Neue Gesetze schreiben Datenverschlüsselung vor

# Mit der Keule

**Klaus Schmeh, Udo Wichert**

Nachdem zahlreiche Appelle nicht gefruchtet haben, sollen nun Gesetze und EU-Verordnungen erzwingen, dass sensible Daten endlich verschlüsselt werden. Nahezu jedes Unternehmen und jede Behörde wird von den diversen Vorschriften betroffen sein.

„Eine E-Mail ist wie eine Postkarte, denn sie kann von Unbeteiligten gelesen werden." Diesen Spruch hat wohl jeder schon einmal gehört, der sich auch nur im Entferntesten mit IT-Sicherheit beschäftigt hat. Die Lösung ist seit einem Vierteljahrhundert bekannt: Verschlüsselung. Dumm nur, dass kaum jemand diese Technik nutzt [1]. Nach Untersuchungen der Westfälischen Hochschule ist gerade einmal jede fünfundzwanzigste E-Mail verschlüsselt. Wenn es um Dateiverschlüsselung geht, sieht die Sache nicht viel besser aus.

Nachdem die zahllosen Appelle von IT-Sicherheitsexperten, man solle doch endlich seine Daten verschlüsseln, nicht gefruchtet haben, hat sich inzwischen der Gesetzgeber eingeschaltet. Getreu dem Motto „Wer nicht hören will, muss fühlen" läuft momentan ein halbes Dutzend gesetzlicher Vorhaben, die das Verschlüsseln bestimmter Daten vorschreiben. Bei Zuwiderhandlung drohen im Extremfall sogar Haftstrafen.

Dass die Freiwilligkeit beim Verschlüsseln nun ein Ende haben soll, liegt – wenn auch nicht ausschließlich – an Whistleblower Edward Snowden. Dieser hatte als Administrator bei der NSA Zugriff auf zahlreiche Daten, die ihn inhaltlich nichts angingen, und konnte durch deren Verrat der NSA einen enormen Schaden zufügen (und allen anderen einen großen Dienst erweisen). Die zahlreichen Sicherheitsmaßnahmen, die die NSA getroffen hatte, liefen ins Leere, da Snowden diese im Rahmen seines Administratorenjobs umgehen konnte. Dabei ist durchaus bekannt, dass ein Großteil aller Angriffe auf die IT-Sicherheit von innen kommt – nicht nur bei der NSA. Mit Verschlüsselung könnte man vieles verhindern, wenn sie denn genutzt werden würde.

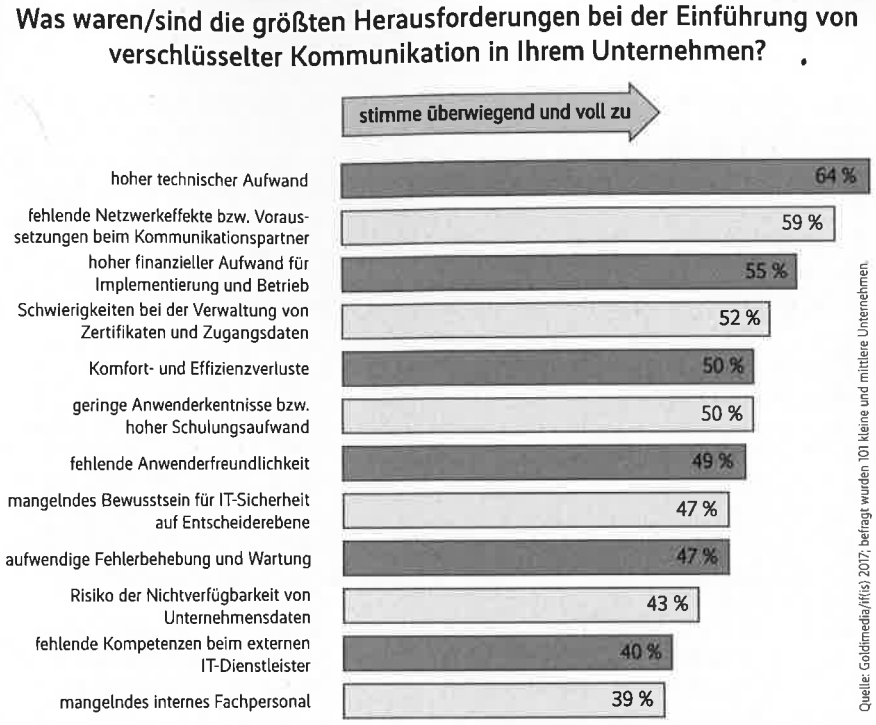
## StGB: Das Schweigen der Berufsgeheimnisträger

Eine Verschlüsselungspflicht hat der Gesetzgeber beispielsweise für Berufsgeheimnisträger wie Rechtsanwälte, Patentanwälte, Notare, Wirtschaftsprüfer und Steuerberater eingeführt. Diese findet sich im Ende 2017 neugefassten § 203 des Strafgesetzbuchs. Er trägt die Überschrift „Verletzung von Privatgeheimnissen". § 203 gilt zwar laut dem ersten Abschnitt auch für Ärzte, Apotheker und andere Heilberufe, doch für diese gibt es inzwischen mit dem E-Health-Gesetz (siehe unten) eine eigene Vorschrift, die Vorrang hat.

Die Neufassung von § 203 ermöglicht es den betroffenen Berufsgruppen, digitale Daten auszulagern (insbesondere in die Cloud). Allerdings müssen sie diese Informationen schützen. Dies ist de facto nur durch Verschlüsselung möglich, auch wenn dieser Begriff im Gesetz nicht wörtlich vorkommt. Hierbei gilt eine Beweislastumkehr: Anwälte, Notare, Wirtschaftsprüfer und Steuerberater müssen belegen, dass sie die notwendigen Sicherheitsmaßnahmen inklusive Verschlüsselung getroffen haben. Können sie dies nicht, drohen empfindliche Strafen, im Höchstfall ein Jahr Gefängnis. Da Rechtsanwälte häufig mit der Polizei, Detekteien, Gerichtsvollziehern und ähnlichen Einrichtungen kommunizieren, wird man sich auch dort mit den entsprechenden Verschlüsselungsmaßnahmen auseinandersetzen müssen.

**iX-TRACT**

- Gleich mehrere Gesetze sollen sicherstellen, dass sich das Verschlüsseln sensibler Daten endlich durchsetzt.
- Bei Nichtbeachtung drohen empfindliche Schadenersatzforderungen und Strafen – bis hin zu Gefängnisstrafen.
- Die Umsetzung der Gesetze ist noch im Gange. Meist ist noch unklar, welche Technik sich durchsetzen wird.




**Es gibt viele Gründe, warum sich das Verschlüsseln in Unternehmen (hier: KMU) noch nicht durchgesetzt hat. Neue Gesetze sollen das nun ändern (Abb. 1).**

Wie genau der neugefasste § 203 in die Praxis umgesetzt wird, ist noch unklar. Eine entscheidende Rolle wird voraussichtlich die DATEV spielen, die bekanntlich als IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte fungiert. Spezialisten entwickeln derzeit Konzepte zu den neuen Vorschriften, die auch Verschlüsselung vorsehen werden. Es steht zu erwarten, dass eine Empfehlung der DATEV wohl zum De-facto-Standard werden wird, selbst wenn sie nicht bindend ist und obwohl nicht alle vom Gesetz betroffenen Einrichtungen Mitglied der DATEV sind.

## Das leidige Thema E-Mail

Besonderes Augenmerk müssen Berufsgeheimnisträger auf das Thema E-Mail legen. Geeignete Produkte gibt es zwar seit über 20 Jahren, doch so richtig durchgesetzt hat sich das Verschlüsseln der elektronischen Post auch bei Anwälten und Notaren nie. Am einfachsten wäre es, auf die Kryptofunktionen von Outlook oder Notes zu setzen – doch im deutschen Rechtswesen wird man sich wohl kaum auf Verschlüsselungstechnik aus dem Lande der NSA verlassen. Auch E-Mail-Krypto-Gateways, die im Backend verschlüsseln, kommen nicht infrage, da Ende-zu-Ende-Verschlüsselung ein Muss ist. So bleiben nur noch E-Mail-Krypto-Plug-ins, von denen es mehrere am Markt gibt (beispielsweise Gpg4win, GreenShield oder das Outlook-Privacy-Plug-in). Interessant ist hierbei vor allem die Frage, ob die DATEV PGP oder S/MIME als Format für verschlüsselte E-Mails bevorzugt. Beides ist denkbar.

Ein weiterer Knackpunkt ist das Thema verschlüsseltes Telefonieren. Es gehört traditionell zu den Sorgenkindern unter den Kryptoanwendungen. Außer im Hochsicherheitsbereich (etwa beim Militär) hat die Sprachverschlüsselung jedoch bisher Exotenstatus. Lösungen, die auf GSM-, UMTS- oder LTE-Ebene verschlüsseln, existieren praktisch nicht. Die Produkte SecuSUITE (von SecuSmart) und SimKo 3 (von der Deutschen Telekom), die sich um den Titel „Merkelphone" streiten, sind daher als gehärtete Smartphones realisiert, die Datenverbindungen zur Sprachübertragung nutzen. Diese Hochsicherheitsprodukte sind jedoch für die breite Masse viel zu teuer.

Voraussichtlich werden die Berufsgeheimnisträger daher mit einer geeigneten App auf einem ungehärteten Smartphone verschlüsselt telefonieren müssen. Entsprechende Lösungen gibt es beispielsweise von T-Systems (Mobile Encryption App), Vodafone (Secure Call App) und certgate (cgPhone). Auch für das Verschlüsseln von Chats sind verschiedene Produkte auf dem Markt. Dem Marktführer WhatsApp, der seine Server in den USA stehen hat, wird man nicht trauen. Teamwire und das bereits erwähnte cgPhone zählen zu den Alternativen.

## Für viele ein Schreckgespenst: die DSGVO

Die mit Abstand bekannteste Vorschrift, die Verschlüsselung einfordert, ist die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union. Nicht zuletzt durch die zahlreichen Cookie-Warnungen und „Wollen Sie auf dem Verteiler bleiben?"-E-Mails dürfte inzwischen jeder von dieser Verordnung gehört haben. Während § 203 des Strafgesetzbuchs nur einige wenige Berufsgruppen betrifft, müssen sich mit der DSGVO so gut wie alle Branchen beschäftigen.

Wie der Name andeutet, geht es in der DSGVO um personenbezogene Daten, die geschützt werden sollen. Sie ist für alle Unternehmen relevant, die in der EU ansässig sind, dort eine Niederlassung haben oder personenbezogene Daten von EU-Bürgern verarbeiten. Personenbezogene Daten sind etwa Name, Adresse, E-Mail-Adresse, Telefonnummer, IP-Adresse und Cookies, sogar Fahrzeugkennzeichen und Kontonummern – eben alles, wodurch man auf eine konkrete Person schließen kann.

Die DSGVO vereinheitlicht das Datenschutzrecht innerhalb der EU, nachdem bisher jeder Mitgliedsstaat sein eigenes Süppchen gekocht hat. Die Verordnung trat am 25. Mai 2016 in Kraft. Sie muss seit dem 25. Mai 2018 angewendet werden. Als EU-Verordnung gilt die DSGVO in den Mitgliedsstaaten direkt – anders als eine EU-Richtlinie, die jeweils eine nationale Umsetzung erfordert. Allerdings können die einzelnen Staaten eine EU-Verordnung mit eigenen Vorschriften ergänzen, wobei es durchaus Gestaltungsspielräume gibt. In Deutschland ersetzt die DSGVO Teile des Bundesdatenschutzgesetzes (BDSG), das zudem an einigen Stellen angepasst wird. Ähnlich verhält es sich mit dem Telemediengesetz (TMG). Voraussichtlich wird es mit der ePrivacy-Verordnung demnächst noch eine weitere Vorschrift geben. Diese sollte ursprünglich 2018 mit der DSGVO in Kraft treten, ist aber inzwischen auf 2019 verschoben.

## Nicht explizit genannt, aber ...

Auch in der DSGVO und den anderen genannten Datenschutzvorschriften kommt der Begriff „Verschlüsselung" nicht wörtlich vor. De facto müssen die betroffenen Unternehmen jedoch Doku-

mente mit personenbezogenen Daten verschlüsseln, sobald sie sie in der Cloud ablegen, per E-Mail oder Chat übermitteln. Auf Nichtbeachtung steht zwar kein Gefängnis, dafür drohen empfindliche Schadenersatzklagen und hohe Geldstrafen. Bisher sah das Bundesdatenschutzgesetz ein Bußgeld von maximal 50 000 Euro (300 000 Euro für sehr schwere Verstöße) vor, wobei die Datenschutzbehörden diese Möglichkeiten nur sehr selten ausschöpften. Das wird sich nun ändern, denn die DSGVO droht mit Bußgeldern von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Vorjahresumsatzes. Damit sollen die Behörden auch gegen global agierende Unternehmen ein effektives Mittel in der Hand haben.

Eine Neuerung ist das Recht auf Datenübertragbarkeit, das in Artikel 20 der DSGVO geregelt ist. Es berechtigt den Nutzer dazu, seine Daten von einem zum anderen Anbieter mitzunehmen – beispielsweise beim Wechsel der Bank oder des Arbeitgebers. Die Übergabe der Daten muss in einem „gängigen Format" erfolgen. Dies wird wohl kaum ohne Verschlüsselung möglich sein, die die Anwender dann auch belegen müssen, denn die DSGVO sieht ausdrücklich eine Rechenschaftspflicht vor (Artikel 5).

Die DSGVO war in den letzten Monaten ein Hype-Thema in der IT-Branche, insbesondere rund um den 25. Mai, als sie wirksam wurde. Doch während inzwischen fast alle Unternehmen ihre Webseiten und E-Mail-Verteiler DSGVO-konform gemacht haben, sehen viele bei den tiefer greifenden Sicherheitsmaßnahmen, auch bei der Verschlüsselung, noch keinen Handlungsbedarf. Das Kalkül hierbei: Bis zu den ersten Gerichtsurteilen kann man noch warten, ohne ein zu großes Risiko einzugehen; sobald diese Urteile vorliegen, weiß man deutlich besser, wie eine sinnvolle Umsetzung der Maßnahmen aussieht.

Anders als bei § 203 des Strafgesetzbuchs ist beim Verschlüsseln nach der DSGVO kein De-facto-Standard zu erwarten. Man kann also davon ausgehen, dass beim Schutz von E-Mails die inkompatiblen Formate S/MIME und PGP nebeneinander existieren werden. Beim Verschlüsseln von Daten in der Cloud, in der die Interoperabilität nicht so wichtig ist, ist ohnehin mit einer Vielzahl von Lösungen zu rechnen.

## Für kritische Bereiche: das IT-Sicherheitsgesetz

Eine Pflicht zum Verschlüsseln ergibt sich auch aus dem IT-Sicherheitsgesetz und der zugehörigen Kritisverordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese Vorschriften, die am 25. Juli 2015 in Kraft getreten sind, sollen zum Schutz kritischer Infrastrukturen in Deutschland beitragen und generell die IT-Sicherheit hierzulande erhöhen. Die Kritisverordnung regelt unter anderem, welche Branchen unter die Vorschriften des IT-Sicherheitsgesetzes fallen. Entscheidend ist hierbei, dass „ein Ausfall oder eine Beeinträchtigung [...] erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit zur Folge haben kann". Wie man sich leicht vorstellen kann, ist dies beispielsweise in der Informationstechnik, der Telekommunikation, der Energieversorgung und der Lebensmittelbranche der Fall.

Das IT-Sicherheitsgesetz verpflichtet die betroffenen Organisationen dazu, ein Mindestmaß an IT-Sicherheit einzuhalten und dies auch nachzuweisen. Insbesondere ist ein Information Security Management System (ISMS) Pflicht – neben einer Meldepflicht gegenüber dem BSI und dem Kunden. Auch Partner und Lieferanten der Organisationen müssen dem IT-Sicherheitsgesetz nachkommen.

Im Gegensatz zu den meisten anderen in diesem Artikel angeführten Gesetzen erwähnt das IT-Sicherheitsgesetz die Verschlüsselung wörtlich. In Artikel 4 des Gesetzes heißt es: „Eine Maßnahme nach Satz 1 [des Telemediengesetzes] ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens." Diese Passage bezieht sich auf die Anbieter von „Telemedien", womit vor allem Internetangebote aller Art gemeint sind. Für andere im Gesetz genannte Gruppen, vor allem für die Betreiber der besagten kritischen Infrastrukturen, gibt es zwar keine explizite Verschlüsselungspflicht, doch implizit wird sich das Verschlüsseln kaum vermeiden lassen.

Bei Verstößen sieht das IT-Sicherheitsgesetz eine Geldbuße von bis zu 100 000 Euro vor – was für ein großes Unternehmen sicherlich nicht allzu viel ist. Das Gesetz wird jedoch als erster Schritt und als wichtige Grundlage bewertet.

## Effizientere Dienste dank E-Government-Gesetz

Im August 2013 ist das Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) in Kraft getreten. Es soll Bund, Ländern und Kommunen die Möglichkeit bieten, einfachere und effizientere Onlineverwaltungsdienste anzubieten. Der Bund gibt mit dem E-Government-Gesetz Rahmenbedingungen vor, die für die Bundesverwaltung und teilweise auch für Länderverwaltungen gelten. Die Länder haben ihre Verwaltungsverfahrensgesetze entsprechend angepasst. Mit dem IT-Planungsrat gibt es seit dem 1. April 2010 zudem ein zentrales Steuerungsgremium für die Zusammenarbeit von Bund, Ländern und Kommunen im Bereich der IT und des E-Governments.

Das E-Government-Gesetz ist jedoch nicht nur ein Angebot, sondern auch eine Verpflichtung. So müssen Behörden einen Onlinezugang zu ihren Diensten anbieten, sobald die entsprechenden Ausführungsbestimmungen vorliegen. Die


**Der Gesetzgeber meint es offenbar ernst. Eine Pflicht zur Verschlüsselung ergibt sich unter anderem aus dem Strafgesetzbuch, der EU-Datenschutz-Grundverordnung und dem IT-Sicherheitsgesetz (Abb. 2).**

dabei verarbeiteten Daten müssen natürlich geschützt – und damit auch verschlüsselt – sein.

Ein wesentliches Hindernis für E-Government-Angebote der öffentlichen Verwaltung bestand bisher darin, dass anstelle der Schriftform nur die qualifizierte elektronische Signatur (QES) zugelassen war und diese noch nicht ausreichend verbreitet ist. Mit dem Gesetz werden daher neben der qualifizierten Signatur zwei weitere Schriftform-Alternativen zugelassen. Die erste ist De-Mail mit der Versandoption „absenderbestätigt", die eine „sichere Anmeldung" voraussetzt. Das zweite Verfahren sind Webanwendungen der Verwaltung in Verbindung mit sicherer elektronischer Identifizierung durch die eID-Funktion des neuen Personalausweises.


**Dank des neugefassten § 203 des Strafgesetzbuchs müssen Juristen und einige andere Berufsgruppen zukünftig vermehrt Verschlüsselung einsetzen (Abb. 3).**

## E-Health-Gesetz mit Hürden

Schließlich wird man sich auch im Gesundheitswesen zukünftig mehr Gedanken über das Verschlüsseln machen müssen. Die Vorschriften dazu sind im E-Health-Gesetz von 2015 enthalten. Es heißt mit vollständigem Namen „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen", betrifft zunächst Ärzte, Apotheker und Krankenhäuser und hat dabei Vorrang gegenüber dem oben erwähnten Strafgesetzbuch-Paragrafen, in dem Heilberufe ebenfalls erwähnt werden.

Betroffen vom E-Health-Gesetz sind außerdem die sogenannten nichtverkammerten Heilberufe, also vor allem Heilpraktiker. Eine Herausforderung wird darin bestehen, dass es für die Nichtverkammerten bisher keine Heilberufsausweise (dies ist der Nachfolger des heutigen Arztausweises) gibt. Das soll sich zukünftig ändern. Noch ist allerdings nicht ganz klar, wer die Ausgabestellen für die Ausweise betreiben wird, da es keine Kammern gibt, die zentral die Daten der angeschlossenen Praxen verwalten.

Das E-Health-Gesetz, so kann man auf der Webseite des Bundesgesundheitsministeriums nachlesen, enthält einen Fahrplan für die Einführung einer digitalen Infrastruktur für das Gesundheitswesen („Telematikinfrastruktur"). Diese soll ein hohes Sicherheitsniveau bieten, wobei die elektronische Gesundheitskarte eine wichtige Rolle spielen soll. Die zentralen Teile der Telematikinfrastruktur existieren bereits, inzwischen sind nahezu alle Arztpraxen und Krankenhäuser daran angeschlossen. Dazu sind spezielle Konnektoren notwendig, die mittlerweile verfügbar sind.

Ein solcher Konnektor, der in erster Linie dazu dient, eine Praxis oder Klinik auf die Telematikinfrastruktur aufzuschalten, ermöglicht sogenannte Massensignaturen. Er kann also mehrere Dokumente nacheinander digital signieren, ohne dass der Anwender jedes Mal seine PIN eingeben muss. Massensignaturen sind technisch zwar kein Problem, müssen aber verschiedene Sicherheitsvorgaben erfüllen, damit sie dem Signaturgesetz genügen.

Die Anwendungen der Gesundheitskarte sind vielfältig. Auf der Karte gespeicherte Notfalldaten sollen dem Rettungsdienst die Arbeit erleichtern, ein Medikationsplan kann lebensgefährliche Wechselwirkungen verhindern und die Telemedizin soll mobil eingeschränkte Menschen unterstützen. Mit der elektronischen Patientenakte und dem Patientenpostfach gibt es weitere interessante Nutzungsmöglichkeiten. Für eine ganze Reihe dieser Anwendungen existieren bereits konkrete Zeitpläne. Praktisch alle davon werden starke Verschlüsselung benötigen.

## Deutsche Anbieter wittern ihre Chance

Blickt man auf die verschiedenen Gesetze, die Verschlüsselung (und die damit eng verwandten digitalen Signaturen) einfordern, dann fällt auf: Nahezu überall wird derzeit an deren Umsetzung gearbeitet, doch die Details sind noch unklar. Interessant wird sein, welche Verschlüsselungslösungen sich durchsetzen. Vor allem im Behördenbereich dürften US-Produkte, die traditionell unter dem Verdacht der NSA-Einflussnahme stehen, schlechte Karten haben. Die in diesem Artikel vorgestellten Gesetze sind daher eine große Chance für Hersteller aus dem deutschsprachigen Raum, die mit Cloud-, E-Mail-, Telefon- und Chat-Verschlüsselungsprodukten gut aufgestellt sind.

Doch die Vorschrift, diese Verschlüsselungstechnik zu nutzen, ist stets nur die eine Seite der Medaille. Mindestens genauso wichtig wird es sein, die betroffenen Anwender zum Einsatz von Verschlüsselung zu motivieren. Dies gelingt nur, wenn die Anwendungen benutzerfreundlich sind oder (besser noch) im Hintergrund ihre Arbeit erledigen. Nachdem die Gesetzeskeule ausgepackt ist, gilt es nun also, Verschlüsselung noch bedienungsfreundlicher und smarter zu gestalten. Die alte IT-Sicherheitsweisheit, wonach es für den Anwender keine Bugfixes gibt, muss daher ergänzt werden: Man kann einen Anwender nicht per Gesetz ändern. (ur@ix.de)


### Klaus Schmeh

ist Berater bei cryptovision (www.cryptovision.com) und Krypto-Blogger (www.schmeh.org).

### Udo Wichert

ist Vice President Public Sector bei cryptovision (www.cryptovision.com).


### Literatur


[1] Markus Hoffmeister, Klaus Schmeh; Kommunikation; Geheime Post; Revisited: E-Mail-Verschlüsselung; *iX* 1/2014, S. 136