug), BGH, Urt. v. 17.7.2009 – Az. 5 StR 384/08, Rn. 26 f. (juris). Beachte auch *Conrad/Huppertz*, in: Auer-Reinsdorff/Conrad, § 33 Rn. 142, die darauf hinweisen, dass „Compliance" Teil der Leitungsaufgabe der Geschäftsführung ist und entsprechende Pflichten zunächst diese treffen.

307 *Hölters*, in: Hölters, § 93 Rn. 251; *Dauner-Lieb*, in: Henssler/Strohn, § 93 AktG Rn. 32; *Fleischer*, in: Spindler/Stilz, § 93 Rn. 206.

308 *Hüffer*, in: Hüffer, § 93 Rn. 43; *Fleischer*, in: Spindler/Stilz, § 93 Rn. 205.

309 *Zöllner/Noack*, in: Baumbach/Hueck, § 43 Rn. 6; *Oetker*, in: Henssler/Strohn, § 43 GmbHG Rn. 11; *Hüffer*, in: Hüffer, § 93 Rn. 51.

4.6.2.4 Beweislast

Kommt es zu einem Prozess um eine – angebliche – Pflichtverletzung, so sieht § 93 Abs. 2 S. 2 AktG eine Umkehr der Beweislast zu Lasten des Vorstandes vor. Die Gesellschaft muss hiernach lediglich beweisen, dass ein Verhalten des Vorstandes für ein bestimmtes Schadereignis kausal war.[310] Der Geschäftsleiter muss hingegen beweisen, dass er der Sorgfaltspflicht genügt hat und ihn kein Verschulden trifft. Er muss insbesondere beweisen, dass der Schaden auch dann eingetreten wäre, wenn er sich wie ein ordentlicher Geschäftsmann verhalten hätte.[311] Insoweit wird ein pflichtwidriges Verhalten vermutet.[312]

In der Praxis wird es aber nur dann zu einem Prozess kommen, wenn ein Schaden eingetreten ist. Das wird im hiesigen Kontext vor allem der Fall sein, wenn sensible Daten Dritten zugänglich geworden sind. Die klagende Gesellschaft würde in diesem Fall ihrem Vorstand vorwerfen, nicht für eine Verschlüsselung gesorgt zu haben. Im Zweifel würde sie außerdem darauf verweisen, dass anerkannte IT-Sicherheitsstandards wie insbesondere der IT-Grundschutz-Katalog eine Verschlüsselung solcher Daten vorsehen bzw. sogar das Gesetz eine Verschlüsselung empfohlen hat. Der Vorstand müsste nun beweisen, dass es im konkreten Fall nicht pflichtwidrig war, auf eine entsprechende Verschlüsselung *nicht* hinzuwirken. Er müsste also beweisen, dass auch ein abstrakt-idealer Geschäftsleiter trotz entsprechender (staatlicher oder gesetzgeberischer) Empfehlungen auf eine Verschlüsselung verzichtet hätte. Dieser Beweis dürfte schwer zu erbringen sein, wenn einerseits eine Verschlüsselung von Standards wie dem IT-Grundschutz-Katalog empfohlen wird und andererseits sich gerade das Risiko realisiert hat, welches durch Maßnahmen nach dem IT-Grundschutz-Katalog abgeschirmt werden sollte. Noch schwieriger dürfte der entsprechende Entlastungsbeweis zu führen sein, wenn sogar eine gesetzgeberische „Verschlüsselungs-Empfehlung" ignoriert wurde, wie sie beispielsweise in der Anlage zu § 9 BDSG,[313] in Art. 32 Datenschutz-Grundverordnung, in § 109 TKG oder in § 13 Abs. 7 TMG enthalten ist.

Denkbar sind freilich auch Fälle, in denen Daten verschlüsselt wurden und nun unbrauchbar sind, weil sie nicht mehr entschlüsselt werden können. Insoweit dürfte grundsätzlich eine Pflicht bestehen, Schlüssel zu sichern. Die hiermit einhergehenden Pflichten sind allerdings vergleichbar mit denen zur Fertigung von Sicherheitskopien[314] und sollen deshalb in diesem Kontext nicht weiter vertieft werden.

Der Vorstand wird also praktisch immer mit einer Situation konfrontiert sein, in welcher ein Schadereignis eingetreten ist, welches sich hätte vermeiden lassen, wenn die Empfehlungen des IT-Grundschutz-Katalogs (oder eines anderen anerkannten Grundsatzes ordnungsgemäßer Datenverarbeitung) bzw. des Gesetzgebers befolgt worden wären. Es stünde damit fest, dass letztlich die eingetretene Gefahr – z.B. dass ein Laptop mit vertraulichen Daten aus einem Hotelzimmer ge-

310 *Fleischer*, in: Spindler/Stilz, § 93 Rn. 221.

311 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 185.

312 *Spindler,* in: Münchener Kommentar zum AktG, § 93 Rn. 181.

313 Vgl. hierzu: S. 11 (unter 4.5.1.1).

314 Vgl. hierzu *Schuppenhauer,* A Rn. 730 ff.

stohlen wird – nicht lediglich abstrakt bestanden, sondern sich auch konkret realisiert hat. Auch wenn es letztlich für die *Pflichtverletzung* nur darauf ankommt, wie eine bestimmte Gefahr *abstrakt* einzuordnen ist, so dürfte es rein *praktisch* äußerst schwerfallen, den Beweis dafür zu führen, dass eine Gefahr, die sich tatsächlich realisiert hat, dermaßen fernliegend (oder zumindest bewusst eingehbar) war, dass sie nicht in ein Sicherheitskonzept eingestellt und abgeschirmt werden musste.

Ein solcher Beweis dürfte insbesondere voraussetzen, dass sich der Geschäftsleiter überhaupt mit dem entsprechenden Risiko auseinandergesetzt hat. Es wird deshalb regelmäßig erforderlich sein, dass entsprechende Entscheidungen – insbesondere aufgrund welcher Erwägungen von einer Verschlüsselung abgesehen wurde – dokumentiert werden.[315]

In diesem Kontext ist schließlich nochmals darauf hinzuweisen, dass es bei der Bestimmung des Sorgfaltsmaßstabs nicht darauf ankommt, ob in einer Branche möglicherweise allgemein sorglos mit bestimmten Gefahren umgegangen wird. Ein Geschäftsleiter könnte sich also insbesondere nicht damit entlasten, dass er ausführt, auch in anderen Unternehmen der Branche verzichte man auf Verschlüsselung.

4.6.2.5 Zusammenfassung

Grundsätzlich zählt die IT-Sicherheit zum Pflichtenkreis der Geschäftsleitung. Welche konkreten Maßnahmen hierunter fallen, lässt sich allerdings nicht abstrakt bestimmen. Insbesondere besteht keine *grundsätzliche* Pflicht, anerkannte Standards – wie etwa den IT-Grundschutz-Katalog des BSI – umzusetzen oder gesetzlichen Verschlüsselungsempfehlungen – wie etwa in Art. 32 Datenschutz-Grundverordnung – zu folgen. Allerdings können solche Standards und Empfehlungen durchaus herangezogen werden, um den Sorgfaltsmaßstab eines ordentlichen und gewissenhaften Geschäftsleiters im Einzelfall zu konkretisieren.

Erleidet das Unternehmen einen Schaden, weil etwa unternehmenskritische oder datenschutzrechtlich sensible Daten nicht verschlüsselt waren, muss der Geschäftsleiter beweisen, dass eine Verschlüsselung nicht erforderlich (bzw. unangemessen) gewesen wäre. Dieser Beweis dürfte schwerfallen, wenn Standards wie der IT-Grundschutz-Katalog des BSI oder gesetzliche Verschlüsselungsempfehlungen ignoriert wurden. Gelingen dürfte der Beweis nur, wenn der Geschäftsleiter dokumentiert hat, aus welchen – tragfähigen – Gründen er von einer Verschlüsselung abgesehen hat.

Grundsätzlich kommt es bei der Frage, ob Daten verschlüsselt werden müssen, nicht darauf an, ob kritische Daten in andere vergleichbaren Unternehmen oder gar in der gesamten Branche nicht verschlüsselt werden. Abzustellen ist vielmehr auf einen idealisierten ordentlichen und gewissenhaften Geschäftsleiter, der ggf. auch entgegen einem branchenüblichen „Schlendrian" seine Pflichten erfüllt.

315 *Conrad/Huppertz*, in: Auer-Reinsdorff/Conrad, § 33 Rn. 42.

Bei der empirischen Befragung hat sich gezeigt, dass der ganz überwiegende Teil der befragten Unternehmen die Meinung teilte, dass die Verschlüsselung von Daten heute zu den Grundsätzen einer ordnungsgemäßen Unternehmensführung" zählt.[316]

4.6.3 § 43 GmbHG

§ 43 GmbHG sieht eine § 93 AktG entsprechende Haftung des GmbH-Geschäftsführers vor. Der diesbezügliche Sorgfaltsmaßstab entspricht (weitestgehend) dem des Aktienrechts.[317] Das gilt auch für die Beweislast. § 93 Abs. 2 S. 2 AktG ist insoweit entsprechend (analog) anzuwenden.[318]

Es wird deshalb vollumfänglich auf die Ausführungen zu § 93 AktG verwiesen.

4.6.4 Sonstige Geschäftsführer

Verbreitet wird davon ausgegangen, dass sich die zum Sorgfaltsmaßstab von Vorständen und GmbH-Geschäftsführern entwickelten Grundsätze (insbesondere in Bezug auf die IT-Sicherheit) auch auf sonstige Geschäftsführer – etwas einer OHG oder KG – übertragen lassen.[319]

4.6.5 (Leitende) Angestellte (insbesondere Leiter IT)

Verfügt ein Unternehmen über eine eigene IT-Abteilung, so stellt sich die Frage, ob der Leiter der Abteilung (und auch ein sonstiger Arbeitnehmer) persönlich haftet, wenn es durch eine unterlassene Verschlüsselung zu Schäden kommt.

Grundsätzlich besteht im Arbeitsrecht Einigkeit darüber, dass Haftungserleichterungen zugunsten von Arbeitnehmern anzuerkennen sind. Hiernach haften Arbeitnehmer bei betrieblich veranlassten Tätigkeiten für „leichte(ste)" Fahrlässigkeit regelmäßig überhaupt nicht und für „normale" Fahrlässigkeit (regelmäßig) nur beschränkt.[320] Selbst bei gröbster Fahrlässigkeit ist eine Haftungsbeschränkung (jedenfalls in Bezug auf die Höhe des Schadensersatzes) nicht ausgeschlossen.[321] Es kommt jeweils auf die Besonderheiten des Einzelfalls an.[322] Das bedeutet aber auch, dass IT-Verantwortliche grundsätzlich einem Haftungsrisiko ausgesetzt sind, wenn es wegen einer fehlenden (oder fehlerhaften) Verschlüsselung von Daten zu Schäden kommt.[323]

Die Höhe des dann zu ersetzenden Schadens wird maßgeblich durch den Grad der Pflichtwidrigkeit mitbestimmt. Es kann insoweit auf die Ausführungen zur Haftung

316 Vgl. oben, S. 8 (unter 3.1).

317 *Oetker*, in: Henssler/Strohn, § 43 GmbHG Rn. 4, 15. Die AG-rechtliche Kommentarliteratur nimmt ganz selbstverständlich Bezug auf die Kommentierungen zu § 43 GmbHG und die GmbH-rechtliche Kommentarliteratur auf die Kommentierungen zu § 93 AktG.

318 Statt aller: BGH, Beschl. v. 18.2.2008 – Az. II ZR 62/07, Rn. 5 (juris); *Oetker*, in: Henssler/Strohn, § 43 GmbHG Rn. 57.

319 Etwa *Röhrborn/Lang,* BB 2015, 2357, 2358. *Schmidl,* in: Hauschka/Moosmayer/Lösler, § 28 Rn. 60; *Trappehl/Schmidl,* NZA 2009, 985, 986.

320 *Zöllner/Noack*, in: Baumbach/Hueck, § 43 Rn. 6.

321 BGH, Urt. v. 11.3.1996 – Az. II ZR 230/94, Rn. 8 ff. (juris).

322 Vgl. statt aller: *Weidenkaff,* in: Palandt, § 611 Rn. 157 (mit weiteren Nachweisen auf die Rechtsprechung).

323 So auch ausdrücklich für die „Haftung des DV-Leiters" *Schuppenhauer,* A Rn. 740 ff.

von Geschäftsleitern verwiesen werden.[324] Jedenfalls als grobe Orientierung kann deshalb gelten, dass das Haftungsrisiko desto größer ist, je naheliegender eine Verschlüsselung (bzw. das Ergreifen sonstiger Sicherungsmaßnahmen) war. Insoweit wird insbesondere eine Rolle spielen, ob die Verschlüsselung von Daten gesetzlich empfohlen war. Jedenfalls dürfte es in der Praxis durchaus schwierig sein, zu begründen, weshalb es nicht (ggf. sogar grob) fahrlässig war, auf eine Verschlüsselung zu verzichten, wenn selbst der Gesetzgeber sie für sinnvoll erachtet hat.

4.6.6 Exkurs: Schadensersatz

Werden sensible Daten Dritten zugänglich, können hierdurch andere Dritte (also Vierte) einen Schaden erleiden. Das ist zunächst denkbar, wenn personenbezogene Daten abhandenkommen. Enthalten diese etwa einen kompletten Adresssatz neben Kreditkarteninformationen, können diese Daten missbraucht werden. Denkbar ist aber auch, dass Betriebs- und Geschäftsgeheimnisse von Geschäftspartnern Dritten zugänglich werden, wenn etwa ein USB-Stick verloren wird, auf dem entsprechende Daten unverschlüsselt gespeichert wurden und nun etwa von einem Wettbewerber genutzt werden können.[325]

Dabei muss grundsätzlich[326] für den gesamten verursachten Schaden gehaftet werden. Theoretisch kann somit eine unterlassene Verschlüsselung existenzvernichtende Folgen haben.

4.6.6.1 Allgemeines zivilrechtliches Haftungsrecht

Ohne an dieser Stelle das zivilrechtliche Haftungsrecht vertiefen zu können, lässt sich grundsätzlich feststellen, dass der bloße Eintritt eines Schadens für die Begründung einer Haftung nicht ausreichend ist. Vielmehr setzt eine solche grundsätzlich ein Verschulden voraus. Dabei reicht (regelmäßig) einfache Fahrlässigkeit aus. „Fahrlässig handelt [oder unterlässt], wer die im Verkehr erforderliche Sorgfalt außer Acht lässt" (§ 276 Abs. 2 BGB). Es muss also grundsätzlich bestimmt werden, ob eine Verschlüsselung von Daten nach der „im Verkehr erforderlichen Sorgfalt" erforderlich gewesen wäre. Soweit nicht eine gesetzliche Pflicht zur Verschlüsselung besteht, stellen sich die gleichen Grundprobleme wie bei der Bestimmung des Sorgfaltsmaßstabs von Geschäftsleitern. Insbesondere ist auch im Rahmen von § 276 BGB anerkannt, dass es nicht auf die „übliche" Sorgfalt oder einen „verbreiten Brauch" ankommt, sondern der Sorgfaltsmaßstab normativ zu bestimmen ist.[327] Anerkannt ist ebenfalls, dass zur Konkretisierung des Sorgfaltsmaßstabes auf „Regelwerke" zurückgegriffen werden kann.[328] Insoweit ist ein Gericht in seiner Beweiswürdigung frei.

Es spricht deshalb sehr viel dafür, dass sich ein Gericht im Schadensfall zunächst maßgeblich daran orientieren würde, ob eine gesetzgeberische Verschlüsselungs-

324 Vgl. insbesondere oben, S. 71 (unter 4.6.1.4).

325 Weitere Beispiele bei *Backu,* ITRB 2003, 251, 252.

326 Eine Ausnahme bildet allerdings das Telekommunikationsrecht. Hier ist in § 44a TKG eine Haftungsbeschränkung vorgesehen, vgl. hierzu *Eckhardt,* DuD 2008, 330, 334.

327 Statt aller *Grüneberg*, in: Palandt, § 276 Rn. 16.

328 Statt aller *Grüneberg*, in: Palandt, § 276 Rn. 18.

empfehlung vorhanden war. Jedenfalls dürfe es sehr schwer sein, zu argumentieren, es habe der im Verkehr erforderlichen Sorgfalt entsprochen, Daten *nicht* zu verschlüsseln, wenn sogar der Gesetzgeber eine Verschlüsselung empfiehlt.

Hinsichtlich anerkannter Standards wie dem IT-Grundschutz-Katalog dürfte hingegen zu differenzieren sein. Wurde dem Standard entsprochen und kommt es dennoch zu einem Schaden, dürfte einiges dafürsprechen, dass ein Gericht einen Sorgfaltspflichtverstoß verneinen würde. Wurde dem Standard nicht entsprochen, dürfte es jedenfalls leichter sein, zu begründen, weshalb die Nichteinhaltung des (anerkannten) Standards sorgfaltswidrig war, als zu begründen, weshalb es der im Verkehr erforderlichen Sorgfalt entsprochen hat, den Standard zu ignorieren. Insoweit dürfte auch zu bedenken sein, dass Gerichte mitunter nicht frei davon sind, sich von Erkenntnissen leiten zu lassen, die gerade aus dem konkreten Schadensfall folgen. So mag man abstrakt durchaus geneigt sein, E-Mail als „sicher" anzusehen, oder davon ausgehen, dass man einen USB-Stick schon nicht verlieren wird. Spätestens wenn eine E-Mail mit fremden Betriebs- und Geschäftsgeheimnissen an den falschen Empfänger versandt wurde oder ein USB-Stick verloren wurde, zeigt sich aber, dass die entsprechenden Gefahren sehr konkret sind und im Zweifelsfall auch mit Mitteln – einer Verschlüsselung – hätten abgewehrt werden können, die dem Gericht (dann) naheliegend erscheinen.

Grundsätzlich müsste in einem Zivilprozess zwar der Geschädigte beweisen, dass das Unterlassen einer Verschlüsselung pflichtwidrig war. Dieser Beweis dürfte aus den genannten Gründen allerdings häufig gelingen. Weiter dürfte davon auszugehen sein, dass den Schädiger ohnehin eine sekundäre Darlegungslast treffen würde. Eine solche sekundäre Beweislast ist anzunehmen, wenn der Beweispflichtige außerhalb des für seinen Anspruch erheblichen Geschehensablaufs steht, während der Anspruchsgegner alle wesentlichen Tatsachen kennt. Der Anspruchsgegner darf sich dann nicht auf ein bloßes Bestreiten beschränken, sondern muss substantiiert dem Vortrag entgegentreten.[329] Es spricht insoweit viel dafür, dass der Geschädigte zunächst nur vortragen müsste, eine Verschlüsselung habe der „im Verkehr erforderlichen Sorgfalt" entsprochen, weil sie bereits vom Gesetzgeber empfohlen wurde bzw. eine solche einem anerkannten Standard im Umgang mit vertraulichen Daten entsprochen habe. Der Unternehmer müsste dem dann entgegenhalten, aus welchen Gründen es im konkreten Fall dennoch nicht erforderlich war, für eine Verschlüsselung zu sorgen. Das dürfte jedenfalls herausforderungsvoll sein.[330]

4.6.6.2 Datenschutzrecht

Datenschutzrechtlich ist zunächst zu berücksichtigen, dass regelmäßig eine Verpflichtung bestehen wird, den Betroffenen über Datenschutzpannen zu informieren. Ein Verstoß hiergegen kann einen eigenen Schadensersatzanspruch auslösen.[331] Allerdings führt eine Information auch dazu, dass der Betroffene überhaupt erst auf einen möglichen Schaden aufmerksam und so in die Lage versetzt wird, Schadensersatzansprüche zu verfolgen.

329 Vgl. BGH, Urt. v. 17.1.2008 – Az. III ZR 239/06, Rn. 16 (juris) mit weiteren Nachweisen.

330 Kritsch zu den Möglichkeiten einer Entlastung auch *Klett/Lee,* CR 2008, 644, 646.

331 *Dix*, in: Simitis, BDSG, § 42a Rn. 21; *Gabel*, in: Taeger/Gabel, § 42a Rn. 6.

§ 7 BDSG und Art. 82 Datenschutz-Grundverordnung enthalten eigene Anspruchsgrundlagen für Schadensersatzansprüche. Beide Vorschriften stellen darauf ab, dass ein Schadensersatzanspruch nur besteht, soweit die „verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat“[332] bzw. „wenn [der Verantwortliche] nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.“[333] Hiernach ändert sich zunächst nichts an dem grundsätzlichen Haftungsmaßstab, wonach es nicht allein auf den Eintritt eines Schadens ankommt, sondern dieser auch verschuldet sein muss. Für ein Verschulden reicht einfache Fahrlässigkeit aus, also das Außerachtlassen der im Verkehr erforderlichen Sorgfalt.

Allerdings wird durch die entsprechenden Vorschriften eine Beweislastumkehr angeordnet.[334] Während im sonstigen Zivilrecht grundsätzlich der Geschädigte beweisen muss, dass der Schädiger den Schaden auch verschuldet hat, muss im Datenschutzrecht die datenverarbeitende Stelle nachweisen, dass sie den Eintritt nicht verschuldet hat. Dieser Nachweis dürfte in Bezug auf eine unterlassene Verschlüsselung besonders schwerfallen, weil sowohl das BDSG als auch die Datenschutz-Grundverordnung eine Verschlüsselung ausdrücklich als Mittel zur Sicherung personenbezogener Daten nennen. Die verantwortliche Stelle müsste insoweit nachweisen, dass es trotz dieser ausdrücklichen gesetzgeberischen Empfehlung im konkreten Fall nicht erforderlich war, Daten zu verschlüsseln. Der entsprechende Nachweis dürfte umso schwerer fallen, als im Schadensfall sich gerade die Gefahr realisiert haben wird, die durch eine Verschlüsselung hätte abgewehrt werden sollen und können.[335]

4.6.7 Zusammenfassung

Die Verschlüsselung von Daten (sowie die Sicherung entsprechender Schlüssel) kann zu den Sorgfaltspflichten eines Geschäftsleiters zählen. Gleiches gilt für die Leiter von EDV-Abteilungen (und letztlich auch einzelne Arbeitnehmer). Soweit keine gesetzlichen Verschlüsselungspflichten bestehen, muss der Sorgfaltsmaßstab im Wege der Auslegung konkretisiert werden. Jedenfalls in Bezug auf Geschäftsleiter ist anerkannt, dass insoweit ein objektiver Maßstab anzulegen ist und es nicht auf eine Branchenüblichkeit ankommt. Der Umstand, dass in anderen kleinen oder mittleren Unternehmen ebenfalls Daten unverschlüsselt gespeichert oder übertragen werden, entlastet insoweit grundsätzlich nicht.

Bei der Bestimmung des Pflichtenmaßstabs können gesetzliche Wertungen und anerkannte Sicherheitsstandards herangezogen werden. Diesen Empfehlungen kommt zwar kein verpflichtender Charakter zu; allerdings dürfte jedenfalls im Grundsatz begründungsbedürftig sein, weshalb sich nicht hieran orientiert wurde. Das ist vor allem bei der Haftung von Geschäftsleitern relevant, weil diese ggf. zu beweisen haben, dass ein Unterlassen einer Verschlüsselung nicht pflichtwidrig war. Dieser Beweis dürfte im Fall gesetzlicher Empfehlungen oder Hinweise auf

332 § 7 S. 2 BDSG.

333 Art. 82 Abs. 3 Datenschutz-Grundverordnung.

334 Vgl. für das BDSG statt aller *Gola/Schomerus,* § 7 Rn. 9; für Art. 82 Abs. 3 Datenschutz-Grundverordnung folgt das bereits aus dem insoweit eindeutigen Wortlaut.

335 Kritisch zu den Möglichkeiten einer Entlastung auch *Bergt,* CR 2014, 726, 731.

eine Verschlüsselung sehr herausforderungsvoll sein. Gleiches dürfte, wenn auch in deutlich abgeschwächter Form, für anerkannte IT-Sicherheitsstandards wie den IT-Grundschutz-Katalog gelten. Das gilt umso mehr, als sich in der Praxis die Frage nach einer Haftung nur stellen wird, wenn es zu einem Schadereignis gekommen ist. Es wird dann feststehen, dass ein bestimmtes Risiko – etwa dass E-Mails mit vertraulichen Informationen versehentlich an Dritte versandt werden oder Laptops mit vertraulichen Daten verloren werden können – nicht lediglich abstrakt besteht, sondern sich gerade konkret realisiert hat. Es wird außerdem feststehen, dass die entsprechenden weitergehenden Gefahren – insbesondere eine Kenntniserlangung vertraulicher Informationen durch einen Dritten – durch eine Verschlüsselung von Daten abzuwenden gewesen wären. Zusätzlich stünde im Raum, dass genau aus diesen Gründen der Gesetzgeber, eine (IT-Fach-) Behörde oder ein Fachgremium eine Verschlüsselung empfohlen haben. In einer solchen Situation den Beweis zu erbringen, dass es einem objektiven Sorgfaltsmaßstab entsprochen hat, auf eine Verschlüsselung zu verzichten, dürfte schwierig sein und nur gelingen, wenn gute und vor allem dokumentierte Gründe vorliegen.

Neben der persönlichen Haftung der Geschäftsleitung oder von Angestellten gegenüber dem Unternehmen, können auch Schadenersatzansprüche des Unternehmens gegenüber geschädigten Dritten bestehen. Auch in dieser Konstellation würde sich die Frage nach einer Sorgfaltspflichtverletzung stellen. Insoweit gelten die soeben erläuterten Grundsätze entsprechend. Soweit Schadensersatzansprüche aus datenschutzrechtlichen Vorschriften folgen, ordnet das Gesetz eine Beweislastumkehr an. D.h. der für die Datenverarbeitung Verantwortliche müsste beweisen, dass es nicht sorgfaltswidrig war, auf eine Datenverschlüsselung zu verzichten. Außerhalb des Datenschutzrechts dürfte den Schädiger jedenfalls eine sekundäre Darlegungslast dahingehend treffen, zu begründen, warum es im konkreten Fall nicht sorgfaltswidrig war, Daten unverschlüsselt zu speichern oder zu übermitteln.

4.7 Behördliche Vorgaben

In einigen Branchen existieren behördliche Vorgaben für eine verschlüsselte Kommunikation in speziellen Fällen. Voraussetzung hierfür ist grundsätzlich eine gesetzliche Ermächtigung, nach der die Behörde befugt ist, entsprechende Vorgaben zu machen. Hierbei handelt es sich regelmäßig um Generalklauseln.[336] Gemeinsam ist den gesetzlichen Vorgaben, dass eine Behörde ermächtigt wird, Formate für einen Datenaustausch vorzugeben.

Möglich ist darüber hinaus, dass Behörden eine Verschlüsselungsinfrastruktur für die Kommunikation bereitstellen (müssen), die freiwillig genutzt werden kann.

336 Da die entsprechenden Generalklauseln keine ausdrückliche Bezugnahme auf eine Verschlüsselung enthalten, ist eine Recherche im Bundesrecht und Landesrecht kaum sinnvoll möglich. Betrachtet werden deshalb *exemplarisch* einzelne Regelungen, deren praktische Bedeutung für kleine und mittlere Unternehmen sich im Rahmen dieser Studie gezeigt hat.

4.7.1 § 42a Gasnetzzugangsverordnung und § 27 Stromnetzzugangsverordnung bzw. § 52 Abs. 2 Messstellenbetriebsgesetz

Im Rahmen der Gas- und Stromversorgung ist in zahlreichen Fallkonstellationen ein Datenaustausch zwischen den Beteiligten (Betreiber von Gasversorgungsnetzen, Marktgebietsverantwortliche, Messstellenbetreiber, Messdienstleister und Netznutzer bzw. Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Bilanzkreisverantwortliche, Direktvermarktungsunternehmer nach dem Erneuerbare-Energien-Gesetz, Energielieferanten sowie jede Stelle, die über eine schriftliche Einwilligung des Anschlussnutzers verfügt, die den Anforderungen des § 4a des Bundesdatenschutzgesetzes genügt) erforderlich. Hierfür bedarf es in einem Massengeschäft Standards hinsichtlich der Kommunikation. § 42a Gasnetzzugangsverordnung und § 27 Abs. 1 Nr. 20 Stromnetzzugangsverordnung bzw. mittlerweile § 52 Abs. 2 Messstellenbetriebsgesetz[337] ermächtigen deshalb die Bundesnetzagentur, „bundesweit einheitliche Formate" für den Datenaustausch zu regeln. Die entsprechenden Datenformate sind von der Bundesnetzagentur unter Beteiligung von Branchenvertreten und Softwareexperten im Rahmen einer Expertengruppe „edi@energy" entwickelt worden.[338]

Der Standard sieht untere anderem eine Verschlüsselung und Signatur von E-Mails vor. Hiernach muss „jede E-Mail" im Rahmen des entsprechenden Datenaustauschs verschlüsselt und signiert werden.[339] Als Standard wird S/MIME (mindestens Version 3.1, RFC 3851) vorgegeben.[340] Außerdem werden Vorgaben hinsichtlich Algorithmen und Schlüssellängen (RSA mit mindestens 2048 Bit und AES-128 oder AES-192) gemacht.[341] Eine elektronische Kommunikation darf erst erfolgen, wenn entsprechende Schlüssel/Zertifikate ausgetauscht wurden.[342]

Jedenfalls in Teilen der Energiewirtschaft existiert somit ein behördlich vorgegebener Standard zur Verschlüsselung – bestimmter – elektronischer Kommunikation.

Hintergrund der entsprechenden behördlichen Ermächtigungen sind zunächst Datenschutzgesichtspunkte.[343] Abgesehen davon zählt der Energiesektor zu den kritischen Infrastrukturen.[344] An der Absicherung dieser Infrastruktur besteht deshalb ein gesamtgesellschaftliches Interesse. Schließlich handelt es sich um Netzwirtschaften, in denen durch regulatorische Vorgaben verhindert werden muss, dass einzelne Marktteilnehmer ihre Marktmacht ausnutzen, um etwa durch diskriminierende Vorgaben hinsichtlich bestimmter Kommunikationsstandards ihre Netze abzuschotten oder Wettbewerber zu benachteiligen. Nicht zuletzt mit Blick hierauf

337 § 22 StromNZV ist durch Art. 5 des Gesetzes zur Digitalisierung der Energiewende, BGBl. 2016 I, 2034 aufgehoben und durch eine entsprechende Regelung in § 52 Abs. 2 Messstellenbetriebsgesetz ersetzt worden.

338 Vgl. Mitteilung Nr. 56 zur Umsetzung der Beschlüsse GPKE und GeLi Gas v. 30.9.2016, abrufbar unter <https://www.bundesnetzagentur.de/DE/Service-Funktionen/Beschlusskammern/Beschlusskammer6/BK6_31_GPKE_und_GeLiGas/Mitteilung_Nr_56/Mitteilung_Nr56_GPKE_GeLi_Gas_Inhalt.html?nn=269610>.

339 Ziffer 5.5 Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien v. 1.10.2016.

340 Ziffer 5.5 tir. 2 Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien v. 1.10.2016.

341 Ziffer 5.5.3 Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien v. 1.10.2016.

342 Ziffer 7 tir. 1 Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien v. 1.10.2016.

343 Vgl. etwa BR-Drs. 543/15, 168 zu § 52 Messstellenbetriebsgesetz.

344 § 2 Abs. 10 Nr. 1 BSIG.

ist es nötig, dass entsprechende Kommunikationsstandards ggf. behördlich vorgegeben werden.

4.7.2 Telekommunikationsüberwachung

Nach § 110 TKG müssen die Betreiber von Telekommunikationsanlagen, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden, eine Überwachung der Telekommunikation ermöglichen. Die nähere rechtliche Ausgestaltung der Telekommunikationsüberwachung erfolgt durch die Telekommunkationsüberwachungsverordnung.[345] Dort finden sich auch generalklauselartige Vorgaben zum Schutz der „abgehörten" Daten. So ist etwa die „Überwachungskopie ... durch angemessene Verfahren gegen eine Kenntnisnahme durch unbefugte Dritte zu schützen".[346] Die weiteren technischen Einzelheiten, insbesondere zur Gestaltung des Übergabepunktes, werden durch die Bundesnetzagentur festgelegt.[347] Hierfür ist beispielsweise die Nutzung von Kryptoboxen auf der Basis der IPSec-Protokollfamilie vorgesehen.[348] Für bestimmte Formen der E-Mailkommunikation wird eine Verschlüsselung nach dem PGP-Standard (RSA-Schlüssellänge von mindestens 1 024 Bit) vorgeschrieben.[349]

Anbieter öffentlich zugänglicher Telekommunikationsnetze müssen zudem nach § 112 TKG über ein automatisiertes Auskunftsverfahren Kundendaten für öffentliche Bedarfsträger (§ 112 Abs. 2 TKG) zur Verfügung stellen (wobei der Abruf über die Bundesnetzagentur als Bindeglied erfolgt). Die Ausgestaltung des Verfahrens soll über eine Verordnung erfolgen (§ 112 Abs. 3 TKG). Soweit ersichtlich ist diese Verordnung bislang nicht erlassen worden. [350] § 113 TK sieht außerdem ein manuelles Auskunftsverfahren vor.

Die technischen Einzelheiten werden in einer Technischen Richtlinie (TR TKÜV) der Bundesnetzagentur geregelt.[351] Die TR TKÜV sieht unter anderem vor, dass die Datenübertragung kryptographisch abgesichert wird (u. a. ETSI-ESB über SINA Boxen oder E-Mail-ESB über OpenPGP).[352]

Soweit Telekommunikationsunternehmen verpflichtet sind, eine Telekommunikationsüberwachung zu ermöglichen, müssen sie also auch über eine Verschlüsselungsinfrastruktur verfügen, um Daten sicher an die Bedarfsträger übermitteln zu können.

Hintergrund der entsprechenden Regelungen ist der Schutz des Fernmeldegeheimnisses und des Rechts auf informationelle Selbstbestimmung. Wenn schon staatlicherseits hierein eingegriffen wird, dann muss wenigstens ausgeschlossen werden, dass unberechtigte Dritte Kenntnis erlangen.

345 § 110 Abs. 2 TKG.

346 § 14 Abs. 2 TKÜV.

347 § 110 Abs. 3 TKG, § 11 TKÜV.

348 Teil A, Anlage A.2 TR TKÜV, Stand 6.4.2016.

349 Teil A, Anlage 2 Ziffer 4.2. Nr. 3, Teil X Anlage X.3 Ziffer 1.2 TR TKÜV, Stand 6.4.2016.

350 Am 9. März 2017 wurde ein Referentenentwurf für eine Kundendatenauskunftsverordnung (KDAV) veröffentlicht, siehe <https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/kdav-entwurf.html>.

351 Ein Verweis auf die TR TKÜV ist im ABl. BNetzA 11/2017, 2631 veröffentlicht worden und am 14.6.2017 in Kraft getreten.

352 Anlage A und Anlage B zur TR TKÜV. Vgl. auch h BfDI, Tätigkeitsbericht 2015/2016.

4.7.3 Ermöglichung einer verschlüsselten Kommunikation

Während eine behördliche Verpflichtung zur verschlüsselten Kommunikation einer grundsätzlichen grundrechtlichen Rechtfertigung bedarf,[353] ist die bloße Eröffnung einer verschlüsselten Kommunikations*möglichkeit* unproblematisch. Unter Grundrechtsgesichtspunkten spricht deshalb nichts dagegen, wenn der Gesetzgeber Behörden verpflichtet, solche Kommunikationskanäle zu eröffnen. So sind etwa ab Juni 2017 alle Berliner Behörden verpflichtet, einen E-Mail-Zugang mit einer gängigen Ende-zu-Ende-Verschlüsselung (z. B. PGP) anzubieten.[354]

4.7.4 Zusammenfassung

In verschiedenen Bereichen – vor allem im Energiesektor sowie im Bereich der Telekommunikationsüberwachung – existieren behördliche Vorgaben zur Verschlüsselung von Daten. Diese beruhen allerdings auf gesetzlichen Ermächtigungen.

Möglich ist zudem, dass Behörden zwar nicht eine Verschlüsselung erzwingen, aber immerhin ermöglichen, indem sie selbst eine entsprechende Infrastruktur zur freiwilligen Nutzung bereithalten. Hierzu können sie auch durch den Gesetzgeber verpflichtet werden.

4.8 Ausbildungsinhalte

Jenseits des Fokus dieser auf die Verschlüsselung in kleineren und mittleren Unternehmen gerichteten Studie ist schließlich zu bemerken, dass Fragen der Datenverschlüsselung Lehrstoff in diversen Berufsausbildungen sind. Exemplarisch werden im Folgenden nur die Ausbildungsrahmenpläne[355] für staatlich anerkannte Ausbildungsberufe im Sinne von § 4 Berufsbildungsgesetz betrachtet:

Verordnung über die Berufsausbildung im Bereich der Informations- und Telekommunikationstechnik

Anlage 1 Teil A (zu § 5) Ausbildungsrahmenplan für die Berufsausbildung zum Informations- und Telekommunikationssystem-Elektroniker/zur Informations- und Telekommunikationssystem- Elektronikerin

Abschnitt I: Gemeinsame Ausbildungsinhalte[356]

Lfd. Nr.	Teil des Ausbildungsberufsbildes	Fertigkeiten und Kenntnisse, die unter Einbeziehung selbständigen Planens, Durchführens und Kontrollierens zu vermitteln sind

353 Dies gilt jedenfalls, wenn eine solche Pflicht einen Grundrechtseingriff darstellt. Unproblematisch sind insoweit etwa HTTPS-Verbindungen, weil diese von allen gängigen WWW-Browsern unterstützt werden.

354 § 4 Abs. 1 und 2 E-Government-Gesetz Berlin; vgl. hierzu LDI Berlin, Jahresbericht 2016, S. 52.

355 Im „dualen System" der Berufsausbildung legen die Ausbildungsrahmenpläne (als Anlage zu den jeweiligen Ausbildungsordnungen) fest, welche Inhalte in der betrieblichen Ausbildung vermittelt werden sollen. In den von der Kultusministerkonferenz erstellten Rahmenlehrplänen werden hingegen die Inhalte des Unterrichts an der Berufsschule spezifiziert.

356 Ebenso Anlage 2 Teil A (zu § 11), Anlage 3 Teil A (zu § 17) und Anlage 4 Teil A (zu § 23).

5.4	Datenschutz und Urheberrecht (§ 4 Abs. 1 Nr. 5.4)	a) Verschlüsselungsverfahren und Zugriffsschutzmethoden anwenden b) Vorschriften zum Datenschutz anwenden c) Vorschriften zum Urheberrecht anwenden d) technische Vorschriften zur Sicherung des Fernmeldegeheimnisses anwenden e) Daten archivieren, nicht mehr benötigte Datenbestände löschen, Datenträger entsorgen

Verordnung über die Berufsausbildung zum Medizinischen Fachangestellten/zur Medizinischen Fachangestellten

Anlage 1 (zu § 5) Verordnung über die Berufsausbildung zum Medizinischen Fachangestellten/zur Medizinischen Fachangestellten

Lfd. Nr.	Teil des Ausbildungsberufsbildes	Zu vermittelnde Fertigkeiten, Kenntnisse und Fähigkeiten
7.3	Datenschutz und Datensicherheit (§ 4 Nr. 7.3)	a) Vorschriften und Regelungen zum Datenschutz anwenden b) Daten sichern c) Datentransfer verschlüsselt durchführen d) Dokumente und Behandlungsunterlagen sicher verwahren und die Aufbewahrfristen beachten

Verordnung über die Berufsausbildung zum Mathematisch-technischen Softwareentwickler/zur Mathematisch-technischen Softwareentwicklerin

Anlage (zu § 3 Abs. 1) Ausbildungsrahmenplan für die Berufsausbildung zum Mathematisch-technischen Softwareentwickler/zur Mathematisch-technischen Softwareentwicklerin

Lfd. Nr.	Teil des Ausbildungsberufsbildes	Zu vermittelnde Fertigkeiten, Kenntnisse und Fähigkeiten
2.2	Datenschutz, Datensicherheit und Urheberrecht (§ 3 Abs. 2 Abschnitt A Nr. 2.2)	a) rechtliche und betriebliche Regelungen zum Datenschutz anwenden b) Vorgaben und Vorschriften zur Datensicherheit, Datensicherung und Archivierung beim Umgang mit Daten beachten c) Vorschriften zum Urheberrecht anwenden d) kryptografische Methoden anwenden

Verschiede staatlich anerkannte Ausbildungsberufe sehen die Vermittlung von Grundkenntnissen über Datenverschlüsselung bzw. Kryptographie vor.

4.9 Exkurs: Cyberrisiko-Versicherungen

Verletzungen der Informationssicherheit können zu immensen Schäden bei Unternehmen führen. Die Absicherung der entsprechenden Risiken durch Versicherungen stellt ein sich gerade entwickelndes Feld für die Versicherungswirtschaft dar.

Mit Blick auf die hiesige Studie ist in diesem Kontext vor allem interessant, inwieweit sich durch solche sog. „Cyberrisiko- oder Cyber-Versicherungen" Verhaltensanforderungen für kleine und mittlere Unternehmen im Hinblick auf eine Verschlüsselung ergeben können. Dies kann unter zweierlei Gesichtspunkten der Fall sein: Zunächst könnten die Versicherer einen Versicherungsschutz davon abhängig machen, dass Daten überhaupt verschlüsselt werden. Will ein Unternehmer also Cyberrisiken versichern, muss er gleichzeitig über eine Verschlüsselungsinfrastruktur verfügen oder eine solche aufbauen. Außerdem könnte die Höhe der Versicherungsprämien davon abhängen, inwieweit Unternehmen über eine Verschlüsselungsinfrastruktur verfügen.

4.9.1 AVB Cyber

Der Gesamtverband der Deutschen Versicherungswirtschaft hat Anfang des 2. Quartals 2017 ein Muster für „Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung" (AVB Cyber) veröffentlicht.

Diese AVB Cyber enthalten eine Reihe von Obliegenheiten des Versicherungsnehmers. Hierzu zählen mit Blick auf den Studiengegenstand etwa:

- die zusätzliche Absicherung von Systemen, „wenn diese einem erhöhten Risiko ausgesetzt sind. Ein erhöhtes Risiko besteht bei Geräten, die über das Internet erreichbar, oder im mobilen Einsatz sind." Als Schutzmaßnahme wird ausdrücklich die „Verschlüsselung von Datenträgern mobiler Geräte" genannt.[357]
- die Einhaltung aller „gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften".[358] Die entsprechenden Vorschriften werden nicht weiter benannt. Hierunter dürften aber insbesondere die datenschutzrechtlichen Vorschriften – etwa § 9 BDSG[359] oder Art. 32 Datenschutz-Grundverordnung[360] – fallen.

Verletzt ein Versicherungsnehmer diese Obliegenheiten, kann der Versicherungsgeber den Vertrag fristlos kündigen.[361] Wesentlich einschneidender dürfte allerdings sein, dass der Versicherungsgeber bei einer vorsätzlichen Verletzung der entsprechenden Obliegenheiten von der Leistung frei wird und bei fahrlässigen Verletzungen seine Leistung immerhin kürzen kann.[362] Kommt also ein unverschlüsseltes Mobilgerät abhanden und erleidet der Versicherungsnehmer hierdurch einen Schaden, muss der Versicherungsgeber diesen nicht (voll) ersetzen. Insofern dürfte

357 Ziffer A1-16.1 lit. b) AVB Cyber.
358 Ziffer A1-16.2 lit. a) AVB Cyber.
359 Vgl. oben, S. 40 (unter 4.5.1.1).
360 Vgl. oben, S. 49 (unter 4.5.1.3).
361 Ziffer B3-4.1 AVB Cyber.
362 Ziffer B3-4.2.1 AVB Cyber.

ein deutliches Eigeninteresse der Versicherungsnehmer bestehen, für eine entsprechende Verschlüsselung zu sorgen, weil andernfalls entsprechende Risiken nicht versichert sind und dementsprechend die Versicherungsprämien nutzlos aufgewendet würden.

4.9.2 Risikofragen

Der Gesamtverband der Deutschen Versicherungswirtschaft hat außerdem einen unverbindlichen Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen erstellt. Dieser Fragebogen soll es den Versicherern ermöglichen, die mit einer Cyberrisiko-Versicherung verbundenen Versicherungsrisiken einzuschätzen. Hiervon dürfte zunächst abhängen, ob die entsprechenden Risiken überhaupt versicherungsfähig sind. Außerdem dürfte die Prämienhöhe hiervon abhängen. Je niedriger bei einem Unternehmen das Risiko einer Inanspruchnahme der Cyberrisiko-Versicherung ist, desto niedriger dürften auch die Prämien ausfallen.

Hierdurch kann ein indirekter Druck auf Unternehmen entstehen, Maßnahmen zur Verringerung entsprechender Risiken zu ergreifen, um niedrigere Prämien bezahlen zu müssen oder überhaupt eine Versicherung abschließen zu können.

Der Muster-Fragebogen sieht eine ganze Reihe von Fragen in Bezug auf das Studienthema vor, etwa:

- „Geräte, die über das Internet erreichbar, oder im mobilen Einsatz sind, haben wir mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen."[363]
- „Es gibt einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben."[364]
- „Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt."[365]
- „Sensible Daten (z. B. personenbezogene Daten und Geschäftsgeheimnisse) werden bei Datenversand verschlüsselt."[366]

Es ist davon auszugehen, dass ein Unternehmen, welches alle Fragen mit „ja" beantworten kann, niedrigere Prämien zahlen muss als ein Unternehmen, welches die Fragen mit „nein" beantwortet. Dementsprechend hoch kann das Eigeninteresse sein, dafür zu sorgen, dass etwa sämtliche Unternehmens-Laptops verschlüsselt sind, Mitarbeiter im Außendienst nur über ein VPN kommunizieren und E-Mails mit sensiblen Daten verschlüsselt werden.

363 Frage A4 Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen.

364 Frage B2 Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen.

365 Frage B6 Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen.

366 Frage C1 Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen.

4.9.3 (Erst-) Bewertung

Da Cyberrisiko-Versicherungen sich noch nicht umfassend im Markt durchgesetzt haben und entsprechende Produkte derzeit noch entwickelt werden, ist eine abschließende Bewertung nicht möglich. Insofern kann vorliegend nur eine erste, sehr grobe Bewertung vorgenommen werden.

Grundsätzlich kann davon ausgegangen werden, dass Unternehmer ein Interesse haben werden, schwer kalkulierbare Cyberrisiken zu versichern. Gleichzeitig haben die Versicherer durch die Gestaltung der allgemeinen Versicherungsbedingungen und der Versicherungstarife eine immense Möglichkeit, Einfluss auf das Verhalten der Versicherten zu nehmen. Insofern ist es sehr gut möglich, dass das Interesse, eine möglichst günstige Cyberrisiko-Versicherung abschließen zu können, dafür sorgt, dass mehr Geräte und Daten in kleinen und mittleren Unternehmen verschlüsselt werden.

Voraussetzung hierfür ist aber zunächst, dass Unternehmer überhaupt sensibilisiert sind für die entsprechenden Cyberrisiken. Weiter ist erforderlich, dass es den Versicherern gelingt, die Versicherungsnehmer anzuhalten, ihren Obliegenheiten mit Blick auf eine Verschlüsselung nachzukommen. Das ist insoweit nicht unproblematisch, als Voraussetzung hierfür ist, dass die allgemeinen Versicherungsbedingungen nicht nur zur Kenntnis genommen, sondern die sich hieraus ergebenden Konsequenzen auch umgesetzt werden. Insoweit kann nämlich nicht unbedingt vorausgesetzt werden, dass ein Versicherungsnehmer ohne weiteres etwa weiß, dass er transportable Datenträger verschlüsseln muss, wenn er mit Blick auf die sich ergebenden Gefahren Versicherungsschutz genießen möchte. Noch problematischer ist dies mit Blick auf die „gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften". Dies setzt nämlich letztlich eine Detailkenntnis des Rechts voraus. Erforderlich wäre insofern, dass dem Versicherungsnehmer kommuniziert wird, welche Verschlüsselungspflichten sich bereits aus dem allgemeinen und besonderen Datenschutzrecht ergeben können und dass sich vor allem die weit gefassten Generalklauseln in Einzelfällen – etwa beim Versand besonders sensibler personenbezogener Daten per E-Mail – zu einer konkreten Verschlüsselungspflicht verdichten können.

Fehlt es an einer entsprechenden Aufklärung, besteht die Gefahr, dass sich Cyberrisiko-Versicherungen sogar kontraproduktiv auswirken: Das könnte insbesondere der Fall sein, wenn Versicherungsnehmer der Fehlintuition folgen sollten, keine weitere Maßnahmen insbesondere in Bezug auf eine Verschlüsselung ergreifen zu müssen, „weil das Risiko ja versichert ist".

4.9.4 Zusammenfassung

Cyberrisiko-Versicherungen können einen wichtigen Beitrag zu mehr Verschlüsselung leisten. Voraussetzung hierfür ist aber, dass es den Versicherern gelingt, die Versicherungsnehmer dafür zu sensibilisieren, dass Voraussetzung für einen Versicherungsschutz bzw. ggf. niedrigere Versicherungsprämien die Einrichtung einer Verschlüsselungsinfrastruktur zur Eigenabwehr von Cyberrisiken ist.

5 Handlungsempfehlungen

Auf Basis der Studienergebnisse, der Hintergrundgespräche mit den Dienstleistern und Anbietern im Bereich Verschlüsselungslösungen sowie der Ergebnisse des Ergebnisworkshops mit IT-Sicherheitsexperten können Handlungsempfehlungen zur Stärkung des Einsatzes von Verschlüsselungslösungen in KMU abgeleitet werden.

Diese lassen sich unterteilen in:

1. Allgemeine Unterstützungsmaßnahmen
2. Konkrete Maßnahmen zur Förderung der E-Mail-Verschlüsselung
3. Konkrete Maßnahmen zur Förderung der Datenverschlüsselung
4. Konkrete Maßnahmen zur Förderung der Verschlüsselung des http-Webtraffics

5.1 Allgemeine Unterstützungsmaßnahmen

5.1.1 Verbände und Anbieter: Awareness steigern durch zielgerichtete Informations- und Motivationskampagnen

Der im Zusammenhang mit dieser Erhebung erstellte Kompass IT-Verschlüsselung zeigt, dass KMU eine Vielzahl von Maßnahmen zur Verbesserung der Daten- und Transportverschlüsselung relativ leicht umsetzen können.

Die Unternehmensbefragung ergab jedoch, dass jeweils mind. ein Viertel der KMU keinerlei E-Mail-, Speicher-/Datei- oder Webtraffic-Verschlüsselung einsetzt. Und dort, wo Verschlüsselung eingesetzt wird, existiert vielfach keine durchgängige Implementierung oder es fehlen Compliance-Vorgaben.

Aus diesem Grunde sollten die Verbände ggf. mit Unterstützung des Bundes eine Kampagne entwickeln, die kleine und mittelständische Unternehmen motiviert, den Grad der Verschlüsselung im Unternehmen und in der Kommunikation mit Geschäftspartnern und Kunden zu erhöhen.

Auf Basis der Expertengespräche im Rahmen der Studie und des Ergebnisworkshops mit IT-Sicherheitsexperten werden folgende Maßnahmen für eine solche Kampagne vorgeschlagen:

- **Stärkere Kommunikation des Themas Verschlüsselung bei Schulungen/Veranstaltungen zu IT-Sicherheit:** Der Einsatz von Verschlüsselungslösungen sowie Best-Practice-Anwendungen aus verschiedenen Branchen müssten gezielter auf IT-Sicherheitsveranstaltungen von Branchen und/oder Kammern kommuniziert werden. Ggf. müssten hierfür eigenständige Formate entwickelt werden, da das Thema Verschlüsselung auf übergreifenden Veranstaltungen zum Thema IT-Sicherheit i.d.R. nur sehr ausschnittsweise behandelt wird.
- **Öffentlichkeitswirksame Events zur Förderung anwenderfreundlicher Verschlüsselungslösungen:** Ähnlich wie bei anderen Innovationspreisen könnte ein Preis für Verschlüsselungslösungen ausgelobt werden, der Aspekte wie Sicherheit, Innovation, Bedienbarkeit, Schnittstellen, Skalierbarkeit oder Flexibilität der Lösungen bewertet. Alternativ könnten auch Hackathons zum Thema Verschlüsselung durchgeführt werden. Hier könnte der Bund bei der Preisauslobung unterstützen. Ein solches Event könnte vom Bund mit initiiert bzw. finanziell unterstützt werden.
- **Bessere Markttransparenz für KMU-Lösungen zur Verschlüsselung schaffen**: Marktplätze und Anbieterverzeichnisse zu Produkten der IT-Sicherheit, wie sie vom Bundesverband IT-Sicherheit e.V. (TeleTrust) oder einzelnen Fachmedien angeboten werden, müssten stärker auf das Thema Verschlüsselung zugeschnitten, breiter kommuniziert und ggf. um Ausschreibungsunterstützung oder Vermittlungsfunktionalitäten für indikative Angebote ergänzt werden.
- **Offensivere Preis- und Aufwandskommunikation der Hersteller:** Ein Ergebnis der Umfrage war, dass Unternehmen ohne Verschlüsselungslösungen gerade im Bereich der Kommunikationsverschlüsselung (E-Mail, VPN) hohe Kosten für Implementierung und Betrieb erwarten.
- **Anwenderfreundlichkeit der Anwendungen betonen:** Darüber hinaus sollten Hersteller/Lösungsanbieter die Usability ihrer Anwendungen im Unternehmenseinsatz in typischen Szenarien stärker hervorheben, da gemäß der Befragung Nicht-Anwender Komfortverluste erwarten.
- **Kommunikation der Rechtslage:** Die hier unternommene Analyse der rechtlichen Verschlüsselungsverpflichtungen und -obliegenheiten sollte zielgruppengerecht aufbereitet und gezielt kommuniziert werden. Insbesondere sich möglicherweise ergebende Meldepflichten und Schadensersatzpflichten dürften nicht in hinreichendem Maße in kleinen und mittleren Unternehmen bekannt sein. Die zentrale Bündelung von Informationen zur Rechtslage im direkten Zusammenhang mit der technischen Lösungskommunikation dürfte eine erhebliche zusätzliche Motivation darstellen, die über die rein technische Kosten-/Nutzenerwägung einzelner Lösungen hinausgeht.
- **Modular aufgebaute Muster-Unternehmensrichtlinien für KMU erstellen**: Aus den Ergebnissen der durchgeführten Umfrage lässt sich zudem ablesen, dass dort, wo Verschlüsselungslösungen eingesetzt werden, der Einsatz vielfach nicht hinreichend formalisiert ist. Dies bedeutet z.B., dass die Mitarbeiter keine ausreichenden Entscheidungsvorgaben erhalten, wann Daten oder E-Mails zu verschlüsseln sind. Branchenverbände könnten entsprechende Musterrichtlinien/Compliance-Vorgaben als Handreichung veröffentlichen.

5.1.2 Bund und Marktteilnehmer: Marke und Plattform entwickeln und bestehende Initiativen nutzen

Neben der Frage, mit welchen Inhalten und Maßnahmen man KMU beim Einsatz von Verschlüsselungslösungen unterstützen kann, ist zu überlegen, über welche Form der Kommunikation und Ansprache das Engagement der Unternehmen bestmöglich erzeugt/gesteigert werden kann.

Hier ist festzustellen, dass bereits eine Vielzahl von Initiativen von Branchen- und Berufsverbänden, Mittelstandsvereinigungen, Kammern und branchenübergreifenden Zusammenschlüssen bestehen, die das Ziel verfolgen, die IT-Sicherheit in den Unternehmen (v.a. auch im KMU-Bereich) und damit den Wirtschaftsschutz zu verbessern. Mehrere dieser Initiativen werden von Bundesministerien oder auch vom Bundesamt für Sicherheit in der Informationstechnik gestützt.

Alle diese Initiativen haben ihre eigene Agenda und kommunizieren zu unterschiedlichen Themen der IT-Sicherheit. Nach Einschätzung der befragten Unternehmen und Branchenexperten wäre es nicht sinnvoll, eine weitere Initiative für das Thema Daten- und Transportverschlüsselung zu gründen, die parallel zu den bestehenden Plattformen aktiv wird.

Sinnvoller wäre es, lediglich eine Online-Informationsplattform mit eigener Marke zum Thema IT-Verschlüsselung zu entwickeln, auf die dann alle Initiativen der Verbände, Initiativen und Ministerien als Multiplikatoren verweisen können. Neue Informationen oder Angebote könnten so mit dieser Marke verbunden werden und einheitlich über die Verteiler/Kanäle der Verbände und bestehenden Initiativen kommuniziert werden.

Durch eine Einbindung aller zentralen Initiativen und deren Kommunikationskanäle könnte ein wahrnehmbarer Kommunikationsdruck aufgebaut werden.

Um dieses Thema inhaltlich zu treiben, müssen jedoch kontinuierlich neue Inhalte mit Informationswert (Service-Angebote, Infomaterial o.ä.) angeboten werden, um eine längerfristige Kommunikation des Themas über die Multiplikatoren zu gewährleisten.

Die Gründung und der Betrieb einer solchen Informationsplattform könnte vom Bund mit initiiert bzw. finanziell unterstützt werden.

Ein Förderprogramm, das gutscheinbasiert Orientierungsberatungen für KMU vorsieht, kann hierbei für die notwendige Transmission der Inhalte in die Unternehmen sorgen und helfen, die Online-Informationsplattform in der Zielgruppe zu etablieren. Zudem wäre ein solches Förderprogramm ein idealer Gradmesser für den spezifischen Bedarf, der in KMU besteht, und kann nachfrageorientiert weiterentwickelt werden. Je nach Ausgestaltung des Förderprogramms sollten auch Investitionen in technische Verschlüsselungslösungen zuschussfähig sein.

Zugleich könnte das Thema Verschlüsselung als Aspekt innerhalb der nationalen Digitalisierungsstrategien des Bundes konkret benannt und in der Evaluation der laufenden Maßnahmen berücksichtigt werden.

5.1.3 Behörden: Öffentlichkeitsarbeit der Aufsichtsbehörden intensivieren

Parallel zu den Aktivitäten der Branche sowie gemeinsamen Aktivitäten von Bund und Unternehmen könnten die mit den Themen IT-Sicherheit und Datenschutz betrauten Behörden ihre Kommunikation in Bezug auf das Thema Verschlüsselung intensivieren. Dies könnte im Rahmen der verschiedenen (behördlichen) Informationsangebote zur Umsetzung der DS-GVO erfolgen. Hier besteht auf Unternehmensseite derzeit ohnehin ein großer Informationsbedarf, so dass die damit einhergehende datenschutzrechtliche Sensibilisierung genutzt werden könnte, um neben juristischen auch über technische Aspekte – wie insbesondere eine Datenverschlüsselung – zu informieren.

Darüber hinaus könnte eine harmonisierte, übergreifende und gemeinsame Ergebnisdarstellung der unabhängigen Datenschutzbehörden des Bundes und der Länder (ggf. über den Düsseldorfer Kreis) zu einer weiteren Erhöhung der Sensibilität der Unternehmen im Umgang mit personenbezogenen Daten führen.

Hierfür bedürfte es zudem einer einheitlichen Kommunikation der Datenschutzbehörden zu Themen wie:

- die Ausgestaltung der innerbetrieblichen Unternehmensorganisation zur Erfüllung der besonderen Anforderungen des Datenschutzes
- die Nutzung von Transportverschlüsselung beim Versand von Daten
- die Nutzung von Transport- und Inhaltsverschlüsselung bei Daten mit erhöhtem Schutzbedarf.

5.2 Konkrete Maßnahmen zur Förderung der E-Mail-Verschlüsselung

Für eine verschlüsselte Business-to-Business-Kommunikation als auch für die Verschlüsselung der Kommunikation zwischen Unternehmen und Privatkunden wird bislang mehrheitlich auf eine strukturierte Plattformkommunikation gesetzt, weil E-Mail-Verschlüsselung bislang nicht weit genug verbreitet ist.

Das bedeutet, der verschlüsselte Austausch schützenswerter Dateien (Angebote, Konstruktionszeichnungen, Rechnungen, Kontoauszüge etc.) erfolgt entweder über Online-Plattformen mit SSL-Verschlüsselung oder unverschlüsselt.

Nachfolgend werden Maßnahmen diskutiert, wie der Einsatz der E-Mail-Verschlüsselung in den Unternehmen und auf Kundenseite weiter vorangetrieben werden kann, da diese eine deutlich direktere und anwenderfreundliche Form der verschlüsselten Kommunikation ermöglicht.

5.2.1 Bestehende Initiativen weiterentwickeln

Ein gemeinsames Vorgehen der großen deutschen E-Mail-Anbieter könnte einen beträchtlichen Hebel zur Förderung der E-Mail-Verschlüsselung zwischen Privatpersonen aber auch zwischen Unternehmen und Kunden auf Grundlage der bereits bestehenden E-Mail-Accounts bedeuten.

Bestehende Verschlüsselungsinitiativen großer deutscher E-Mail-Provider könnten hierfür eine gute Ausgangsbasis darstellen. Die Web-Angebote der großen deutschen E-Mail-Provider werden monatlich von mind. 20 bis 30 Mio. Personen genutzt. Untereinander kommunizieren die Kunden führender deutschen E-Mail-Provider auf der Transportebene bereits verschlüsselt, das Routing und die Datenspeicherung erfolgt ausschließlich in Deutschland.

Der Fokus auf vornehmlich privat genutzte FreeMail-Angebote ist allerdings ein Hemmnis für die verschlüsselte Kommunikation mit E-Mail-Servern von Unternehmen. Der Bund könnte hier als Initiator für eine Weiterentwicklung bestehender Unternehmensinitiativen fungieren. In Gesprächen mit den Stakeholdern sollten u.a. die folgenden Punkte adressiert werden:

- Mit den aktuellen Betreibern sollten die Möglichkeiten ausgelotet werden, weitere E-Mail-Provider (z.B. mit Fokus auf Unternehmenskunden) zu zertifizieren. Wenn hierbei spezifische Hemmnisse bestehen, sollten diese klar benannt werden.
- Auch Unternehmen mit einem hohen Bedarf an verschlüsselter Kommunikation (z.B. Banken und Versicherungen) sollten die Möglichkeit haben, ihre eigenen E-Mail-Server für bereits bestehende Initiativen zu zertifizieren.
- Deutsche E-Mail-Provider könnten künftig ebenfalls den offenen Standard TLS/DANE unterstützen, mit dem sich die Vertrauenswürdigkeit und Integrität von E-Mails sicherstellen lässt und der für kleinere E-Mail-Provider ggf. einfacher als eine Zertifizierung umzusetzen ist.

5.2.2 Dialog mit führenden E-Mail-Client-Anbietern führen

E-Mails werden überwiegend Client-basiert über Mailprogramme und nicht über Webmail-Interfaces gesendet und empfangen. Um eine Inhaltsverschlüsselung der E-Mail-Kommunikation zwischen Unternehmen und zwischen Unternehmen und Privatkunden weiter voranzubringen, müssen die in Unternehmen eingesetzten E-Mail-Clients bzw. auch die zugrunde liegenden Betriebssysteme in den Fokus gerückt werden.

Während im Bereich des E-Mail-Providing deutsche Unternehmen über einen signifikanten Marktanteil verfügen, ist die Anbieterlandschaft bei den gängigen Betriebssystemen und Mailprogrammen für PC/Notebooks und mobile Endgeräte von global agierenden IT- und Softwarekonzernen geprägt.

Ohne die native Integration einer Schlüssel-/Zertifikatsverwaltung für PGP und S/MIME in marktführende E-Mail-Clients und eine einfache und automatisierte Benutzerführung für die zentralen Prozesse wie Schlüsselerstellung, Hinterlegung (Upload) und Bezug bzw. Zertifikatserwerb und -management (inkl. Erneuerung) fehlt die Hebelwirkung für eine deutliche Verbreitung einer Ende-zu-Ende-Verschlüsselung der E-Mail-Kommunikation.

Es fehlt eine native Unterstützung der E-Mail-Clients für Verschlüsselungstechnologien. Viele Mailprogramme können PGP/GnuPG oder S/MIME momentan nicht ohne zusätzliche, externe Plugins nutzen. Dies erschwert den Einsatz von Verschlüsselung, da die Nutzer sich eigenständig um die Integration kümmern müssen. Eine nutzerkonforme Integration der nötigen Technologien unter dem Entwicklungsparadigma Security-by-Design seitens der E-Mail-Client-Anbieter selbst könnte die Verbreitung von Verschlüsselung maßgeblich vorantreiben. Die Benutzerführung würde durch Integration auch intuitiver und die generelle Handhabung einfacher werden.

Der Bund könnte sich hier für einen Dialog zwischen deutschen Anbietern von Verschlüsselungslösungen mit den globalen Marktführern einsetzen. Ggf. könnte dieser Dialog auch auf europäischer Ebene mit Unterstützung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) geführt werden.

5.2.3 Förderung zur Anwendungsentwicklung für eine bessere Systemintegration und verbesserte Nutzerfreundlichkeit von freier Software

Das PGP/GnuPG-Verschlüsselungsverfahren ist insbesondere in Kleinst- und kleinen Unternehmen bevorzugt im Einsatz, während die S/MIME-Verschlüsselung eher in Großunternehmen Anwendung findet (vgl. Abb. 17).

Sämtliche Komponenten zur Nutzung von PGP/GnuPG stehen als freie Plugin-Software für verschiedene Mailprogramme zur Verfügung. Mit PGP/GnuPG lässt sich ad hoc eine leistungsfähige Verschlüsselungslösung nutzen, ohne dass kommerzi-

elle Nutzungslizenzen anfallen. Von Vorteil ist weiterhin, dass PGP/GnuPG plattformübergreifend sowohl auf Windows-, Macintosh- und Linuxsystemen genutzt werden kann.

Aufgrund fehlender Kommerzialisierungsinteressen sind diese Plugins insbesondere bei der Nutzerfreundlichkeit und der zeitnahen Anpassung an Betriebssystem-Updates kommerziellen Lösungen oft unterlegen. Auch fehlen bislang weitgehend Integrationsmöglichkeiten in mobile Betriebssysteme.[367] Der kommerzielle Wettbewerb stellt offenkundig an entscheidenden Stellen keine Lösungen – vor allem, weil die Refinanzierungsmöglichkeiten zu gering sind.

Der Bund könnte die Wartung, Pflege und Weiterentwicklung bestehender Lösungen (Installationspakete, Plugins, Clients etc.) stärker fördern oder gezielt die fehlenden Anwendungsentwicklungen beauftragen.

Für eine solche, durch den Bund initiierte, Entwicklungsförderung gibt es ein besonders erfolgreiches Beispiel: Im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde das Programm, welches bis heute die Nutzung von PGP/GnuPG mit einer freien Softwarelizenz unter Windows ermöglicht, seit dem Jahr 2006 entwickelt. Auf diese Weise hat das BSI die praktische Verwendung von PGP/GnuPG unter Windows wesentlich gefördert.

In Bezug auf die aktuell weiter bestehenden Verschlüsselungsdesiderate ist vor allem die fehlende Integration von E-Mail-Verschlüsselung in mobile Plattformen zu nennen. Eine Professionalisierung und Verstetigung der Softwareentwicklung- und -pflege insbesondere mit Bezug auf mobile Endgeräte könnte einen wesentlichen Beitrag zur betrieblichen Verankerung von Verschlüsselung in KMU leisten. Da es aktuell, trotz der Bedeutung von mobilen Endgeräten, marktseitig keine gängigen, verfügbaren Lösungen für die mobile E-Mail-Verschlüsselung gibt, sollte vorrangig geprüft werden, ob eine Entwicklungsförderung im vorwettbewerblichen Bereich liegt und somit durch die Bundesregierung aktiv unterstützt werden kann.

5.2.4 Infrastrukturen für Vertrauensdienste stärken

Für den professionellen Einsatz einer Inhaltsverschlüsselung im Rahmen der E-Mail-Kommunikation setzen größere Unternehmen aus Praktikabilitätsgründen mehrheitlich auf den S/MIME-Standard. Die S/MIME PKI-Infrastruktur mit ihren Zertifizierungsstellen gewährleistet im Unterschied zum Web-of-Trust-Ansatz bei PGP eine standardmäßige Authentifizierung der Zertifikatsinhaber. Kleinere Unternehmen scheuen hingegen die mit den kontinuierlich zu erneuernden Zertifikaten verbundenen Kosten.

Der Markt für Vertrauensdienste ist derzeit von global operierenden US-amerikanischen Anbietern geprägt. In Deutschland gibt es nur wenige kommerzielle Anbieter, die umfassende Vertrauensdienste anbieten.

367 Abgesehen vom S/MIME-Standard unter der iOS-Plattform wird E-Mailverschlüsselung in mobilen Betriebssystemen nicht nativ unterstützt. Insbesondere die PGP-Verschlüsselung ist in mobilen Umgebungen nur sehr eingeschränkt realisierbar.

Der Bund könnte im Dialog mit den kommerziellen Anbietern aus Deutschland (z.B. TeleSec, Bundesdruckerei) eine Strategie entwickeln, mit der KMU-Unternehmen aktiv für die Nutzung deutscher PKI-Verschlüsselungsinfrastrukturen gewonnen werden können. **Unter einer einheitlichen Dachmarke könnten kommerzielle Anbieter von Vertrauensdiensten ein einheitliches Produkt anbieten, das sich speziell an den Bedürfnissen von KMU orientiert und insbesondere in der Einführungsphase durch eine attraktive Preisgestaltung oder kostenfreie Nutzung überzeugt.** Ggf. ließen sich bestimmte Aspekte der Einführung auch über ein entsprechendes Bundesprogramm gezielt fördern.

5.2.5 Vision für eine vollständig integrierte Verschlüsselungslösung

Verschlüsselung für E-Mail-Kommunikation ist nach heutigem Stand nicht ohne zusätzlichen Aufwand durch den Nutzer bzw. das Unternehmen möglich. Es gibt zwar automatisierte Verschlüsselungslösungen für E-Mail-Kommunikation, jedoch sind diese gebührenpflichtig und nicht für jede Unternehmensgröße oder für Privatnutzer geeignet. Eine globale, nativ integrierte Verschlüsselungslösung, mit der sich ohne großes Wirken und Vorwissen der Nutzer automatisiert E-Mails ver- und entschlüsseln lassen, wäre daher wünschenswert. Der mögliche Einsatz auf Smartphones, Tablets und stationären Rechnern wie Laptops ist dabei eine zwingende Voraussetzung. In der Funktionsweise sollte diese heutigen Instant-Messengern ähneln, da diese bereits heute in der Lage sind, durchgehend verschlüsselte Kommunikation im Hintergrund zu realisieren. Die Schlüsselverwaltung und der sichere Austausch von Schlüsselpaaren im Hintergrund sind bereits heute möglich. Ähnlich verhält es sich mit der Zertifikatverwaltung und Erneuerung.

Es ist daher keine Frage der prinzipiellen Machbarkeit, alle grundlegen Technologien für eine solche Lösung stünden bereits zur Verfügung. Allein geeignete Client-Software und die nötige Infrastruktur zur Umsetzung dieses Vorhabens müssten entwickelt, spezifisch angepasst und anschließend „nur noch" beworben werden. Innerhalb einer Machbarkeitsstudie können die technischen Voraussetzungen, die Kosten und die kritischen Stakeholder für eine vollständig integrierte Verschlüsselungslösung näher untersucht und bestimmt werden.

5.2.6 Verschlüsselte Behördenkommunikation ermöglichen

Bundesministerien und Behörden können auf pragmatische Weise ihren Beitrag zur Förderung von verschlüsselter Kommunikation im Alltag von KMU leisten, indem sie für sämtliche E-Mail-Postfächer den Einsatz von E-Mail-Verschlüsselung im S/MIME- und PGP/GnuPG-Format ermöglichen.

Ein aktiver Hinweis auf die Möglichkeit und Vorteile von verschlüsselter Kommunikation beim Austausch schützenswerter Daten stellt bereits aufgrund der Vielzahl an elektronischen Kommunikationsakten, die von Einrichtungen des Bundes ausgehen oder Einrichtungen des Bundes erreichen, einen relevanten Treiber dar.

Behörden sind zwar bereits seit März 2016 durch das E-Government-Gesetz dazu verpflichtet, eine verschlüsselte Kommunikation über De-Mail zu ermöglichen, jedoch konnte dieser Kommunikationsstandard bislang keine hohe Nutzerakzeptanz erzielen.[368]

Zudem beschränkt sich die verschlüsselte Behördenkommunikation über De-Mail oftmals auf ein generisches Konto einer Bundeseinrichtung („poststelle@einrichtung.bund.de"), sodass auch die Mitarbeiter innerhalb einer Behörde nicht die Möglichkeit haben, ihren schutzbedürftigen Mailverkehr untereinander zu verschlüsseln.

Mit Hilfe professioneller Verschlüsselungslösungen für den B2C-Einsatz (z.B. durch Zustellung von Nachrichten als https-gesicherter Webdownload) wäre es Behörden zudem möglich, schutzbedürftige Kommunikation auch dann verschlüsselt zu versenden, wenn der Empfänger keine verschlüsselten E-Mails empfangen oder versenden kann.

5.3 Konkrete Maßnahmen zur Förderung der Speicher- und Dateiverschlüsselung

Maßnahmen zur Dateiverschlüsselung können von jedem Unternehmen relativ leicht auf Basis der plattform-/geräte-/betriebssystem-inhärenten oder programmspezifischen Verschlüsselungslösungen umgesetzt werden.

Zudem existiert eine Vielzahl kostenfreier/kostengünstiger (Open-Source-) Lösungen für eine plattformunabhängige Verschlüsselung von Dateien und Ordnern auf internen Servern und auf Cloud-Plattformen.

Sofern wichtige Daten in den Unternehmen nicht verschlüsselt abgespeichert werden, liegt dies vornehmlich an fehlenden organisatorischen Strukturen.

Zur Verbesserung der Dateiverschlüsselung in KMU könnte die in Abschnitt 5.1.2 vorgeschlagene Online-Informationsplattform zum Thema IT-Verschlüsselung beitragen, indem Branchenverbände und Mittelstandsvereinigungen auf das Informationsangebot einer solchen Dachmarke/Plattform hinweisen.

Auf der Plattform könnten die Vorteile des Einsatzes von einfach zu implementierenden Lösungen (z.B. Open-Source-Programm Veracrypt) offensiv ggü. Kleinst- und kleinen Unternehmen beworben werden.

Neben technischen Informationen könnten hier auch auf den geschäftlichen Einsatz abgestimmte Bedienvideos und Tutorials präsentiert werden.

368 Im Rahmen einer Repräsentativ-Erhebung gaben 8 Prozent der Befragten an, ein De-Mail-Konto zu besitzen, während 80 Prozent angaben, entweder kein De-Mail-Konto zu besitzen, die Registrierung nicht zu planen bzw. den Dienst nicht kennen (vgl. Initiative D21: eGovernment Monitor 2016, S. 23).

5.4 Konkrete Maßnahmen zur Förderung der Verschlüsselung des http-Webtraffics

Eine gute Möglichkeit, in vergleichsweiser kurzer Zeit und mit geringem Aufwand den Einsatz von Verschlüsselung in der Praxis umzusetzen, ist die Förderung der Nutzung von Transportverschlüsselung. Im Gegensatz zur E-Mailverschlüsselung, deren Gelingen vom erfolgreichen, oft manuellen Schlüsseltausch der Kommunikationspartner abhängt, läuft der „TLS-Handshake" auf Transportebene automatisiert und ohne einen Eingriff des Nutzers ab. Daher lassen sich mit der Transportverschlüsselung des Webtraffics die größten Hebeleffekte erreichen.

Eine im Rahmen der Studienerstellung durchgeführte Anfrage beim Internetknoten-Betreiber DE-CIX in Frankfurt a.M. hat ergeben, dass der Anteil des http-Traffics immer noch genauso groß ist, wie der Anteil des https-Traffics. Erfahrungsgemäß liegt der Anteil des https-Traffics, der von Unternehmensarbeitsplätzen abgerufen wird, deutlich höher. Jedoch ist insgesamt festzustellen, dass immer noch ein hoher Anteil des Webtraffics unverschlüsselt übertragen wird, obwohl dem Einsatz von Transportverschlüsselung aufgrund des vom Nutzer unbemerkten Protokollwechsels (von http zu https) und des automatisch ablaufenden Schlüsseltausches zwischen Browser und Server keine besonderen Hemmnisse entgegenstehen.

Im Unterschied zur E-Mail-Kommunikation lassen sich bei der Transportverschlüsselung zudem enorme Skalenerträge realisieren: Auch wenn ein Webserver mehrere 100.000 Anfragen gleichzeitig bedient, kann ein einzelnes Server-Zertifikat ausreichen, um sämtlichen ein- und ausgehenden Webverkehr zuverlässig durch Verschlüsselung abzusichern.

Viele größere Webseitenbetreiber bieten Transportverschlüsselung an, insbesondere, wenn schützenswerte personenbezogene Daten der Nutzer Bestandteil der Webseitennutzung sind (Online-Banking-Portale, E-Mail-Portale etc.). Doch andere reichweitenstarke Websites wie etwa führende deutsche Online-Nachrichtenangebote verzichten bislang auf Transportverschlüsselung.

Es besteht somit noch ein erhebliches ungenutztes Potenzial zur Absicherung der Authentizität und Vertraulichkeit der Internetkommunikation. Insbesondere für KMU in Branchen mit geringerem IT-Reifegrad stellt die Transportverschlüsselung eine besonders einfache Möglichkeit dar, eine effektive Kommunikationsverschlüsselung zu implementieren.

Neben Aufklärungs- und Motivierungskampagnen (vgl. Abschnitt 5.1.1 und 5.1.2) steht noch eine weitere, innovative Möglichkeit zur Verfügung, den Einsatz der Transportverschlüsselung insbesondere in Kleinstunternehmen zu unterstützen.

Der Bund könnte die Einrichtung einer nicht-kommerziellen Zertifizierungsstelle fördern, die kostenlose TLS-Zertifikate an private Nutzer, nicht-kommerzielle Einrichtungen und kleine Unternehmen ausgibt, die kein hinreichendes ökonomisches Eigeninteresse daran haben, kommerzielle TLS-Zertifikate zu implementieren.

Eine vergleichbare Einrichtung existiert in den Vereinigten Staaten mit der industriefinanzierten Stiftung „Internet Security Research Group" (ISRG), die eine für Nutzer kostenlose Zertifizierungsstelle betreibt. Die ISRG hat bereits über 40

Mio. TLS-Zertifikate zur kostenlosen Nutzung herausgegeben, auch an deutsche Website-Betreiber.

Die automatisierten Prozesse, die auf Seiten der Zertifizierungsstelle mit dem Namen „Let's Encrypt" ablaufen, ersetzen die gängigen händischen Vorgänge bei der Erstellung, Validierung, Signierung, Einrichtung und Erneuerung von Zertifikaten für verschlüsselte Websites. Da „Let's Encrypt" nur Basis-Zertifikate (sogenannte Domain-Validation-Zertifikate) ausgestellt, wird der Markt für kommerzielle Zertifizierungsstellen nicht tangiert, da für Webanwendungen mit erhöhtem Schutzbedarf zusätzlich Organization-Validation- und Extended-Validation-Zertifikate notwendig sind, die Let's Encrypt nicht anbietet.

Ein solches Modell ist auch in Deutschland denkbar. Insbesondere, wenn die führenden Zertifizierungsstellen von der strategischen Bedeutung einer solchen gemeinnützigen Einrichtung überzeugt werden können. Eine kostenlose Ausgabe einfacher Basis-Zertifikate ist zudem die einfachste Möglichkeit, Unternehmen für weitergehende Einsatzfelder von Verschlüsselungslösungen zu sensibilisieren.

Daher sollten vor allem die führenden deutschen Trust-Center dazu motiviert werden, auf ähnliche Weise gemeinnützig tätig zu werden. Insbesondere unter dem Gesichtspunkt der künftigen Geschäftsfeldentwicklung sind, neben der kostenlosen Bereitstellung von Basis-Zertifikaten, auch weitere innovative Fördermodelle denkbar, etwa eine in der Zahl der Zugriffe beschränkte kostenlose Bereitstellung von Extended-Validation-Zertifikaten.

Ähnlich wie der Vorschlag zur Förderung einer deutschen PKI-Infrastruktur (vgl. Abschnitt 4.2.4) zielt auch dieser Ansatz auf die langfristige Stärkung einer souveränen deutschen/europäischen Vertrauensinfrastruktur ab.

6 Fazit

Die Studie zum Einsatz elektronischer Verschlüsselung in KMU sowie zu den Hemmnissen und Treiben für die Implementierung und Nutzung dieser Systeme ergab in der Gesamtschau folgende Ergebnisse:

Unternehmensbefragung

Über drei Viertel der KMU nutzen bereits Verschlüsselungslösungen. Auch stimmen nahezu alle KMU der These zu, dass Verschlüsselung von Daten zu den Grundsätzen einer ordnungsgemäßen Unternehmensführung gehört. Verschlüsselung wird jedoch oft nur in isolierten Einsatzbereichen eingesetzt und überdies nicht durchgängig in allen Endgerätetypen unterstützt.

Die Gründe für den unstrukturierten Einsatz von Verschlüsselungslösungen in KMU sind vielfältig, sie reichen von einer unübersichtlichen Anbieter- und Lösungslandschaft bis zu fehlenden Kompetenzen – auf Ebene der eigenen IT-Fachabteilung, der externen IT-Dienstleister sowie der Anwender im eigenen Unternehmen. Verschlüsselung wird daher zumeist nur dort durchgehend eingesetzt, wo es der Schutzbedarf unbedingt erfordert.

Zwischen den Branchen zeigen sich derzeit durchaus Unterschiede beim Einsatz von Verschlüsselung in KMU. Während in einigen Branchen die KMU Verschlüsselungslösungen entsprechend ihrem Schutzbedarf einsetzen, liegt der Einsatz in anderen Branchen deutlich unter ihrem tatsächlichen Bedarf.

Für die Einführung und Nutzung von E-Mail-Verschlüsselung ist der fehlende Netzwerkeffekt weiterhin eines der Haupthemmnisse, den die KMU nannten. Es mangelt an Möglichkeiten, mit Geschäftspartnern und Kunden verschlüsselt zu kommunizieren. Dieses klassische Henne-Ei-Problem könnte auf der Endkundenebene durch intensivere Anstrengungen der großen E-Mail-Provider und Mailprogramm-Anbieter sowie auch der öffentlichen Hand (Behörden-Bürger-Kommunikation) deutlich verbessert werden. Eine stärkere Verbreitung im Privatkundenumfeld würde auch den Einsatz von verschlüsselter E-Mail-Kommunikation im Geschäftsverkehr fördern.

Rechtliche Analyse

Die Analyse der für KMU relevanten rechtlichen Vorgaben ergab, dass nur sehr wenige Vorschriften ausdrücklich zu einer Verschlüsselung von Daten verpflichten. Allerdings gibt es eine ganze Reihe von Normen, die allgemeine Anforderungen an den Schutz bestimmter – meist personenbezogener – Daten aufstellen. Zum Teil wird dabei eine Verschlüsselung beispielhaft genannt. Diese allgemeinen Vorgaben können sich in der Praxis aber zu einer Verschlüsselungspflicht verdichten. Weitere indirekte Verschlüsselungspflichten können sich aus dem zivilrechtlichen Haftungsrecht ergeben, weil die Sicherung unternehmenskritischer Daten etwa zu den Pflichten von Geschäftsleitern zu zählen ist.

Handlungsempfehlungen

Als Konsequenz aus den erhobenen Studienergebnissen könnte der Bund neben der Weiterentwicklung der Kommunikationsangebote der Behörden verstärkt als Vermittler zwischen den Stakeholdern im Markt agieren, um die Entwicklungen auf Marktseite weiter voranzubringen.

Der Bund könnte zudem im Dialog mit den kommerziellen Anbietern aus Deutschland eine Strategie entwickeln, mit der KMU-Unternehmen aktiv für die Nutzung deutscher PKI-Verschlüsselungsinfrastrukturen gewonnen werden. Unter einer einheitlichen Dachmarke könnten kommerzielle Anbieter von Vertrauensdiensten ein einheitliches Produkt anbieten, das sich speziell an den Bedürfnissen von KMU orientiert und insbesondere in der Einführungsphase durch eine attraktive Preisgestaltung oder kostenfreie Nutzung überzeugt. Ggf. ließen sich bestimmte Aspekte der Einführung auch über ein entsprechendes Bundesprogramm gezielt fördern.

Bei den Unternehmen, die keinerlei E-Mail-Verschlüsselung einsetzen, sollte eine stärkere Adressierung der Befürchtungen zu Komfortverlust/erhöhtem Bedienaufwand in der Vermarktungskommunikation erfolgen. IT-Dienstleister und Branchenverbände sollten ihr Engagement in Bezug auf Transparenz und Beratung zu bestehenden Lösungen und tatsächlichen Kosten verstärken.

Für die weitere Unterstützung der Verschlüsselung des Web-Traffics von KMU in Deutschland könnte der Bund die Einrichtung einer nicht-kommerziellen Zertifizierungsstelle fördern, die kostenlose TLS-Zertifikate an private Nutzer, nicht-kommerzielle Einrichtungen und kleine Unternehmen ausgibt.

Die begrenzte Nutzung teilweise kostenfreier On-board-/Software-Embedded-Technologien zur Datei- und Datenträgerverschlüsselung ist im Wesentlichen auf organisatorische Ursachen in den Unternehmen zurückzuführen. Dies könnte sowohl durch intensivere Branchenkommunikation zur Steigerung der Awareness als auch durch Sensibilisierung der IT-Dienstleister im KMU-Umfeld verbessert werden.

Als zentrale Unterstützungsmaßnahme des Bundes werden eine Online-Informationsplattform sowie die Entwicklung einer Marke zum Thema elektronische Verschlüsselung vorgeschlagen. Zugleich sollte das Thema Verschlüsselung als Aspekt innerhalb der nationalen Digitalisierungsstrategien des Bundes konkret benannt und in der Evaluation der laufenden Maßnahmen berücksichtigt werden.

Als zusätzlicher Treiber könnten rechtliche oder regulatorische Vorgaben dienen, die den Einsatz von Verschlüsselungslösungen vorschreiben oder zumindest empfehlenswert machen.

7 Anhang

7.1 Quellen

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, 2014, zitiert: Arbeitskreise Technik und Medien, Orientierungshilfe – Cloud Computing

Arbeitskreise Technik und Medien, Orientierungshilfe – Cloud Computing, Version 2.0, Stand 9.10.2014

Arndt, Hans-Wolfgang / Fetzer, Thomas / Scherer, Joachim / Graulich, Kurt, TKG – Telekommunikationsgesetz, 2. A., 2015, zitiert: Bearbeiter, in: Arndt/Fetzer

Auer-Reinsdorff, Astrid / Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 2. A., 2016, zitiert: Bearbeiter, in: Auer-Reinsdorff/Conrad

Auernhammer, Herbert, BDSG – Bundesdatenschutzgesetz und Nebengesetze, 4. A., 2014

Backu, Frieder, ITRB 2003, 251, Pflicht zur Verschlüsselung?

Baumbach, Adolf / Hueck, Alfred, Gesetz betreffend die Gesellschaften mit beschränkter Haftung, 21. A, 2017, zitiert: Bearbeiter, in: Baumbach/Hueck

BayLDA, 7. Tätigkeitsbericht 2015/2016, zitiert: BayLDA, Tätigkeitsbericht 2015/2016

Bergt, Matthias, CR 2014, 726, Verschlüsselung nach dem Stand der Technik als rechtliche Verpflichtung

BfDI, 23. Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010, zitiert: BfDI, Tätigkeitsbericht 2009/2010

BfDI, 24. Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012, zitiert: BfDI, Tätigkeitsbericht 2011/2012

BfDI, 25. Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014, zitiert: BfDI, Tätigkeitsbericht 2013/2014

BfDI, 26. Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014, zitiert: BfDI, Tätigkeitsbericht 2015/2016

BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, zitiert: BMI, KRITIS-Strategie

BSI, Diskussionspapier „Absicherung von Telemediendiensten nach Stand der Technik", 2016, zitiert: BSI, Diskussionspapier

BSI, Technische Richtlinie des BSI, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1

Büscher, Wolfgang / Dittmer, Stefan / Schiwy, Peter, Gewerblicher Rechtsschutz, Urheberrecht, Medienrecht, 2. A., 2011, zitiert: Bearbeiter, in: Büscher/Dittmer/Schiwy

Conrad, Isabell / Huppertz, Peter, Bearbeiter, in: Auer-Reinsdorff/Conrad

Conrad, Isabell, Bearbeiter, in: Auer-Reinsdorff/Conrad

Dauber-Lieb, Barbara, Bearbeiter, in: Henssler/Strohn

Dix, Alexander, Bearbeiter, in: Simitis

Djeffal, Christian, Neue Sicherungspflicht für Telemediendiensteanbieter - Webseitensicherheit jetzt Pflicht nach dem IT-Sicherheitsgesetz, MMR 2015, 716

Eckhardt, Jens, Bearbeiter, in: Beck'scher TKG-Kommentar

Eckhardt, Jens, DuD 2008, 330, Rechtliche Grundlagen der IT-Sicherheit

Ernestus, Walter, Bearbeiter, in: Simitis

Fleischer, Holger, Bearbeiter, in: Spindler/Stilz

Franck, Lorenz, ZD 2016, 324, Verlust und Fund von Datenspeichern – Zivil- und datenschutzrechtliche Pflichten für Verlierer, Finder und Fundbüros

Gabel, Detlev, Bearbeiter, in: Taeger/Gabel

Geppert, Martin / Schütz, Raimund, Beck'scher TKG-Kommentar, 4. A., 2013, zitiert: Bearbeiter, in: Beck'scher TKG-Kommentar

Gerlach, Carsten, Sicherheitsanforderungen für Telemediendienste - der neue § 13 Abs. 7 TMG, CR 2015, 581

Gola, Peter / Schomerus, Rudolf, BDSG – Bundesdatenschutzgesetz, 12. A., 2015, zitiert: Gola/Schomerus

Grages, Jan-Michael, Bearbeiter, in: Plath

Graulich, Kurt, Bearbeiter, in: Arndt/Fetzer

Grentzenberg, Verena / Schreibauer, Marcus / Schuppert, Stefan, K&R 2009, 368, Die Datenschutznovelle (Teil 1) – Ein Überblick zum „Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften"

Grüneberg, Christian, Bearbeiter, in: Palandt

Haas, Ullrich / Ziemons, Hildegard, Bearbeiter, in: Beck'scher Online-Kommentar GmbHG

Haas, Ullrich / Ziemons, Hildegard, Bearbeiter, in: Michalski

Hauck, Ronny, NJW 2016, 2218, Geheimnisschutz im Zivilprozess – Was bringt die neue EU-Richtlinie für das deutsche Recht

Hauschka, Christoph / Moosmayer, Klaus / Lösler, Thomas, Corporate Compliance, 3. A., 2016, zitiert: Bearbeiter, in: Hauschka/Moosmayer/Lösler

Heinemeyer, Dennis / Kreitlow, Matthias, MMR 2013, 623, Umgehung technischer Schutzmaßnahmen von Medienangeboten – Rechtmäßige Nutzung von Streaming-Technologie und Wirksamkeit des RTMPE gem. § 95a UrhG

Henssler, Martin / Strohn, Lutz, Gesellschaftsrecht, 3. A., 2016, zitiert: Bearbeiter, in: Henssler/Strohn

Herbst, Tobias, Bearbeiter, in: Auernhammer

Herchenbach-Canarius, Judith / Illies, Georg / Lochter, Manfred / Sommer, Antonius / Stein, Oliver, Bearbeiter, in: Kilian/Heussen

Hölters, Wolfgang, Aktiengesetz, 2. A., 2014, zitiert: Bearbeiter, in: Hölters

Hölters, Wolfgang, Bearbeiter, in: Hölters

Hornung, Gerrit, NJW 2010, 1841, Informationen über „Datenpannen"- Neue Pflichten für datenverarbeitende Unternehmen

Hüffer, Uwe / Koch, Jens, Aktiengesetz, 12. A., 2016, zitiert: Bearbeiter, in: Hüffer/Koch

Hüffer, Uwe, Bearbeiter, in: Hüffer/Koch

Hullen, Nils / Roggenkamp, Jan Dirk, Bearbeiter, in: Plath

Hullen, Nils, Bearbeiter, in: Plath

Jenny, Valerian, Bearbeiter, in: Plath

Killian, Wolfgang / Heussen, Benno, Computerrechts-Handbuch, 32. A., 2013, zitiert: Kilian/Heussen

Klett, Detlef / Lee, Sang-Woon, CR 2008, 644, Vertraulichkeit des E-Mailverkehrs

Koch, Alexander, DuD 2014, 691, Rechtliche und ethische Verschlüsselungspflichten? – Am Beispiel der Rechtsanwaltschaft

Koch, Alexander, RTkom 2001, 217, Das strafbewehrte Abhörverbot nach § 86 TKG

Koch, Alexander, Strafrechtliche Probleme des Angriffs und der Verteidigung in Computernetzen, 2008, zitiert: Koch, Angriff und Verteidigung

Koch, Alexander, Verschlüsselung in der beruflichen und privaten Praxis – Schritt für Schritt zu verschlüsselten E-Mails und Daten, 2014, zitiert: Koch, Verschlüsselungspraxis

Koch, Jens, Bearbeiter, in: Hüffer/Koch

Köhler, Helmut / Bornkamm, Joachim, Gesetz gegen den unlauteren Wettbewerb – UWG – Preisangabenverordnung – Unterlassungsklagengesetz – Dienstleistungs-Informationspflichten-Verordnung, 35. A., 2017, zitiert: Bearbeiter, in: Köhler/Bornkamm

Köhler, Helmut, Bearbeiter, in: Köhler/Bornkamm

Kommission Arbeitsschutz und Normung, Rechtsprechung zu technischen Normen und normenähnlichen Dokumenten hinsichtlich ihrer Bedeutung für Sicherheit und Gesundheitsschutz, 2016

Koós, Clemens, MMR 2016, 224, Die europäische Geschäftsgeheimnis- Richtlinie - ein gelungener Wurf?

LDI Berlin, Datenschutz und Informationsfreiheit – Bericht 2012, zitiert: LDI Berlin, Jahresbericht 2012

LDI Berlin, Datenschutz und Informationsfreiheit – Bericht 2013, zitiert: LDI Berlin, Jahresbericht 2013

LDI Berlin, Datenschutz und Informationsfreiheit – Bericht 2014, zitiert: LDI Berlin, Jahresbericht 2014

LDI NRW, Datenschutz und Informationsfreiheit – 23. Bericht 2017, zitiert: LDI NRW, Bericht 2017

Lehmler, Lutz, Bearbeiter, in: Büscher/Dittmer/Schiwy

LfD Bayern, 25. Tätigkeitsbericht Berichtszeitraum 2011/2012, zitiert: LfD Bayern, Tätigkeitsbericht 2011/2012

LfD Bayern, 26. Tätigkeitsbericht Berichtszeitraum 2013/2014, zitiert: LfD Bayern, Tätigkeitsbericht 2013/2014

Lurz, Hanna / Scheben, Barbara / Dolle, Wilhelm, BB 2015, 2755, Das IT-Sicherheitsgesetz: Herausforderungen und Chancen für Unternehmen – vor allem für KMU

Marschall, Kevin, DuD 2015, 183, Datenpannen – „neue" Meldepflicht nach der europäischen DS-GVO? – Rechtliche Änderungen durch Art. 31 und Art. 32 DS-GVO

Michalski, Lutz, Kommentar zum Gesetz betreffend die Gesellschaften mit beschränkter Haftung, 2. A., 2010, zitiert: Bearbeiter, in: Michalski

Moos, Flemming, Bearbeiter, in: Taeger/Gabel

Mozek, Martin, Bearbeiter, in: Säcker

Müller-Michaels, Olaf, Bearbeiter, in: Hölters

Münchener Kommentar zum Aktiengesetz, 4. A., 2014, zitiert: Bearbeiter, in: Münchener Kommentar zum AktG

Musielak, Hans-Joachim / Hau, Wolfgang, Grundkurs BGB, 14. A., 2015

Oetker, Hartmut, Bearbeiter, in: Henssler/Strohn

Palandt, Otto, Bürgerliches Gesetzbuch, 76. A., 2017, zitiert: Bearbeiter, in: Palandt

Plath, Kai- Uwe, Bearbeiter, in: Plath

Plath, Kai-Uwe, BDSG/DSGVO – Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen von TMG und TKG, 2. A., 2016, zitiert: Bearbeiter, in: Plath

Röhrborn, Stefan / Lang, Valentin, BB 2015, 2357, Zunehmend sorgloser Umgang mit mobilen Geräten - ein unbeherrschbares Risiko für den Arbeitgeber?

Säcker, Franz Jürgen, TKG – Telekommunikationsgesetz, 3. A., 2013, zitiert: Bearbeiter, in: Säcker

Scherer, Josef / Fruth, Klaus, CZZ 2015, 9, Der Einfluss von Standards, Technikklauseln und des „Anerkannten Standes von Wissenschaft und Praxis" auf Organhaftung und Corporate Governance – am Beispiel der ISO 19600 (2015) Compliance-Managementsystem

Schmidl, Michael, Bearbeiter, in: Büscher/Dittmer/Schiwy

Schmidl, Michael, Bearbeiter, in: Hauschka/Moosmyer/Lösler

Schultze-Melling, Jyn, Bearbeiter, in: Taeger/Gabel

Schuppenhauer, Rainer, GoDV-Handbuch – Grundsätze ordnungsmäßiger Datenverarbeitung und DV-Revision, 6. A., 2007, zitiert: Schuppenhauer

Simitis, Spiros, Bundesdatenschutzgesetz, 8. A., 2014

Spindler, Gerald / Schuster, Fabian, Recht der elektronischen Medien, 3. A., 2015, zitiert: Bearbeiter, in: Spindler/Schuster

Spindler, Gerald / Stilz, Eberhard, Kommentar zum Aktiengesetz, 3. A., 2015, zitiert: Bearbeiter, in: Spindler/Stilz

Spindler, Gerald, Bearbeiter, in: Münchener Kommentar zum AktG

Spindler, Gerald, Bearbeiter, in: Spindler/Schuster

Stiemerling, Oliver / Hartung, Jürgen, CR 2012, 60, Datenschutz und Verschlüsselung – Wie belastbar ist Verschlüsselung gegenüber dem Anwendungsbereich des Datenschutzrechts?

Taeger, Jürgen / Gabel, Detlev, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. A., 2013, zitiert: Bearbeiter, in: Taeger/Gabel

Trappehl, Bernhard / Schmidl, Michael, NZA 2009, 985, Arbeitsrechtliche Konsequenzen von IT-Sicherheitsverstößen

ULD Schleswig-Holstein, Tätigkeitsbericht 2011 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, zitiert: ULD Schleswig-Holstein, Tätigkeitsbericht 2011

ULD Schleswig-Holstein, Tätigkeitsbericht 2015 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, zitiert: ULD Schleswig-Holstein, Tätigkeitsbericht 2015

von Holleben, Kevin Max / Menz, Monika, CR 2010, 63, IT-Risikomanagement - Pflichten der Geschäftsleitung

Weidenkaff, Walter, Bearbeiter, in: Palandt

Withus, Karl Heinz, CZZ 2015, 139, Die Angemessenheit eines CMS – eine rein juristische Bewertung oder anerkannter Stand von betriebswirtschaftlichen Grundsätzen?

Ziemons, Hildegard / Jaeger, Carsten, Beck'scher Online-Kommentar zum GmbHG, 28. Edition, 2016, zitiert: Bearbeiter, in: Beck'scher Online-Kommentar GmbHG

Zöllner, Wolfgang / Noack, Ullrich, Bearbeiter, in: Baumbach/Hueck

7.2 Abkürzungen

a. a. O.	am angegebenen Ort
Abs.	Absatz
aE	am Ende
AES	Advanced Encryption Standard
AG	Aktiengesellschaft / Arbeitsgericht
Art.	Artikel
Az.	Aktenzeichen
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BDSG	Bundesdatenschutzgesetz
Beschl.	Beschluss
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImSchG	Bundes-Immissionsschutzgesetz
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
bzw.	beziehungsweise
d. h.	das heißt
DIMDI	Das Deutsche Institut für Medizinische Dokumentation und Information
DIN	Deutsches Institut für Normung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
ESB	Elektronische Schnittstelle Behörden
etc.	et cetera
ETSI	European Telecommunications Standards Institute

EU	Europäische Union
f./ff.	folgende
FG	Finanzgericht
Fn.	Fußnote(n)
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GoDV	Grundsätze ordnungsgemäßer Datenverarbeitung
HTTPS	Hypertext Transfer Protocol Secure
i. S. d.	im Sinne der / im Sinne des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IMAP	Internet Message Access Protocol
ISO	International Organization for Standardization
IT	Informationstechnik
KG	Kommanditgesellschaft
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRITIS	Kritische Infrastruktur(en)
LDI Berlin	Berliner Beauftragte für Datenschutz und Informationsfreiheit
LDI NRW	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfD Bayern	Bayerischer Landesbeauftragter für den Datenschutz
lit.	litera (Buchstabe)
Nr.	Nummer
OHG	Offene Handelsgesellschaft
OVG	Oberverwaltungsgericht
PGP	Pretty Good Privacy
POP3	Post Office Protocol version 3
Rn.	Randnummer(n)
RTMPE	Encrypted Real Time Messaging Protocol
S.	Seite(n)

SGB	Sozialgesetzbuch
SMTP	Simple Mail Transfer Protocol
SSL/TLS	Secure Sockets Layer/ Transport Layer Security
StGB	Strafgesetzbuch
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.	und
u. a.	und andere / unter anderem
UAbs.	Unterabsatz
ULD Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UrhG	Urheberrechtsgesetz
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom
VG	Verwaltungsgericht
vgl.	vergleiche
VwZG	Verwaltungszustellungsgesetz
WLAN	Wireless Local Area Network
WWW	World Wide Web
z. B.	zum Beispiel
ZPO	Zivilprozessordnung