Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

1
K&R

Editorial: Der Nachtrag zu einer ursprünglich zulässigen Verdachtsberichterstattung · *Dr. Simon Haug*

1 Embedded Content und das Recht der öffentlichen Wiedergabe – Svensson ist die (neue) Realität!
Dr. David Jahn und *Christoph Palzer*

6 Datenschutzcompliance leicht(er) gemacht: Das „Hausaufgabenheft" der Art. 29-Gruppe für Google
Dr. Lina Böcker und *Dr. Carlo Piltz*

11 Verschlüsselte Kommunikation im Unternehmensalltag: Nice-to-have oder notwendige Compliance?
Dr. Florian Deusch und *Prof. Dr. Tobias Eggendorfer*

18 Arbeitsrecht & Neue Medien
Peter Kaumanns und *Sebastian Böhm*

23 Aktuelle Entwicklungen im Steuerrecht in der Informationstechnologie 2013/2014 · *Prof. Dr. Jens M. Schmittmann*

30 Vom schwierigen Umgang mit Drittsendezeitverpflichtungen im Rahmen des Eilrechtsschutzes
Prof. Dr. Karl-E. Hain und *Thomas Wierny*

34 Länderreport Schweiz · *Dr. Ursula Widmer*

36 BGH: Presseveröffentlichung privater E-Mails aus gestohlenem Laptop kann zulässig sein
mit Kommentar von *Christine Libor*

41 BGH: Olympia-Rabatt: Werbung mit „Olympischen Preisen" zulässig
mit Kommentar von *Eckart Haag*

67 BVerwG: Presserechtlicher Auskunftsanspruch zu Namen von Funktionsträgern im Strafverfahren

Beilage

Jahresregister 2014

18. Jahrgang **Januar 2015** Seiten 1 – 72

dfv Mediengruppe · Frankfurt am Main

auch dann erfüllt werden müssen, wenn der Betroffene verschiedene Arten von Endgeräten nutzt, wie etwa einen PC, ein Handy oder ein Tablet. Wenn jedoch das Endgerät aufgrund seiner Konstruktion nicht die Möglichkeit bietet, die erforderlichen Informationen zur Datenverarbeitung anzuzeigen (etwa aufgrund eines fehlenden Bildschirms), so sehen es die europäischen Datenschützer durchaus als gangbare Alternative an, wenn die Informationen auf demjenigen Endgerät angezeigt werden und abrufbar sind, auf dem der Nutzer das intelligente Gerät konfigurieren kann.

Die Datenschützer erwähnen explizit Geräte des Unternehmens *Nest*, welches intelligente Rauchmelder und Thermostate vertreibt.[21] Auf diese Weise böte sich damit natürlich auch die Möglichkeit, auf dem „Konfigurationsgerät" die Einwilligung der Nutzer für eine Datenverarbeitung einzuholen. Die so vorgeschlagene Vorgehensweise lässt sich in jedem Fall begrüßen und bietet für Unternehmen, die Produkte für das „Internet der Dinge" herstellen und vertreiben, eine interessante Alternative, um ihren datenschutzrechtlichen Pflichten nachzukommen. Sie löst allerdings nicht das Problem, wie mit Nutzern umzugehen ist, die keine Gelegenheit haben, das Konfigurationsgerät zu konsultieren und die die fraglichen Geräte „aus Versehen" nutzen, zum Beispiel Rauchmelder in Büroräumen.

VI. Ergebnis

Der Leitfaden der Art. 29 Gruppe bietet Anlass zu positiver und negativer Kritik. Der ursprüngliche Grund für die von den europäischen Datenschützern veröffentlichten Empfehlungen zur Umsetzung von rechtskonformen Datenschutzklärungen, sollte stets im Hinterkopf behalten werden. Es geht prinzipiell um Vorgaben an eines der größten Technologieunternehmen der Welt und Hinweise, wie dieses die Datenflut seiner Nutzer rechtskonform und nutzerfreundlich in den Griff bekommen kann. Die Datenschützer machen das selbst gleich Eingangs deutlich und erklären in einer zusätzlichen, dem Dokument vorangestellten „Note", das Dokument diene „illustrativen Zwecken" („…for illustrative purposes only…") und könne behördliche Maßnahmen nicht vorwegnehmen.

Nichtsdestotrotz ist es zu begrüßen, dass sich die Datenschützer überhaupt mit praktischen Hinweisen zur Umsetzung der gesetzlichen Vorgaben auseinandersetzen und Vorschläge unterbreiten – auch wenn sie dabei bisweilen über das Ziel hinaus schießen. Darüber hinaus bietet das Dokument ausreichend Interpretationsspielraum, um für jede datenverarbeitende Stelle, die im Internet eine Webseite betreibt oder Dienstleistungen anbietet, als Richtschnur bei der Erstellung oder Überarbeitung von eigenen Datenschutzerklärungen zu dienen und zumindest Hinweise zu geben, wo es an der Umsetzung hapert.

Die europäischen Datenschützer legen öffentlich dar, wie aus ihrer Sicht – und damit aus Sicht der für eine Prüfung von Datenverarbeitungsprozessen zuständigen Aufsichtsbehörden – eine Erfüllung der datenschutzrechtlichen Anforderungen aussehen kann. In der Praxis sollten daher Ansätze wie das Modell einer Datenschutzerklärung mit mehreren Ebenen oder die Anforderungen an eine Einwilligung für Datenverarbeitungen im „Internet der Dinge" durchaus Beachtung finden, wenngleich sie natürlich nicht die Verbindlichkeit gesetzlicher Vorgaben erreichen können. „Blinder Gehorsam" scheint daher fehl am Platz zu sein, denn bei jeder verantwortlichen Stelle unterscheiden sich die Datenverarbeitungsprozesse. Individuellen Bedürfnissen oder technischen Feinheiten sollte daher stets Rechnung getragen werden. Ein Seitenblick auf dieses „Hausaufgabenheft für Google" dürfte dagegen weder bei der rechtlichen Beratung noch bei der praktischen Umsetzung schaden.

21 www.nest.com.

RA Dr. Florian Deusch, Ravensburg und Prof. Dr. Tobias Eggendorfer, Weingarten*

Verschlüsselte Kommunikation im Unternehmensalltag: Nice-to-have oder notwendige Compliance?

Die „Snowden-Enthüllungen" haben bestätigt, wovor die IT-Sicherheit schon lange gewarnt hat: Kommunikation über das Internet ohne Schutzmaßnahmen ist immer unsicher. Es besteht insbesondere das Risiko des Mitschneidens von Nachrichten.[1] Der folgende Beitrag zeigt, ob und wie diesen Risiken im Unternehmensalltag durch Verschlüsselung zu begegnen ist, insbesondere bei der digitalen Kommunikation zwischen Vertragspartnern.

I. Einleitung und Praxisbeispiel

Der Beitrag stellt zunächst die Funktionsweise digitaler Verschlüsselung dar (Ziffer II). Sodann zeigt Ziffer III an einem Beispielsfall, wie in der Unternehmenspraxis mit dem Risiko des Datenabflusses und dem Schutz durch Verschlüsselung umzugehen ist. Ein Fazit schließt die Untersuchung ab (Ziffer IV).

Beispielsfall: Das Konstruktionsbüro K hat mit dem Automobilbauer A eine Geheimhaltungsvereinbarung (NDA) nach dem Muster des Verbands der deutschen Automobil-

* Der Autor Deusch ist als Rechtsanwalt, Fachanwalt für Informationstechnologierecht und als zertifizierter Datenschutzbeauftragter in der Anwaltskanzlei Dr. Gretter tätig; der Autor Tobias Eggendorfer ist Professor für IT-Sicherheit an der Hochschule Weingarten, freiberuflicher IT-Berater und ebenso zertifizierter Datenschutzbeauftragter. Der Beitrag geht auf einen Vortrag bei der DSRI-Herbstakademie 2014 zurück, der im Tagungsband Jürgen Taeger (Hrsg.), BIG DATA & Co – Neue Herausforderungen für das Informationsrecht, DSRI-Herbstakademie 2014, Edewecht 2014, dokumentiert wurde. Er ist jedoch aktualisiert zum Stand Dezember 2014. Mehr über die Autoren erfahren Sie auf S. XII.

1 Nach jüngsten Nachrichtenmeldungen greifen die Geheimdienste auf den vollständigen Datenstrom der Provider zu und kartografieren mit diesen Angaben weltweit alle Netzwerkverbindungen einschließlich der angeschlossenen Endgeräte, siehe Heise Newsticker v. 14. 9. 2014, http://www.heise.de/newsticker/meldung/Bericht-NSA-und-GCHQ-hoeren-Datenverkehr-deutscher-Provider-ab-2391075.html (Bericht: „NSA und GCHQ hören Datenverkehr deutscher Provider ab").

industrie (VDA) abgeschlossen. Diese lautet auszugsweise:[2] „Die Parteien sichern sich gegenseitig zu, Informationen weder an Dritte weiterzugeben noch in anderer Form Dritten zugänglich zu machen und alle angemessenen Vorkehrungen zu treffen, um einen Zugriff Dritter auf diese Informationen zu vermeiden. Informationen (…) sind insbesondere die Bezeichnung und der Inhalt des Projektes (…).“ K möchte ein Angebot über die Konstruktion eines Scheibenwischers an A per E-Mail versenden. Muss K aufgrund dieser Vereinbarung E-Mails verschlüsseln?

II. IT-Praxis: Verschlüsselte, digitale Kommunikation

Das Bedürfnis, Informationen geheim zu halten, lässt sich bis ins Altertum verfolgen. 1900 v. Chr. deuten ungewöhnliche Hieroglyphen auf eine Geheimschrift; 1500 v. Chr. nutzen Mesopotamier eine verschlüsselte Rezeptur für eine Tonmischung gegen Industriespionage.[3] Seither hat der dauerhafte Wettbewerb zwischen Kryptanalytikern und Kryptographen die Verschlüsselungsverfahren stetig verbessert, doch die Neugier Unberechtigter ist, wie der Fall Snowden zeigt, konstant.

1. Technik und Einsatz von Verschlüsselungsverfahren

Die Kryptologie untergliedert sich in die Steganographie, Kryptographie und Kryptanalyse, dem Brechen von Schlüsseln.

a) Steganographie

Die Steganographie versteckt eine geheime Nachricht so, dass sie nur eingeweihte Empfänger erkennen. So transportiert in einem Gemälde die Länge von Grashalmen an einem Bach Geheimes als Morsezeichen, ein Text die geheime Nachricht in jeder zweiten Zeile. In der IT eignen sich für die verdeckte Übertragung von Nachrichten u. a. ungenutzte Bits in Dateien, minimale Farbveränderungen in Bilddateien[4] oder das Verstecken von verschlüsselten Nachrichten in Zufallsdaten.[5]

Zensur ist ein Weg, um Steganographie zu stören: Dabei wird die Nachricht sinngleich verändert.[6] So sollte in einem Fall die geglückte Flucht durch „Father is dead“ telegraphiert werden, der gleichwertige Ersatz durch „Father has deceased“ führte zur Rückfrage „Is father dead or has he deceased?“. Dies bewies die verdeckte Kommunikation.[7]

Das zeigt: Steganographie erfordert sichere Nutzung. Dann ist sie ein hervorragendes Verfahren zum geheimen Datenaustausch, denn ein Beobachter bemerkt ihn nicht einmal. Zudem ist die Wahl der Verfahren völlig frei, mithin unendlich. Sie müssen die Parteien nur im Vorfeld sicher vereinbaren.

b) Symmetrische Kryptographie

Genau dieses Problem gilt auch für die symmetrische Verschlüsselung: Der sichere Austausch des sowohl zur Ver- als auch zur Entschlüsselung nötigen Schlüssels ist Gegenstand zahlreicher Agententhriller. Dafür sind symmetrische Verfahren schneller zu berechnen und bei gleicher Schlüssellänge sicherer als asymmetrische. Dadurch eignen sie sich immer wenn kein Schlüsseltausch nötig ist: Z. B. zur Festplattenverschlüsselung.

c) Asymmetrische Kryptographie

Für E-Mail-Verschlüsselung dagegen sind asymmetrische Verfahren besser: Zum Chiffrieren dient ein problemlos zu veröffentlichender public Key. Der zugehörige, zur Dechiffrierung dienende private Key dagegen muss geheim bleiben. Die Ver- und Entschlüsselung ist ungleich rechenzeitaufwendiger als bei symmetrischen Verfahren, zudem sind für vergleichbare Sicherheit wesentlich längere Schlüssel nötig: 1024 bis 8192 Bit im Vergleich zu 128 bis 512 Bit.

Andererseits ist eine Kommunikation in Gruppen mit asymmetrischer Verschlüsselung einfacher: Während bei symmetrischer Verschlüsselung *n!* Schlüssel[8] nötig sind, reichen bei der asymmetrischen *n* Schlüssel aus.

d) Hybride Kryptographie

Phil Zimmermann hat, um die Vorteile beider Verfahren zu kombinieren und ihre Nachteile zu eliminieren, die hybride Verschlüsselung (PGP, „Pretty Good Privacy“) entwickelt. Dabei wird zunächst zur symmetrischen Verschlüsselung der Nachricht ein zufälliger Sitzungsschlüssel generiert, der dann zur sicheren Übertragung mit dem public Key des Empfängers verschlüsselt und zusammen mit der Nachricht versandt wird. Der Empfänger entschlüsselt den Sitzungsschlüssel mit seinem private Key und kann so die Nachricht dechiffrieren. Da ein symmetrischer Schlüssel in der Regel wesentlich kleiner ist als die zu übertragenden Nachrichten, reduziert sich der Rechenzeitaufwand erheblich. Gleichzeitig ist das Problem des Schlüsseltausches gelöst, so dass hybride Verfahren heute Standard für den digitalen Nachrichtenaustausch sind.

e) Kryptographisch sichere Prüfsummen

Verschlüsselung macht es unmöglich, eine verschlüsselt übertragene Nachricht mitzulesen (Vertraulichkeit), aber nicht, sie ungezielt zu verändern (Integrität). Die Integrität wird realisiert durch kryptographisch sichere Prüfsummen, die zusätzlich zur Nachricht übermittelt werden. Da die Prüfsumme (fast) einzigartig ist, sind Manipulationen zu erkennen.

f) Digitale Signatur

Verschlüsselt der Absender die Prüfsumme mit seinem private Key, ist eine Manipulation oder ein Austausch unmöglich. Ist zudem der private Key eindeutig einem Absender zugeordnet, z. B. durch das PGP Web of Trust oder den neuen e-Personalausweis, weiß der Empfänger, wer der Absender ist. Damit ist das für E-Mail wichtige Schutzziel der Authentizität erreicht, denn eine E-Mail unter falschem Namen zu verschicken, ist trivial.[9]

2 http://www.vda.de/de/publikationen/publikationen_downloads/detail.php?id=633.
3 U. a. *Müller-Quade*, Hieroglyphen, Enigma, RSA. Eine Geschichte der Kryptographie, Uni Karlsruhe, Vorlesungsfolien, https://crypto.iti.kit.edu/fileadmin/User/enigma.pdf.
4 U. a. *Cole*, Hiding in Plain Sight, 2003.
5 Z. B. TrueCrypt, http://www.truecrypt.org, abgerufen am 17. 2. 2014 (am 11. 7. 2014 offline).
6 Bei moderneren Verfahren erreicht denselben Effekt z. B. die Konvertierung einer Bitmap in das JPEG-Format oder eine Änderung der Bildgröße.
7 *Bauer*, Kryptologie: Methoden und Maximen, 1993.
8 n-Fakultät.
9 U. a. *Eggendorfer*, Methoden der Spambekämpfung und Vermeidung, Dissertation, 2007.

g) Angriffe auf Verschlüsselung

Grob lassen sich Angriffe auf Verschlüsselung in Angriffe auf den Schlüssel, auf das Verschlüsselungsverfahren sowie auf Rahmenbedingungen der Verschlüsselung bzw. Datenübertragung einteilen.

aa) Angriffe auf den Schlüssel

Gute Verschlüsselung darf nach der „Kerkhoff-Regel“[10] nicht von der Geheimhaltung des Algorithmus abhängen, sondern nur von der des Schlüssels. Da ein Erraten des Schlüssels durch Ausprobieren aller möglichen Varianten („Brute-Forcing“) mehrere Millionen Jahre dauern kann, nutzen Angreifer in der Regel andere Verfahren: Dazu zählt zum Beispiel der „Heart-Bleed“-Angriff, der am 7. 4. 2014 bekannt und behoben wurde. Durch einen Programmfehler in der Verschlüsselungssoftware konnten Speicherinhalte entfernt ausgelesen werden, in denen unter Umständen auch der private Key zu finden war. Damit können sämtliche verschlüsselte Nachrichten entschlüsselt werden, auch ältere Mitschnitte.[11]

Andere Angriffe nutzen Bedienfehler, zum Beispiel der „Known-Plain-Text“-Angriff. Dabei kennt der Angreifer sowohl das Chiffrat als auch den Klartext einer bestimmten Nachricht und kann so den Schlüssel leichter brechen. Das geht, wenn z. B. Nutzer auf verschlüsselte Nachrichten Antworten im Klartext senden.

bb) Angriffe auf Verschlüsselungsverfahren

Sind die Verschlüsselungsverfahren selbst fehlerhaft oder unsicher, sind spezifische Angriffe gegen sie denkbar: Bei der WLAN-Verschlüsselung WEP z. B. waren einige Parameter ungeschickt gewählt, weshalb sie als geknackt gilt.

cc) Angriffe auf Rahmenbedingungen

Exotischere Angriffe nutzen Untersuchungen, die die Veränderung des elektromagnetischen Feldes oder des Stromverbrauchs des Prozessors in Abhängigkeit von den ausgeführten Instruktionen messen. Darüber können unter extremen Laborbedingungen Daten und Befehle erkannt werden.

dd) Fazit Angriffe

Es zeigt sich, dass Verschlüsselung an sich zwar sicher ist, allerdings, wie alle Sicherheitsmaßnahmen, nicht isoliert wirkt, sondern geeignete organisatorische Maßnahmen braucht, um effektiv zu sein. Dazu zählen zum Beispiel sichere Passphrases und Nutzerschulungen, um z. B. „Known-Plain-Text“-Angriffe zu erschweren.

h) Anwendungsbeispiele

Nach dem Wirkort der Verschlüsselung unterscheidet man zwischen Transportverschlüsselung, bei der nur der Transportweg, nicht jedoch die Speicherung der Daten geschützt ist, der End-Zu-End-Verschlüsselung, bei der die Nachricht vom Nutzer ver- und entschlüsselt wird, sie somit auch auf dem lokalen Datenträger geschützt ist und einer reinen Datenträger-Verschlüsselung.

aa) Transportverschlüsselung

HTTPS, also z. B. Online-Banking und -Shopping, nutzt Transportverschlüsselung, genauso wie IMAPS oder SMTP/TLS zum Abruf und Versand von Mails. Bei E-Mail ist das Ziel, die nötigen Kennwörter zu schützen, nicht die Nachrichten; diese werden unterwegs mehrfach unverschlüsselt zwischengespeichert.

bb) End-Zu-End-Verschlüsselung

Im Gegensatz dazu verschlüsselt der Nutzer bei End-Zu-End-Verschlüsselung die Nachricht vor der Übertragung. Erst nach Ankunft entschlüsselt sie der Empfänger. Dadurch kann kein an der Übertragung beteiligtes System die Nachricht mitlesen, weshalb das Verfahren für E-Mail geeignet ist. Beispiele sind S/MIME und PGP/GnuPG. Die E-Mail lagert auch auf der lokalen Festplatte verschlüsselt.

cc) Datei- und Plattenverschlüsselung

Verfahren zur Platten- und Dateiverschlüsselung sind primär dazu gedacht, Daten zu schützen, sollten Dritte den Rechner erlangen – angeblich sind Laptops der häufigste Fundgegenstand an Flughafensicherheitskontrollen.[12] Im Gegensatz zu den End-Zu-End-Verschlüsselungsverfahren, die asymmetrisch arbeiten, nutzen Dateiverschlüsselungen symmetrische Verfahren; der Nutzer behält den Schlüssel, so dass das Problem des Schlüsseltauschs hier irrelevant ist. Gängige Vertreter sind die sicheren Plattenverschlüsselungen „FileVault“ von Apple und „TrueCrypt“ sowie unsichere Dateiverschlüsselungen von Büro- oder Kompressionssoftware. Für Letztere gibt es Programme, die helfen sollen, vergessene Schlüssel zu knacken.[13] Das Schutzniveau ist entsprechend niedrig und wohl eher als Hinweis im Sinne des § 202 a Abs. 1 StGB zu verstehen als tatsächlich wirksam.

dd) Fazit: End-Zu-End ggü. Transportverschlüsselung

Aus technischer Sicht ist daher die Dateiverschlüsselung zum Schutz der eigenen Systeme sinnvoll, für eine Datenübertragung eine End-Zu-End-Verschlüsselung. Die Transportverschlüsselung schützt nur eine (Teil-)Strecke des Transportweges vor dem Abhören. Für das Ziel, Nutzernamen und Passwörter zu schützen, ist das suffizient, für eine schützenswerte E-Mail-Kommunikation jedoch nicht. Insofern ist die aktuelle Werbung mehrerer großer deutscher E-Mail-Anbieter,[14] Mails per SSL zu verschlüsseln, irreführend: Es ist nur eine Transportverschlüsselung. Erst eine End-Zu-End-Verschlüsselung würde Vertraulichkeit gewährleisten.

i) Verbreitung von Verschlüsselung

Ein häufiges Gegenargument zu Verschlüsselung: Sie sei umständlich, daher verzichte man auf die Nutzung. Dabei ist sie für den Nutzer transparent, z. B. im Online-Banking oder -Shopping. Während daher die E-Mail-Verschlüsselung noch unüblich ist, ist Verschlüsselung in anderen Bereichen Standard: Zur Fernwartung von Rechnern hat das verschlüsselte SSH schon vor ca. 20 Jahren Telnet abgelöst, für die Abholung von E-Mails beim Provider

10 U. a. *Bauer* (Fn. 7), S. 137 f.

11 In diesem Fall besonders kritisch, weil die Sicherheitslücke mehrere Jahre bestand.

12 So z. B. Stern v. 24. 5. 2006, http://www.stern.de/wissen/technik/verlust-mobiler-geraete-dem-laptop-auf-der-spur-561632.html („Verlust mobiler Geräte: Dem Laptop auf der Spur“).

13 Siehe http://www.heise.de/security/meldung/Tool-knackt-Office-Verschluesselung-binnen-weniger-Minuten-978956.html, abgerufen am 6. 12. 2014.

14 So z. B. Heise Newsticker v. 9. 8. 2013, http://www.heise.de/newsticker/meldung/E-Mail-Made-in-Germany-SSL-Verschluesselung-fuer-fast-alle-1932962.html („E-Mail Made in Germany: SSL-Verschlüsselung für (fast) alle“).

wird meist das verschlüsselte POP3S und IMAPS genutzt, HTTPS beim Online-Banking und -Shopping. Moderne Betriebssysteme verschlüsseln Passwörter, viele integrieren Festplattenverschlüsselung, wie z. B. Apple „FileVault". Damit ist Verschlüsselung, außer für E-Mails, bereits Standard und Stand der Technik. Aus Sicht der IT-Sicherheit sind vertrauliche Daten stets zu verschlüsseln. Das beinhaltet E-Mails. Die nötigen Programme integrieren sich problemlos in gängige Mail-Clients, bis auf die eventuell nötige Eingabe von Passphrases ist deren Nutzung für den Nutzer transparent und sehr komfortabel. Im Bereich der E-Mail-Kommunikation ist der einzige Nachteil, dass mit S/MIME und PGP/GnuPG zwei Verfahren konkurrieren. Zudem ist die Schlüsselverwaltung noch nicht automatisiert, was den Verwaltungsaufwand für die Anwender minimal erhöht. Diese Komfort-Probleme reduzieren die Akzeptanz.

j) Alternativen zur Verschlüsselung

In der Praxis ist asymmetrische Verschlüsselung für die Nutzer das bequemste Verfahren: Steganographie lässt sich schwieriger mit Standardsoftware umsetzen und erfordert wie die symmetrische Verschlüsselung den sicheren Austausch von Verfahren und „Schlüssel". Beide benötigen pro Absender-Empfänger-Paar einen gesonderten Schlüssel, bei der Steganographie sogar unterschiedliche Verfahren. Das treibt den Verwaltungsaufwand so massiv in die Höhe, dass er schon bei 10 Kontakten und damit über 3 Millionen Kommunikationspaarungen praktisch unbeherrschbar wird. Alternative Verfahren, wie USB-Sticks zu verschicken, sind denkbar; um einen Verlust auf dem Postweg zu vermeiden, empfiehlt sich dennoch Verschlüsselung.

2. Effektivität von Verschlüsselung

Verschlüsselung mit modernen Verfahren kann als praktisch sicher betrachtet werden: Gängige Angriffe auf Schlüssel dauern selbst unter Berücksichtigung künftiger Hardwareentwicklungen um Größenordnungen länger als der anzunehmende Geheimhaltungsbedarf: Geheimnisse, die zu Beginn der Erdgeschichte verschlüsselt worden wären, wären mindestens noch einmal so lange sicher. Dem stimmt auch *Peter Gutmann* zu, obwohl er kürzlich das „Ende" der Kryptographie als Sicherheitsmaßnahme postuliert hat, denn seine Kritik richtet sich im Kern nicht gegen sichere Verschlüsselungsverfahren, sondern gegen fahrlässigen Umgang damit. Sicherheitsmaßnahmen wirken nur in Kombination: Eine Hochsicherheitstür in einer Schnellbauwand bringt nichts, weil die Wand nicht hält. Genauso ist Verschlüsselung eine Maßnahme in einem Paket von IT-Sicherheitsmaßnahmen. Oder, wie Peter Gutmann *Drew Gross* zitiert: „I love crypto, it tells me what part of the system not to bother attacking."[15]

Wie bei jedem Werkzeug, liegt die Verantwortung für die richtige Verwendung beim Anwender. Das zeigt auch „DE-Mail", das aus IT-Sicherheitssicht untauglich ist.[16] Es wirbt zwar mit Verschlüsselung, bietet jedoch nur Transport-Verschlüsselung. Damit stehen die E-Mails auf jedem dazwischen liegenden Mailserver im Klartext. Statt echter Sicherheit definiert das Gesetz, dass die kurzfristige Entschlüsselung von Mails u. a. für einen Malware-Scan kein Bruch der Verschlüsselung sei.[17]

Aus technischer Sicht wird genau dadurch die Verschlüsselung gebrochen, erschwerend erleichtert das auch noch „Know-Plain-Text"-Angriffe. Zudem gab es in der Vergangenheit immer wieder Interessen von Geheimdiensten, auf gespeicherte Dateien bei den Providern zuzugreifen, darüber berichtete zuerst Yahoo.[18] Auch die §§ 94 ff. der deutschen StPO sehen die Beschlagnahme von E-Mail-Postfächern beim Provider vor.[19]

Die E-Mail-Daten können gesetzlich oder vertraglich begründeten Geheimhaltungsansprüchen unterliegen. Lagern sie unverschlüsselt bei einem Provider, sind sie den Ermittlungsbehörden zumindest zugänglich. Ob das nötige „Vergessen" der unberechtigten Beweismittel im Verfahren dann wirklich den gewünschten Effekt hat, nachdem möglicherweise durch die Mails weitere Beweismittel bekannt wurden, kann offen bleiben.

Ebenso erfüllt die angeblich „qualifizierte Signatur" in DE-Mail die technischen Anforderungen nicht: Für den Beweis der Absendereigenschaft muss der Absender signieren, bei DE-Mail leistet das der erste Mailserver. Auf Briefe übertragen würde der Postbote für den Absender rechtsverbindlich unterschreiben.

Zwar hat die Bundesregierung erkennbare Klimmzüge unternommen, um die Mängel per Gesetz für gewollt zu erklären, dennoch erfüllt DE-Mail wesentliche technische Anforderungen nicht und ist damit keinesfalls für eine sichere und beweiskräftige Kommunikation geeignet.

3. Organisatorischer und finanzieller Aufwand

Dabei ist die Umsetzung von sicherer End-zu-End-Verschlüsselung mit geringem Aufwand möglich: Die nötige Software ist Open Source, die nötige Infrastruktur zum Schlüsselaustausch steht kostenlos zur Verfügung. Daher entsteht nur organisatorischer Aufwand: Die Software muss verteilt und installiert, Schlüssel erzeugt und verteilt und Mitarbeiter geschult werden. Der Gesamtaufwand dürfte bei unter 0,5 Manntagen pro Mitarbeiter liegen – inklusive Schulung und Support.

Moderne Systeme reduzieren den Aufwand für End-Zu-End-Verschlüsselung auf einen Klick und die Eingabe der Passphrase zur Ver- und Entschlüsselung. Dass End-Zu-End-Verschlüsselung dennoch nachgesagt wird, sie sei kompliziert, ist vermutlich eher ein Vermarktungsproblem: In vielen Schulungen neigen Dozenten dazu, Verschlüsselungsverfahren inklusive der zugrunde liegenden, schwer verständlichen, aber praktisch irrelevanten Mathematik zu erklären.

4. Übertragung von E-Mails

E-Mail ist unsicher: Die erste E-Mail, die 1977 an der Universität in Wisconsin übertragen wurde, war ein Ex-

15 *Gutmann*, Crypto won't save you either, http://regmedia.co.uk/2014/05/16/0955_peter_gutmann.pdf, Vortrag an der University of Auckland, 2013.

16 In der den Mitgliedern des Chaos Computer Clubs eigenen, etwas drastischeren Ausdrucksweise nannte Linus Neumann das auf dem 30. Chaos Computer Congress in Berlin „Bullshit made in Germany", nachzuhören unter: https://www.youtube.com/watch?v=p56aVppK2 W 4. Umso erschreckender ist, dass DE-Mail gerade massiv beworben wird, Kunden sogar Payback-Punkte und Lufthansa-Meilen versprochen werden, um das technisch unsinnige System zu nutzen.

17 Bericht der Bundesregierung nach Art. 5 des Gesetzes zur Regelung von DE-Mail-Diensten und zur Änderung weiterer Vorschriften; siehe auch *Koreng*, Rechtssichere elektronische Kommunikation, in: Taeger (Hrsg.): Law as a Service, Recht im Internet- und Cloud-Zeitalter, 2013, S. 623 ff.; sowie die Ausführungen in Fußnote 16.

18 So z. B. Tagesschau v. 12. 9. 2014, http://www.tagesschau.de/ausland/yahoo-102.html („US-Behörden setzen Yahoo unter Druck").

19 BVerfG 16. 9. 2009 – 2 BvR 902/06, K&R 2009, 559 ff.; *Marbeth-Kubicki*, in: Lehmann/Meents (Hrsg.), Handbuch des Fachanwalts IT-Recht, 2. Aufl. 2011, Kapitel 26 Rn. 358; kritisch dazu *Meinicke*, in: Taeger (Hrsg.): IT und Internet – mit Recht gestalten, 2012, S. 773, 784 m. w. N.

periment, um nachzuweisen, dass Nachrichten zwischen Computern versandt werden können. Unter anderem deswegen ist für den Versand von Mails keine Authentifizierung erforderlich, jedermann kann in wenigen Minuten erlernen, E-Mails unter falscher Absenderkennung zu versenden. Damit ist ohne weitere Maßnahmen die Absendereigenschaft nicht beweisbar.

E-Mails werden beim Versand im Regelfall über mindestens zwei Server weitergereicht: Den SMTP-Server des E-Mail-Providers des Absenders und den des Empfänger-Providers. Weitere Server können dazwischen geschaltet sein. Jeder Server erhält die Mail im Klartext, speichert sie zwischen, überträgt sie an den Empfänger-Server bzw. das Nutzerpostfach. Während der nur kurzen Zwischenspeicherung kann die Mail dupliziert und mitgelesen werden. Die temporäre Zwischenspeicherung wird nicht forensisch sicher gelöscht, wodurch E-Mails auch mit Zeitversatz rekonstruierbar sein können. Auch auf dem Server des Providers des Empfängers liegt die Mail unverschlüsselt und kann so von jedermann gelesen werden. Bei IMAP-Servern bleibt die Mail in der Regel sogar dauerhaft auf dem Server. Unverschlüsselt.

Neben der ungesicherten Übertragung können Mails jederzeit auf den Servern der Anbieter mitgelesen und ausgeleitet werden. Das fordert sogar § 3 Abs. 2 Nr. 5 TKÜV für Provider mit mehr als 10 000 Nutzern.[20] Das erschwert es für deutsche E-Mail-Provider, rechtskonform eine End-Zu-End-Verschlüsselung anzubieten. Während bei Briefen der Umschlag Postboten vor ihrer Neugier schützt, gibt es für E-Mail keine vergleichbaren Konzepte. Für vertrauliche Kommunikation ist daher End-Zu-End-Verschlüsselung technisch notwendig.

III. Rechtliche Rahmenbedingungen für die Verschlüsselung digitaler Kommunikation

In einigen Bereichen gibt es ausdrückliche gesetzliche Verschlüsselungspflichten (Ziffer 1). Ob sich aus diesen Wertentscheidungen Erkenntnisse für eine Verschlüsselungspflicht zwischen vertraglich verbundenen Kommunikationspartnern ergeben, wird in Ziffer 2 dargestellt.

1. Ausdrückliche gesetzliche Pflichten zur Verschlüsselung digitaler Kommunikation

Beispielhaft werden folgende gesetzliche Verschlüsselungspflichten für die elektronische Kommunikation durch staatliche und private Stellen dargestellt:

a) Verschlüsselte digitale Kommunikation durch staatliche Stellen

- Übermittelt die Finanzbehörde Daten, die dem Steuergeheimnis unterliegen, sind diese gemäß § 87 a Abs. 1 S. 3 Abgabenordnung (AO) mit einem geeigneten Verfahren zu verschlüsseln. Obgleich bei DE-Mail-Diensten eine Entschlüsselung beim Provider stattfindet (siehe oben Ziffer II. 2.), ist diese Verschlüsselungsform durch § 87 a Abs. 1 S. 4 AO ausdrücklich anerkannt.[21]
- Datenübermittlungen an das und zum Nationalen Waffenregister sind nach dem jeweiligen Stand der Technik zu verschlüsseln (§§ 8 Abs. 5, 11 Nationales Waffenregistergesetz (NWRG) und § 2 NWRG-Durchführungsverordnung). Dadurch sollen die „erforderlichen Datenschutzstandards" gewährleistet werden.[22]
- Gemäß § 3 Abs. 1 Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV) übermittelt die Passbehörde die Daten zu einem Passantrag an den Passhersteller verschlüsselt.[23]

b) Verschlüsselungspflichten von Unternehmen

Unternehmen müssen elektronische Nachrichten z. B. in folgenden Bereichen verschlüsseln:[24]

- Arbeitgeber müssen die Gehaltsdaten ihrer Arbeitnehmer an das Finanzamt und die Sozialbehörden elektronisch verschlüsselt melden (§ 41 a Abs. 1 Einkommensteuergesetz, § 1 Steuerdatenübermittlungsverordnung, §§ 23 c und 28 a SGB IV, 2 Beitragsüberwachungsverordnung und 16 Datenerfassungs- und Übermittlungsverordnung). Die Steuerbehörden stellen hierfür die Schnittstelle ELSTAM zur Verfügung; für die Meldung an die Krankenkassen müssen die Arbeitgeber Computerprogramme verwenden, die von der Servicestelle der Gesetzlichen Krankenversicherung GmbH zertifiziert sind.[25]
- Gemäß § 7 a Abs. 2 Atomrechtliche Sicherheitsbeauftragten- und Meldeverordnung müssen elektronische Meldungen der Sicherheitsbeauftragten von Kernkraftwerken an die Aufsichtsbehörden verschlüsselt werden. Der Gesetzgeber will damit sicherstellen, dass die Daten „entsprechend den gängigen Datenschutzbestimmungen anderer Gesetze (so z. B. § 23 a PassG, § 2 c PAG) geschützt werden."[26]
- Die Übertragung von Energiemessdaten, die Energieversorger bei ihren Kunden mit intelligenten Messeinrichtungen erheben, ist gemäß § 21 e Energiewirtschaftsgesetz zu verschlüsseln. Grund ist der Personenbezug der Daten.[27]
- Gemäß § 13 Abs. 2 VOL/A sind elektronische Angebote, mit denen sich Unternehmen um öffentliche Aufträge bewerben, zu verschlüsseln. Das Angebot wird von der Vergabestelle erst nach Ablauf der Bewerbungsfrist entschlüsselt, um einen fairen Wettbewerb zu ermöglichen.[28]
- § 9 Bundesdatenschutzgesetz (BDSG) verpflichtet zu den technischen und organisatorischen Maßnahmen des Datenschutzes. Dies können Verschlüsselungsverfahren nach dem Stand der Technik sein (Anlage zu § 9 BDSG, S. 2). Geschuldet sind aber nur Maßnahmen in angemessenem Verhältnis zum angestrebten Schutzzweck (§ 9 S. 2 BDSG).

20 In Anbetracht dieses Interessenkonfliktes zwischen E-Government-, E-Justice- und DE-Mail-Gesetzen auf der einen und der TKÜV auf der anderen Seite, ist nachvollziehbar, warum DE-Mail keine sichere Verschlüsselung anbieten kann.

21 Wie dargelegt, handelt es sich jedoch ausschließlich um eine gesetzliche Anerkennung. Die oben in Ziffer II. 2 beschriebenen Sicherheitslücken bestehen weiter, technisch bleibt DE-Mail untauglich.

22 BR-Drs. 849/11 vom 30. 12. 2011, S. 4 f. zum Punkt „Begründung".

23 Entsprechendes gilt gemäß den §§ 12, 18 PAG.

24 Die Bundesregierung erwägt, de lege ferenda E-Mail-Anbieter zu verpflichten, ihren Nutzern Ende-zu-Ende-Verschlüsselungen anzubieten, http://irights.info/artikel/wir-muessen-bei-jeder-regelung-mit-bedenken-ob-sie-auch-im-digitalen-raum-passt/23367.

25 https://www.elster.de/arbeitg_elstam.php; beck-aktuell v. 21. 10. 2005, http://www.beck-online.de, becklink 159344. Auch Arbeitgeber-Anträge auf Erstattung geleisteter Entgeltfortzahlung für kranke Arbeitnehmer sind gemäß § 2 Abs. 3 Aufwendungsausgleichsgesetz zu verschlüsseln; entsprechendes gilt für Meldungen über Daten zur privaten Altersversorgung von Steuerpflichtigen an die Finanzbehörden gemäß § 4 Altersvorsorge-Durchführungsverordnung. Zu verschlüsseln sind auch digitale Meldungen zur betrieblichen Altersversorgung durch die Zahlstelle (Versorgungsträger) an die Krankenkassen (§ 202 Abs. 2 SGB V).

26 BR-Drs. 170/10, S. 58.

27 *Karg*, in Wolff/Brink (Hrsg.), BDSG, 1. 8. 2014, § 9 Rn. 36 a ff.

28 *Klett/Lee*, CR 2008, 644, 648; *Grützmacher*, ITRB 2002, 236, 240.

Ob hiernach eine Verpflichtung besteht, E-Mails mit personenbezogenen Daten in jedem Fall zu verschlüsseln, ist umstritten. Einige Autoren halten die Verschlüsselung bei der Datenübertragung via Internet- und E-Mail für alternativlos bzw. als „das tatsächliche Mittel der Wahl". Das VG Berlin dagegen hat eine Anordnung der Datenschutzbehörde an einen Personalvermittler für unverhältnismäßig gehalten, die Übertragung von Bewerberdaten per E-Mail an potentielle Arbeitgeber zu verschlüsseln.[29] Jedenfalls aber bei der Übermittlung besonderer persönlicher Daten (§ 3 Abs. 9 BDSG) wird eine Verschlüsselungspflicht bei E-Mails angenommen.[30]

Auch für die elektronische Übermittlung von Gehaltsdaten zwischen Privaten (etwa zwischen Arbeitgeber und Lohnbüro/Gehaltsbuchhaltung) ist von einer Verschlüsselungspflicht auszugehen. Wenn der Gesetzgeber dem Arbeitgeber die Verschlüsselung für die Meldung von Gehaltsdaten an die Steuer- und Sozialversicherungsbehörden vorgeschrieben hat (siehe oben), ist kein Grund ersichtlich, weshalb für die Übermittlung derselben Daten zwischen Privaten ein geringerer Schutzbedarf bestehen könnte.

Die vorgenannten Regelungen sehen jeweils eine Verschlüsselung „nach dem Stand der Technik" vor. Dieses Kriterium ist erfüllt, wenn das angewendete Verschlüsselungsverfahren in der Praxis bewährt ist und einen hohen Sicherheitsstandard hat.[31] Es scheiden hiernach alle Verfahren aus, zu denen bereits Sicherheitslücken festgestellt wurden sowie solche, die für den jeweiligen Schutzzweck untauglich sind: Transportverschlüsselung schützt Inhalte nur für ein kurzes Segment, „schwache" Passphrasen sind zu schnell zu „knacken" und die Dateiverschlüsselung mancher Office-Produkte können auch Anfänger leicht umgehen, da zu diesem Zweck Software im Internet erhältlich ist (siehe oben Ziffer II. 1. h, cc).

2. Inhalt und Sorgfaltsmaßstab vertraglicher Geheimhaltungspflichten

Wenn Vertragspartner miteinander kommunizieren, kann sich eine Verschlüsselungspflicht aufgrund einer ungeregelten, nebenvertraglichen Geheimhaltungspflicht oder einer ausdrücklichen Verschwiegenheitsregelung ergeben. Mit oder ohne Vertraulichkeitsregelung stellt sich die Frage, ob eine Verschlüsselung von E-Mails deswegen entbehrlich ist, weil die unbefugte Kenntnisnahme von E-Mails durch Dritte strafbar ist.

a) Verschlüsselungspflicht als vertragliche Nebenpflicht ohne ausdrückliche Regelung

Ohne ausdrückliche Regelung kann sich eine Verschlüsselungspflicht als Bestandteil einer nebenvertraglichen Geheimhaltungspflicht ergeben. Ob zu verschlüsseln ist, kann dabei nur anhand der konkreten Umstände des Einzelfalls beurteilt werden. Als maßgebliche Kriterien werden diskutiert:

- Der *Grad der Vertraulichkeit* der Information: Als besonders schützenswert werden z. B. Betriebs- und Geschäftsgeheimnisse, Passwörter, Angebote und Verträge genannt.[32] Auch die Verschlüsselung beim E-Banking ergibt sich z. T. aus der nebenvertraglichen Geheimhaltungspflicht der Bank.[33] Allerdings gibt es seit *Big Data* keine unbedeutenden Daten mehr.[34] Die graduelle Abstufung der Vertraulichkeit einer Information wird deshalb zunehmend schwieriger.
- Jeder kann selbst darüber entscheiden, ob er seine personen- oder unternehmensbezogenen Daten schützen möchte.[35] Folglich ist bei der Frage der Verschlüsselung auch zu beachten, wessen Daten von der digitalen Kommunikation betroffen sind. Sensibel sind daher grundsätzlich Daten Dritter, die nicht unmittelbar am Kommunikationsvorgang beteiligt sind.
- Teilweise wird von einem Verzicht auf Verschlüsselung ausgegangen, wenn die schutzberechtigte Vertragspartei selbst unverschlüsselt kommuniziert.[36] Die Aussagekraft dieses Kriteriums ist jedoch sehr begrenzt, denn die Geheimhaltungsbedürftigkeit richtet sich nach der jeweils betroffenen Information und nicht nach der Kommunikationsform, die für eine andere Information gewählt wurde. Im Ausgangsfall (siehe Ziffer I) könnte z. B. der Automobilbauer A den K unverschlüsselt um ein Angebot gebeten haben, während das von K erstellte Angebot selbst dagegen sensible und verschlüsselungspflichtige Tatsachen enthalten kann.
- Wenn der jeweilige Informationsempfänger Möglichkeiten zur verschlüsselten Kommunikation bereithält, sollten diese vom Absender auch genutzt werden.[37]
- Falls sich durch die Anwendung der Verschlüsselung eine Erschwerung der E-Mail-Kommunikation ergibt, wäre dieser Punkt in die Interessenabwägung einzubeziehen. Zumindest das OLG Köln hat mit diesem Argument das Erfordernis der Signatur bzw. Verschlüsselung einer E-Mail für den Nachweis einer Gerichtsstandsvereinbarung gemäß Art. 23 EuGVO abgelehnt.[38] Die Tragfähigkeit dieses Arguments ist jedoch fraglich, da das Gericht im entschiedenen Fall nicht differenziert zwischen Verschlüsselung und Signatur (zu diesem Unterschied siehe oben Ziffer II. 1. f.). Zudem ist eine Erschwernis aus technischer Sicht kaum zu begründen; die geeignete Software reduziert den Aufwand beim Versenden einer verschlüsselten E-Mail auf einen Klick.

b) Verschlüsselung bei ausdrücklicher vertraglicher Geheimhaltungsregelung (NDA)

Auch eine ausdrückliche Geheimhaltungsvereinbarung (NDA) regelt nur selten, dass und wie elektronische Nachrichten zu verschlüsseln sind. Dies trifft auch auf die vom VDA empfohlene Klausel im Beispielsfall zu (siehe oben

29 *Klett/Lee*, CR 2008, 644, 647; *Plath*, in: Plath (Hrsg.), BDSG, 2012, § 9 Rn. 59; VG Berlin, 24. 5. 2011 – 1 K 133.10, CR 2012, 191.

30 *Ernestus*, in: Simitis (Hrsg.), BDSG, 8. Aufl. 2014, § 9 Rn. 175; *Karg*, in: Wolff/Brink (Fn. 27), § 9 Rn. 46.

31 *Ernestus*, in: Simitis (Fn. 30), § 9 BDSG Rn. 171; *Stiemerling/Hartung*, CR 2012, 60, 66. Konkrete rechtliche Bewertungen zum Stand der Technik einzelner Verschlüsselungsverfahren bietet *Bergt*, in: Taeger (Hrsg.), Big Data & Co. – Neue Herausforderungen für das Informationsrecht, DSRI-Herbstakademie 2014, 2014, S. 571, 577.

32 *Backu*, ITRB 2003, 251 f.; *Klett/Lee*, CR 2008, 644, 645. Im Beispielfall (Ziff. I) würde sich daher eine Verschlüsselungspflicht für die E-Mail des K ergeben, da diese ein Angebot enthält.

33 *Gößmann*, in: Schimansky/Bunte/Lwowski (Hrsg.), Bankrechtshandbuch Band I, 3. Aufl. 2007, § 55 Rn. 13 ff. Die Verschlüsselung liegt auch im Eigeninteresse der Banken, da diese z. T. für Fehlbuchungen haften, siehe § 675 u BGB und BGH, 24. 4. 2012 – XI ZR 96/11, K&R 2012, 504 ff. = NJW 2012, 2422. In technischer Hinsicht ist durch Verschlüsselung Online-Banking überhaupt erst sicher umsetzbar.

34 *Taeger/Schmidt*, in: Taeger/Gabel (Hrsg.), BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2014, Einführung BDSG Rn. 3.

35 *Wytibul*, ZD 2013, 539, 542; *Stancke*, BB 2013, 1418, 1424 f.

36 *Backu*, ITRB 2003, 251, 252; ebenso wohl *Herrn*, NWB 2012, 4249, 4250.

37 Die VW AG stellt ihren Zulieferern sogar eine verschlüsselte Web-Plattform zur Verfügung (http://www.vwgroupsupply.com).

38 OLG Köln, 24. 4. 2013 – I-16 U 106/12.

Ziffer I). Folglich ist die VDA-Geheimhaltungsvereinbarung auszulegen.[39]

Aus der Systematik und Entstehung der Klausel ergeben sich keine Erkenntnisse, zumal der VDA selbst hierzu keine Informationen zur Verfügung stellt.[40] Aus dem Wortlaut lässt sich die Vermeidung des „Zugriffs Dritter auf die Informationen" als Zweck der Regelung ableiten. Hierbei ergibt sich eine Parallele zu den gesetzlichen Verschlüsselungspflichten (siehe oben Ziffer III. 1.). Diese bezwecken nach ihrem Wortlaut bzw. der Gesetzesbegründung den Schutz (meist personenbezogener) Daten vor unbefugtem Zugriff, insbesondere bei der Datenübertragung durch öffentlich zugängliche Netze. Der Gesetzgeber führt damit seinen Schutzauftrag aus, der sich aus den Schutzpflichten der betroffenen Grundrechte ergibt. Dieser Schutzauftrag verpflichtet den Staat, bei Gefährdungssituationen der in Rede stehenden Grundrechte aktiv geeignete Maßnahmen zu treffen.[41]

Wie die grundrechtliche Schutzpflicht vermittelt auch die VDA-Regelung die Pflicht an die Vertragspartner, aktiv Maßnahmen zum Schutz der Informationen zu treffen. Da es bei der Kommunikation über öffentlich zugängliche Netze keine andere geeignete Schutzmöglichkeit als die Verschlüsselung gibt (siehe oben II. 1. j), verdichtet sich im Beispielsfall die Geheimhaltungs- zur Verschlüsselungspflicht.

Laut VDA-Vereinbarung ist auch die „Bezeichnung des Projekts" geheimhaltungsbedürftig. Die Geheimhaltungspflicht ist im Beispielsfall daher nur gewahrt, wenn K für seine E-Mail eine Ende-zu-Ende-Verschlüsselung einsetzt und dabei keine projektrelevanten Daten wie etwa den Projektnamen in die Betreffzeile der E-Mail aufnimmt. Denn der Betreff einer E-Mail zählt zu den sogenannten „Meta-Daten", die selbst bei einer Ende-zu-Ende Verschlüsselung offen liegen.[42]

c) Ist die Verschlüsselung wegen des Vertrauensgrundsatzes entbehrlich?

Der sogenannte „Vertrauensgrundsatz" setzt voraus, dass sich jeder im Rahmen seiner Pflichtenkreise ordnungsgemäß verhält; Pflichtwidrigkeiten anderer schließen eigene Sorgfaltswidrigkeiten aus.[43] Im Beispielsfall (Ziffer I) könnte K deswegen auf die Verschlüsselung seiner Mails verzichten, wenn er darauf vertrauen darf, dass unbefugte Dritte nicht mitlesen. Schließlich ist das unbefugte „Mitlesen" von E-Mails gemäß § 202 b StGB strafbar, auch wenn diese nicht verschlüsselt sind.[44] Dieses Vertrauen ist jedoch nicht geschützt, wenn es einen triftigen Anlass gibt, mit dem Fehlverhalten Dritter zu rechnen.[45] Für den digitalen Nachrichtenaustausch ist folgendes zu erwägen:

Einzuräumen ist zwar, dass bislang keine belastbaren Daten dazu publik sind, wie häufig E-Mails während des Übertragungswegs unbefugt gelesen werden. Selbst als nach den „*Snowden*-Enthüllungen" wegen der NSA-Spionage ca. 2000 Strafanzeigen erhoben wurden, hat der Generalbundesanwalt in diesen Fällen keinen Anfangsverdacht zur Einleitung von Ermittlungen gesehen.[46]

Jedoch hat das Europäische Parlament bereits im Jahr 2001 festgestellt, dass staatliche Nachrichtendienste flächendeckend private und kommerzielle Kommunikation abhören.[47] Seit *Snowden* ist weiterhin bekannt, mit welchen Methoden digitale Kommunikation abgehört und ausgewertet wird,[48] und damit auch, dass sowohl der Wille als auch die Fähigkeit zur flächendeckenden E-Mail-Überwachung existieren. Die IT-Sicherheit definiert den *Willen* und die *Fähigkeit* eines Täters als maßgebliche Kriterien für die Analyse von Bedrohungen.[49] Somit liegt ein reales Bedrohungsszenario vor für geheimhaltungsbedürftige Informationen beim unverschlüsselten Datenverkehr. Folglich gibt es einen triftigen Anlass, nicht darauf zu vertrauen, dass E-Mails gemäß der Anforderung des § 202 b StGB nicht unbefugt auf den Transportweg gelesen werden.[50]

Gegen das Vertrauen auf die Einhaltung des § 202 b StGB spricht weiter, dass die Norm nicht in jedem Fall zweifelsfrei anwendbar ist. Denn beim E-Mail-Austausch werden weltweit verteilte Server und Netze eingesetzt, auch wenn Absender und Empfänger in Deutschland sind (siehe oben Ziffer II. 4). Liest der Täter die abgefangene E-Mail außerhalb Deutschlands, gilt das deutsche Strafrecht jedenfalls nicht nach § 3 StGB (Geltung für Inlandstaten). Auch die Anwendbarkeit nach § 9 Abs. 1 StGB ist fraglich, da sich der Taterfolg (das „Sich-Verschaffen" von Daten) am Bildschirm des Täters realisiert (sofern man § 202 b nicht als Gefährdungsdelikt versteht). Tritt jedoch der Taterfolg außerhalb Deutschlands ein, gilt das StGB nicht.[51] Überdies stellen sich die in der Praxis fast unlösbaren Probleme der internationalen Strafverfolgung.

IV. Fazit und Thesen

1. Beim digitalen Nachrichtenaustausch ist stets zu prüfen, ob eine spezialgesetzliche Regelung die Verschlüsselung anordnet. Die Anzahl solcher Regelungen steigt.

39 *Klett/Lee*, CR 2008, 644, 645. Zur Vertragsauslegung und den maßgeblichen Gesichtspunkten Wortlaut, Systematik, Entstehung/Begleitumstände, Zweck siehe *Wendtland*, in: Bamberger/Roth, BGB, 2014, § 157 Rn. 11 ff.

40 Dies hat der VDA den Verfassern auf deren Frage per E-Mail mitgeteilt.

41 Der Schutzauftrag aus Art. 2 Abs. 1 und 1 Abs. 1 GG im IT-Bereich wurde zuletzt ausdrücklich herausgearbeitet etwa von *Masing*, NJW 2012, 2305, 2306; *Gurlit*, NJW 2010, 1035, 1040; *Heckmann*, in: Rüssmann, FS-Käfer, 2009, S. 129 ff., Ziffer I 2; zur Pflicht des Gesetzgebers, aktiv zu werden BVerfG, 29. 10. 1987 – 2 BvR 624/83, BVerfGE 77, 170, 215 – Lagerung chemischer Waffen; *Hoffmann/Borchers/Schulz*, MMR 2014, 89, 92.

42 siehe oben Ziffer II. 1. h) dd); ebenso *Koch*, Verschlüsselung in der privaten und beruflichen Praxis, 2014, Kapitel „Verschlüsselung der Metadaten".

43 *Spindler*, in: Bamberger/Roth (Fn. 39), § 823 Rn. 244; *Vogel*, in: Laufhütte/Rissing-van Saan/Tiedeman, StGB, Band 1, 12. Aufl. 2009, § 15 Rn. 224 ff.

44 *Hilgendorf* in: Laufhütte/Rissing-van Saan/Tiedemann, StGB, Band 6, 12. Aufl. 2009, § 202 b Rn 9.

45 BGH, 18. 7. 2006 – X ZR 44/04, NJW 2006, 2918, 2919; *Spindler*, in: Bamberger/Roth (Fn. 39), § 823 Rn. 244; *Vogel*, in: Laufhütte/Rissing-van Saan/Tiedeman (Fn. 43), § 15 Rn. 227.

46 Pressemitteilung 17/2014 des Generalbundesanwalts unter https://www.generalbundesanwalt.de/txt/showpress.php?themenid=16&newsid=506, abgerufen am 6. 12. 2014.

47 Das satellitengestützte „Echolon-System" zielte jedoch nicht auf das Internet ab, http://www.europarl.europa.eu/sides/getDoc.do?type=PRESS&reference=DN-20010905-1&format=XML&language=DE#SECTION1.

48 Abhören an Internetknotenpunkten und Glasfaserkabeln; Auswertung der „Meta-Daten" mittels „Big-Data-Anwendungen", Heise Newsticker v. 22. 6. 2013, http://www.heise.de/newsticker/meldung/Bericht-Britenschnueffeln-Internet-noch-massiver-aus-als-die-USA-1894852.html („Bericht: Briten schnüffeln Internet noch massiver aus, als die USA").

49 siehe z. B. *Boehmer*, in: Katzenbeisser/Lotz/Weippl (Hrsg.), Sicherheit 2014, 2014. S. 305, 314 ff.

50 Auch *Kirchberg* (BRAK-Mitteilungen 2014, S. 170) fordert – allerdings von der Anwaltschaft mit Blick auf das Berufsgeheimnis – ein „Umdenken" beim derzeit „naiven Umgang" mit der E-Mail-Kommunikation. *Voßhoff/Büttgen* rufen in ZRP 2014, 232 ff. ebenso zur Nutzung der vorhandenen Verschlüsselungslösungen auf.

51 *Marbeth-Kubicki* (Fn. 19), Kapitel 26 Rn. 23, sofern man nicht den Taterfolg im „Datenabfluss" sieht, der beim Opfer in Deutschland eintritt und von § 5 Nr. 7 StGB (Verletzung von Geschäftsgeheimnissen deutscher Unternehmen) absieht. Soweit dem ausländischen Täter nicht bekannt ist, dass er E-Mails aus Deutschland abfängt, wo die Tat strafbar ist, kann zudem der Vorsatz (Tatbestandsirrtum) oder die Schuld (Erlaubnisirrtum) fraglich sein.

2. Zwischen Vertragspartnern kann ohne eine ausdrückliche Regelung die Verschlüsselung aufgrund einer vertraglichen Nebenpflicht nötig sein. Da hier zahlreiche Kriterien im Einzelfall gegeneinander abzuwägen sind, steigt die Rechtsunsicherheit ohne eine ausdrückliche Vertragsvereinbarung, je komplexer die technischen Sachverhalte werden.

3. Bei ausdrücklichen vertraglichen Geheimhaltungspflichten ist durch Auslegung zu ermitteln, ob digitale Nachrichten zu verschlüsseln sind. Dabei ist bei Wortlauten wie z. B. „vor Zugriffen Dritter schützen" prima facie eine Verschlüsselungspflicht anzunehmen.

4. Es gibt ein reales Bedrohungsszenario, wonach E-Mails von unbefugten Dritten erfasst, ausgewertet und bei Bedarf mitgelesen werden. Deshalb kann bei der Frage, ob eine bestimmte digitale Nachricht zu verschlüsseln ist, nicht auf die Einhaltung des § 202 b StGB (Abfangen von Daten) vertraut werden.

5. Für eine sichere Verschlüsselung ist eine End-Zu-End-Verschlüsselung nötig. Eine Transportverschlüsselung wie bei DE-Mail entspricht nicht dem Stand der Technik.

RA/FA IT-Recht Peter Kaumanns, LL.M. und RA/FA ArbR Sebastian Böhm, Düsseldorf*

Arbeitsrecht & Neue Medien

Eine Übersicht der aktuellen Rechtsprechung

Die fortschreitende Entwicklung der Arbeitswelt hat seit einigen Jahren auch die (Arbeits-)Gerichte erreicht. Neben klassischen Kündigungsrechtsstreitigkeiten sind in letzter Zeit vermehrt Verfahren geführt worden, die auf den wachsenden und neuen Nutzungsmöglichkeiten der Neuen Medien begründen. Schwerpunkte zeichnen sich insbesondere in den Bereichen Soziale Netzwerke, Internetnutzung am Arbeitsplatz und Datenschutz ab. Der nachfolgende Beitrag stellt eine Übersicht interessanter Entscheidung der Schnittstellen des Arbeitsrecht und der Neuen Medien dar.

I. Kündigungen mit Bezug zur Nutzung neuer Medien

Kündigungsrelevante Sachverhalte im Zusammenhang mit neuen Medien liegen zumeist in der innerbetrieblichen (exzessiven[1] bzw. illegalen) Nutzung der neuen Medien im Rahmen der Arbeitszeit begründet oder entstehen dadurch, dass insbesondere kritische Äußerungen, durch Arbeitnehmer gegenüber ihrem Arbeitgeber, Kunden,[2] Vorgesetzten[3] oder Kollegen auf sozialen Netzwerken[4] oder im Internet kundgetan werden.

1. Illegale Downloads am Arbeitsplatz

Illegale Downloads am Arbeitsplatz, insbesondere durch sogenannte Filesharing-Programme können als erhebliche Pflichtverletzung zu einer fristlosen Kündigung führen, wenn die Downloadaktivitäten zweifelsfrei dem zu kündigenden Arbeitnehmer zugerechnet werden können. Das LAG Hamm hatte über zwei fristlose Kündigungen eines als Informationstechniker bei einer Polizeibehörde beschäftigten Arbeitnehmers zu entscheiden.[5] Es ist zu dem Ergebnis gekommen, dass die gegenüber dem Arbeitnehmer ausgesprochenen Kündigungen unwirksam waren, weil kein wichtiger Grund für die sofortige Beendigung des Arbeitsverhältnisses gegeben war.[6] In der Funktion als Informationstechniker standen dem Kläger zwei Computer, ein Desktop-Rechner und ein Notebook zur Verfügung, weiterhin ein allgemein genutztes Notebook in seinem Büro.

Durch Dritte wurde die Polizeibehörde darauf hingewiesen, dass unter einer ihr zuzuordnenden IP-Adresse ein Musikalbum mittels des Filesharing-Systems BitTorrent zum illegalen Herunterladen verfügbar gemacht wurde. Die Polizeibehörde erstattete darauf Strafanzeige und nahm Ermittlungen auf. Auf dem Desktop-Rechner des Klägers und dessen Notebook wurden daraufhin Hinweise auf das Vorhandensein spezieller Software zum unwiederbringlichen Löschen, Filesharing-Programme sowie urheberrechtlich geschützte diverse Musikartikel und sonstige urheberrechtliche Werke gefunden. Dem Arbeitnehmer wurden fristlose Kündigungen ausgesprochen, gegen die er sich wehrte.[7] Der Arbeitgeber war der Auffassung, dass dem Arbeitnehmer die Downloads eindeutig zuzuordnen waren, da es die ihm zugeordneten Rechner waren, die in seinem abschließbaren Büro standen. Der Arbeitnehmer konnte darstellen, dass er bei der Hälfte der ermittelten Downloadvorgänge nicht in seinem Dienstzimmer war und ein Drittzugriff auf seine Rechner jederzeit auch durch andere Mitarbeiter möglich war. Gegen die Ortsabwesenheit hat der Arbeitgeber auf die Möglichkeit hingewiesen, Downloadvorgänge auch zeitgesteuert ohne Mitwirkung vor Ort in Gang zu setzen.

Das LAG Hamm hat mit dem erstinstanzlichen Arbeitsgericht[8] entschieden, dass ein wichtiger Grund für eine fristlose Kündigung nicht nachgewiesen ist. Es habe der Nachweis nicht erbracht werden können, dass die illegalen Downloads eindeutig dem Arbeitnehmer zuzuordnen waren. Die Rechner des Klägers hätte grundsätzlich auch von anderen Mitarbeitern genutzt werden und eine Anmeldung zum System ohne Kennworteingabe erfolgen können. Auch die Ortsabwesenheit des Arbeitnehmers spräche gegen seine

* Mehr über die Autoren erfahren Sie auf S. XII.

1 So. z. B. LAG Niedersachsen, 31. 5. 2010 – 12 SA 875/09, K&R 2010, 613 f.

2 So z. B. VGH München, 29. 2. 2012 – 12 C 12.264.

3 So z. B. ArbG Dessau-Roßlau, 21. 3. 2012 – 1 Ca 148/11, K&R 2012, 442 f.

4 So z. B. LAG Rheinland-Pfalz, 21. 10. 2011 – 9 Sa 110/11.

5 LAG Hamm, 6. 12. 2013 – 13 Sa 596/13.

6 Neben dem illegalen Download hatten sich die Instanzen auch mit weiteren Vorwürfen (Unterschlagung, Betrug, Computersabotage) beschäftigt, die allerdings aus Tatsachengründen nicht durchgriffen. Die Darstellung bezieht sich alleine auf den Vorwurf des illegalen Downloads/dessen Nachweisbarkeit.

7 Formale Einwendungen über Personalratsanhörung, etc. werden ebenfalls nicht dargestellt.

8 ArbG Arnsberg, 23. 4. 2013 – 1 Ca 1139/12.