GOLDMEDIA

if(is) internet-sicherheit.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

EINSATZ VON ELEKTRONISCHER VERSCHLÜSSELUNG – HEMMNISSE FÜR DIE WIRTSCHAFT

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

Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft

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

– Kurzfassung –

Datum: 22.02.2018

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 Skizze des Untersuchungsganges

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 Methodisches Vorgehen

In einem ersten, vorbereitenden Schritt wurde 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.

Die **Analyse der spezifischen Hemmnisse und Motivationsgründe beim Einsatz von Verschlüsselungslösungen** in KMU erfolgte auf Basis einer im Anschluss durchgeführten, 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.

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 Erzielte Stichprobe

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

- In Summe konnten 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).

2 Wesentliche Ergebnisse der Unternehmensbefragung

2.1 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:

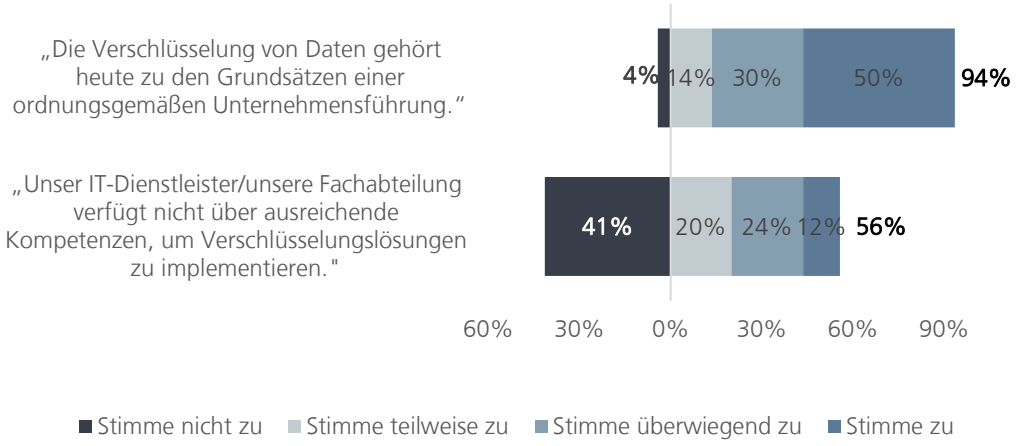
- Schutzbedarf des Unternehmens und der Branche
- Allgemeine Aspekte der Verschlüsselung
- Konkrete Nutzung von Verschlüsselung im Unternehmen
- Motivationsgründe und Hemmnisse bei der Nutzung

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

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

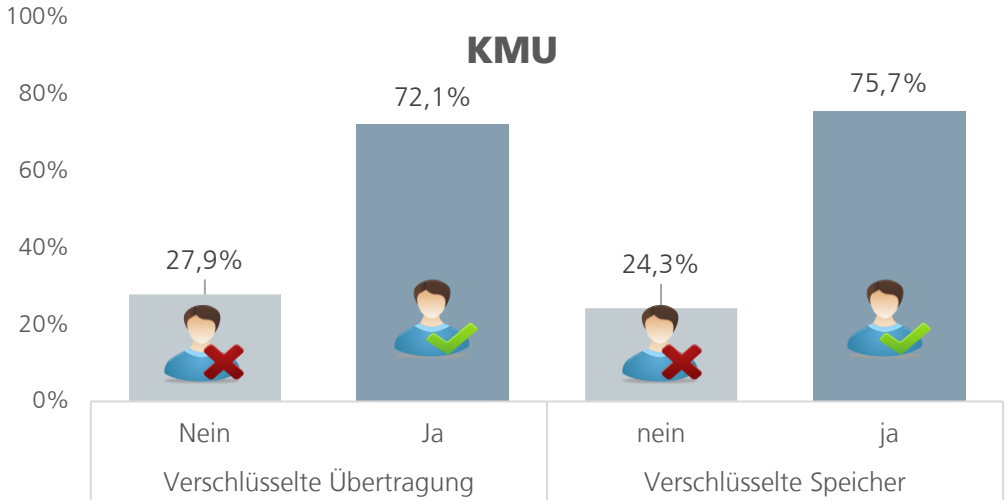


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=140.
Frage: Inwiefern können Sie folgenden Thesen zur generellen Bedeutung von Verschlüsselung in Ihrem Unternehmen zustimmen?

2.3 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 **deutliche Unterschiede zwischen KMU und Großunternehmen**.

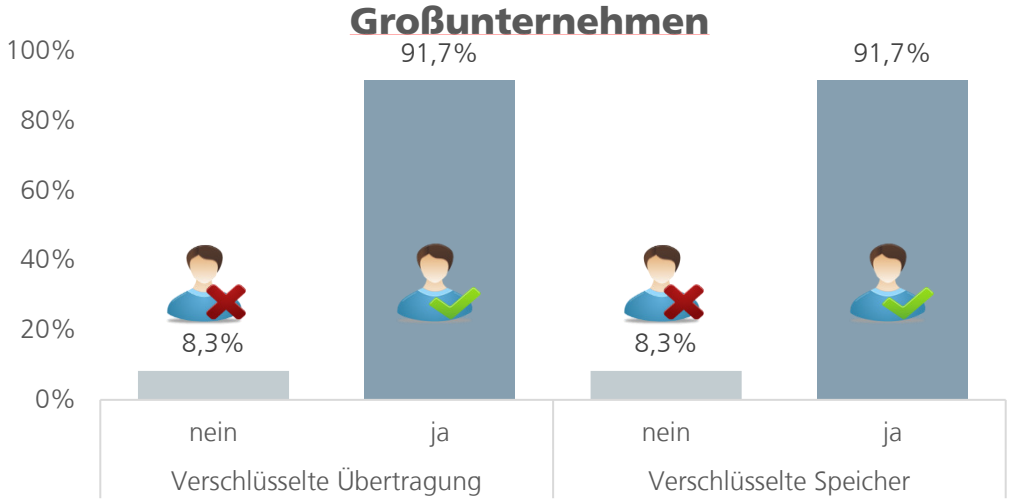
Abb. 2: Anteil der KMU, die Verschlüsselung einsetzen



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.[1]

Abb. 3: Anteil der Großunternehmen mit Verschlüsselung

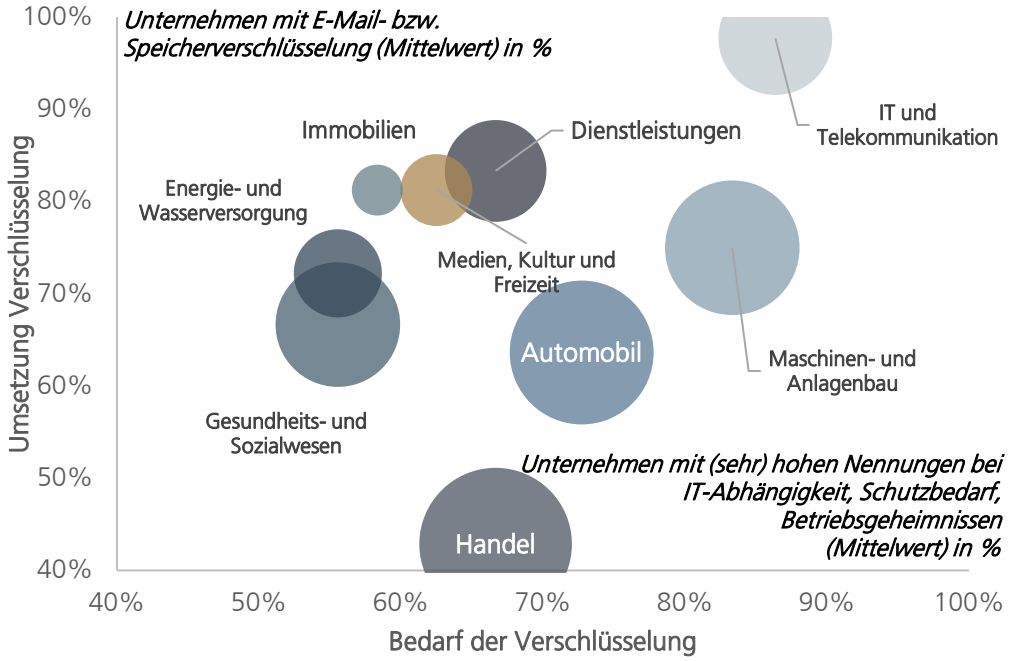


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=72.

[1] 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. 4 Mapping der Branchen nach Verschlüsselungsbedarf und Verschlüsselungsumsetzung (KMU), in Prozent



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

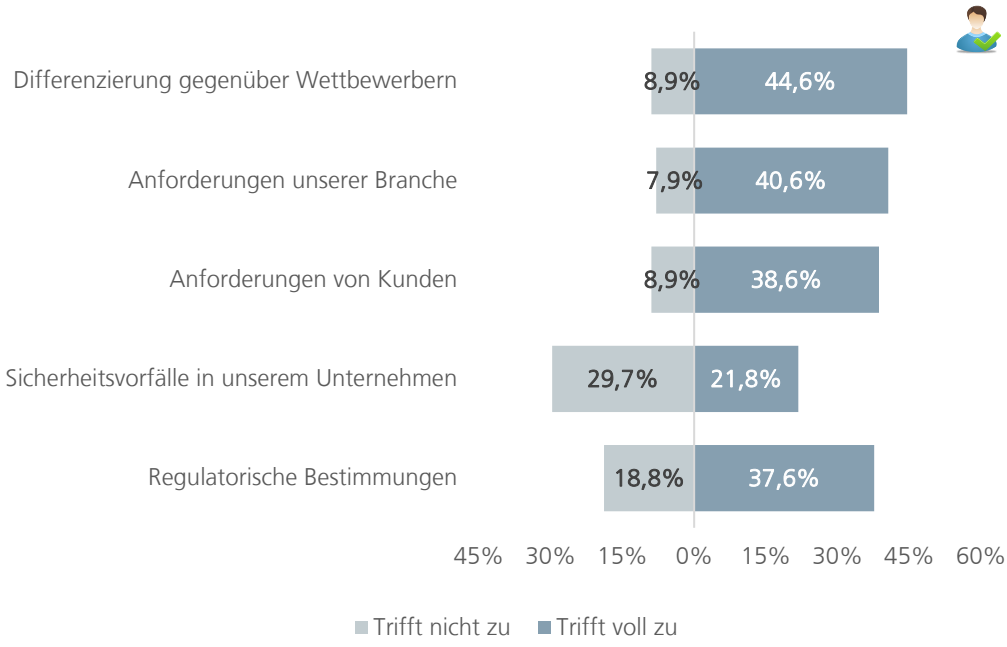
- Die **IT- und Telekommunikationsbranche** gibt einen sehr hohen IT-Reifegrad an und weist zugleich auch einen **sehr hohen Umsetzungsstand** bei der Verschlüsselung auf.
- KMU in der **Automobil- sowie Maschinen- und Anlagenbaubranche** weisen einen relativ hohen IT-Reifegrad und hohe IT-Abhängigkeit 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**.

2.4 Einsatz von Kommunikationsverschlüsselung

2.4.1 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.

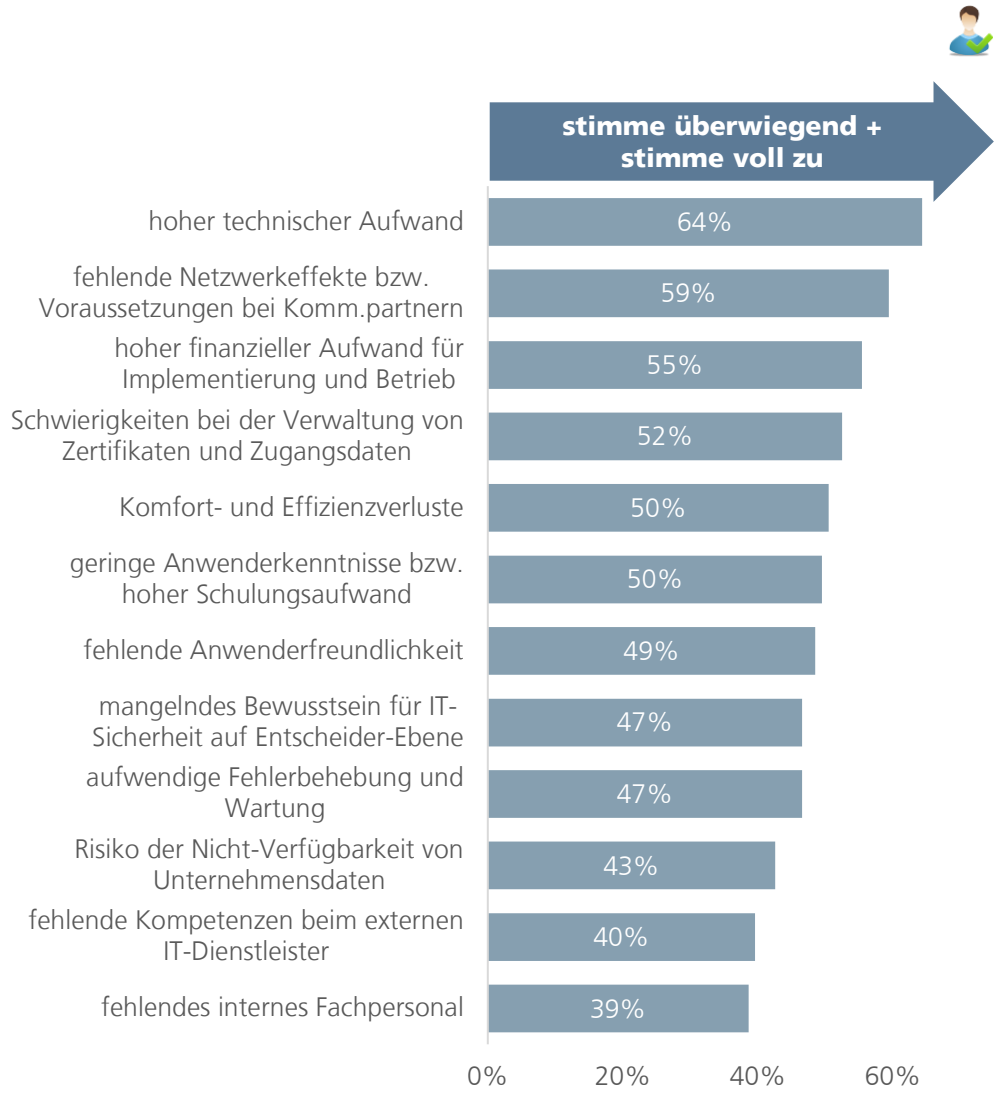
Abb. 5 Anwender von Kommunikationsverschlüsselung in KMU: Gründe für den Einsatz



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.

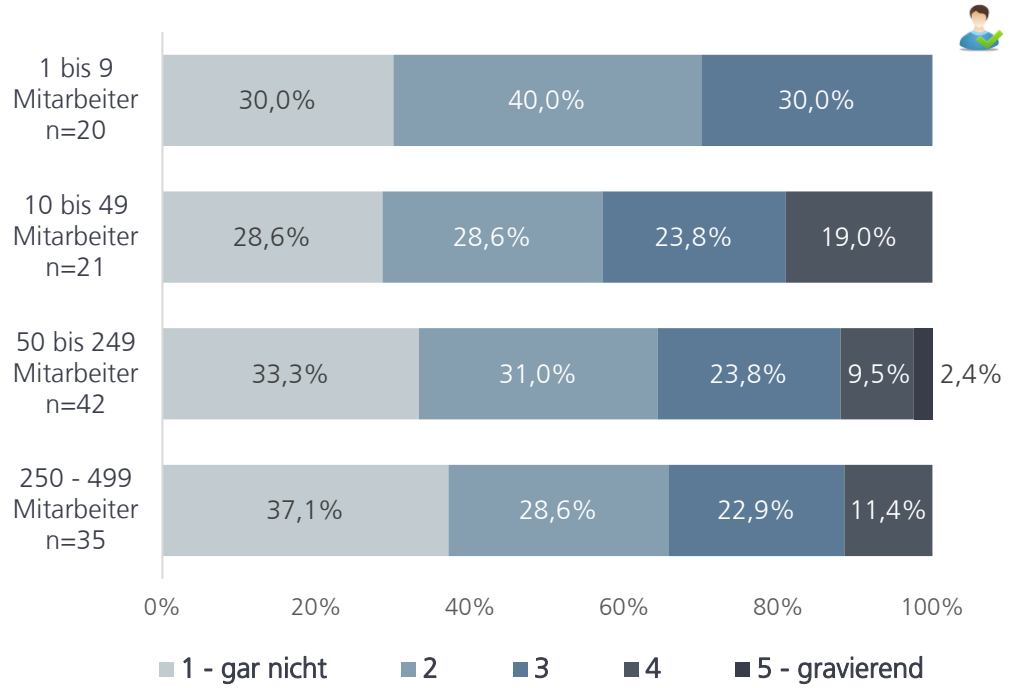
Abb. 6 Herausforderungen bei der Einführung von Kommunikationsverschlüsselung in KMU



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?

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. 7 Komfort- Produktivitätsverluste beim Einsatz von Verschlüsselung bei KMU



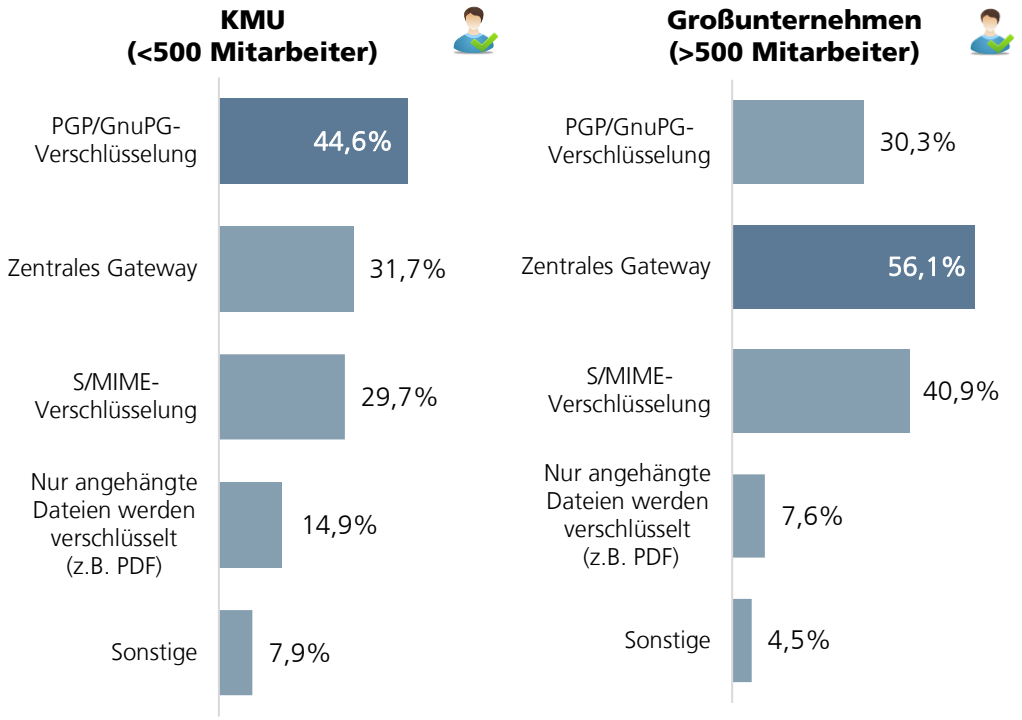
Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=118. Frage: Kam es aufgrund des Einsatzes von Verschlüsselung zu Komfort- und Produktivitätsverlusten?

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.

2.4.2 Einsatz von E-Mail-Verschlüsselung

Laut der Umfrageergebnisse nutzen 72 Prozent der KMU verschlüsselte Übertragungswege (vgl. Abb. 2), 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. 8 Genutzte E-Mail-Verschlüsselungslösungen

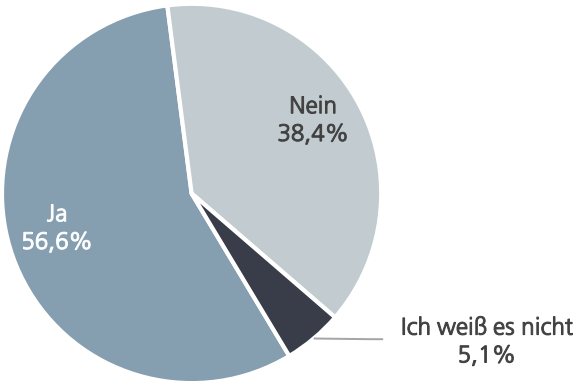


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=101 KMU; n=66 Großunternehmen; Mehrfachantworten. Frage: Welche Verschlüsselungsart nutzen Sie beim E-Mail-Versand Ihrer Daten?

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.

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

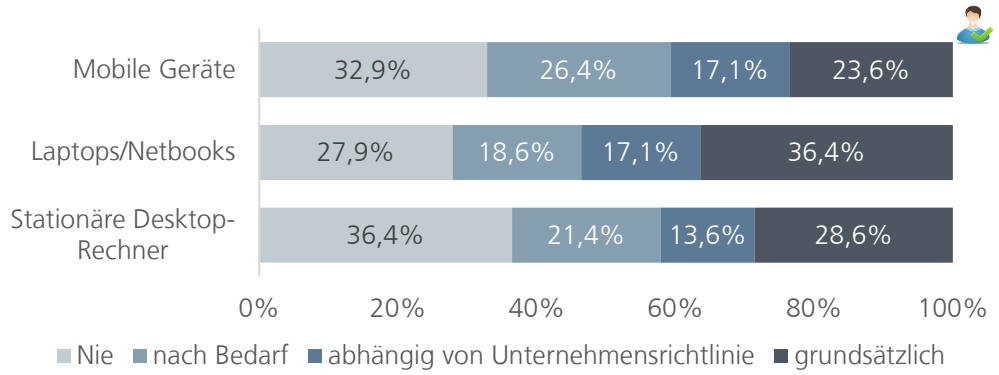


Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=99. Frage: Können Sie verschlüsselte E-Mails auch auf Ihrem Smartphone/Tablet nutzen?

2.5 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.

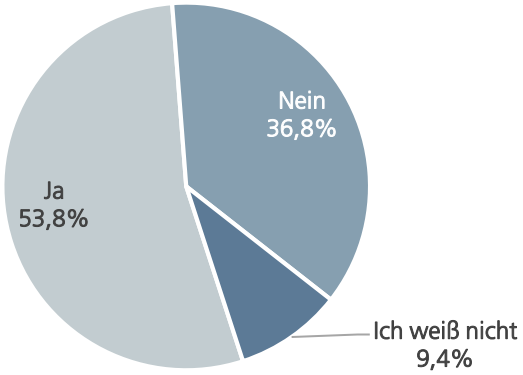
Abb. 10 Einsatz von Geräteverschlüsselung bei verschiedenen Gerätegruppen bei KMU



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. 11 Unternehmensrichtlinie zur Datenspeicherung bei KMU, die über Datenverschlüsselung verfügen



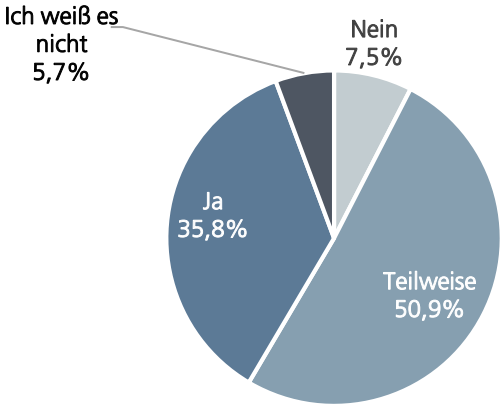
Quelle: Goldmedia/if(is)-Befragung „Einsatz von elektronischer Verschlüsselung" 2017; n=106. Frage: Existiert eine interne Unternehmensrichtlinie (Compliance), welche die verschlüsselte Datenspeicherung regelt?

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.

2.6 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.

Abb. 12 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?

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

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.

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.

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

Abb. 13 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?

3 Wesentliche Ergebnisse der rechtlichen Analyse

3.1 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.

3.1.1 Allgemeines

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

1. ausdrückliche Verschlüsselungspflichten,
2. Verschlüsselungsobliegenheiten,
3. Generalklauseln,
4. behördliche Vorgaben,
5. Ausbildung *(nicht Bestandteil dieser Zusammenfassung)*

3.2 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.

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.

3.3 Verschlüsselungsobliegenheiten und Hinweispflichten

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.[2] Unter einer Verschlüsselungsobliegenheit werden deshalb im Folgenden gesetzliche Regelungen verstanden, die zwar Bezug auf eine Verschlüsselung nehmen, eine solche aber nicht zwingend vorschreiben.

3.3.1 Datenschutzrecht[3]

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.

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. 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.

---

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

3 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.

3.3.2 Benachrichtigungs- und Meldepflichten

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 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.[4] 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.[5]

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.

3.3.3 Schutz von Betriebs- und Geschäftsgeheimnissen

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.

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

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

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.

3.4 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.

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 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.

3.5 Behördliche Vorgaben

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 Handlungsempfehlungen

4.1 Generelle Unterstützungsmaßnahmen

4.1.1 Verbände und Anbieter: Markttransparenz steigern durch zielgerichtete Angebote

- 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.
- 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.
- Bessere Markttransparenz für KMU-Lösungen zur Verschlüsselung schaffen: Marktplätze und Anbieterverzeichnisse zu Produkten der IT-Sicherheit müssten stärker auf das Thema Verschlüsselung zugeschnitten und ggf. um Ausschreibungsunterstützung oder Vermittlungsfunktionalitäten für indikative Angebote ergänzt werden. Hierbei sollte eine offensive Preis- und Aufwandskommunikation der Hersteller stattfinden, da Unternehmen ohne Verschlüsselungslösungen hohe Kosten für Implementierung und Betrieb erwarten.
- Ein Förderprogramm, das gutscheinbasiert Orientierungsberatungen für KMU vorsieht, kann hierbei für die notwendige Transmission der Inhalte in die Unternehmen sorgen. 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.
- 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.
- 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. Branchenverbände könnten entsprechende Musterrichtlinien/Compliance-Vorgaben als Handreichung veröffentlichen.

4.1.2 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.

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.

4.2 Konkrete Maßnahmen zur Förderung der E-Mail-Verschlüsselung

4.2.1 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). Sämtliche Komponenten zur Nutzung von PGP/GnuPG stehen als freie Plugin-Software für verschiedene Mailprogramme zur Verfügung.

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.[6] 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. In Bezug auf die bestehenden

6 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.

Verschlüsselungsdesiderate ist vor allem die fehlende Integration von E-Mail-Verschlüsselung in mobile Plattformen zu nennen. 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.

4.2.2 Dialog mit führenden E-Mail-Client-Herstellern führen

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. 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.

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.

4.2.3 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. 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.

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.

4.2.4 Vision einer vollständig integrierte, automatisierte Verschlüsselungslösung

Eine globale, nativ integrierte Verschlüsselungslösung, mit der sich ohne großes Wirken und Vorwissen der Nutzer automatisiert E-Mails ver- und entschlüsseln lassen, wäre wünschenswert. Die Schlüsselverwaltung und der sicherere 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.

4.2.5 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.

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.

4.3 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.

Es besteht 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.

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 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 solche 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.

5 Fazit

Auf Basis der Studienergebnisse 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 Verschlüsselung des HTTP-Webtraffics

Der Bund könnte 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.