BUNDESRECHTSANWALTSKAMMER

BRAK MAGAZIN

AUGUST 2015 · AUSGABE 4/2015

WIE BEKOMME ICH MEIN beA?

Die Sicherheitsarchitektur des beA
IT-Sicherheit in der Kanzlei
Sichere elektronische Mandantenkommunikation

ottoschmidt

© Coloures-pic - Fotolia.com

Wer den bestellt, bekommt mehr Geld.

Schneider/Herget **Streitwert-Kommentar** für Zivilprozess und FamFG-Verfahren. *Begründet von Dr. Egon Schneider, in der 11. Auflage fortgeführt von Richter am AG Kurt Herget. Ab der 12. Auflage bearbeitet von RA Norbert Schneider, Richter am LG Ralf Kurpat, RA Norbert Monschau, Richter am OLG Mark Noethen, LL.M. (USA) und RAin Lotte Thiel. 14., neu bearbeitete und erweiterte Auflage 2015, rd. 1.800 Seiten Lexikonformat, gbd. 139,– €. Erscheint im September. ISBN 978-3-504-47092-0*

Kein anderes Werk amortisiert sich schneller als der Streitwert-Kommentar – das unangefochtene Standardwerk zu einem durchweg geldwerten Thema. Durch schnelle und einfache Ermittlung der richtigen Werte in allen zivilrechtlichen Fällen.

Mehr als 480 alphabetisch geordnete Stichwörter zu praktisch allen relevanten Streitwertfragen, getrennt nach ZPO- und FamFG-Verfahren, ermöglichen Ihnen in jeder Situation auf Anhieb über den richtigen Wertansatz Auskunft zu geben.

Mit vielen Fall- und Berechnungsbeispielen, einsatzbereiten Schriftsatzmustern, Hinweisen auf typische Fehlerquellen und kritischer Verarbeitung der Flut neuer Rechtsprechung, die in dem kasuistisch geprägten Rechtsgebiet von entscheidender Bedeutung ist.

Schneider/Herget, Streitwert Kommentar. Jetzt Probe lesen und bestellen bei **www.otto-schmidt.de/sk14**

ottoschmidt

BITTE EINSTEIGEN....

RA Christoph Sandkühler,
Vorsitzender des Ausschusses Elektronischer Rechtsverkehr der BRAK

Am 1.1.2016 ist es soweit: Jeder in der Bundesrepublik zugelassene Rechtsanwalt wird ein beA haben, sein eigenes ‚besonderes elektronisches Anwaltspostfach'.

Der Gesetzgeber wollte dieses neue Kommunikationsmittel für jede Anwältin und jeden Anwalt. Deshalb wurde die BRAK gesetzlich mit einem neuen § 31a BRAO beauftragt, für alle ca. 165.000 Kolleginnen und Kollegen ein beA einzurichten.

Das heißt, ab dem 1.1.2016 wird jeder von Ihnen ein digitales Postfach besitzen, das – und jetzt kommt das Wichtigste – ab diesem Datum empfangsbereit ist. Sämtliche Kollegen und alle Gerichte, die an den Elektronischen Rechtsverkehr angeschlossen sind, können Sie ab dem 1.1.2016 über das beA adressieren und Ihnen auf diesem Weg Post zukommen lassen. Das gleiche gilt selbstverständlich auch umgekehrt.

Sie werden in einigen Tagen Post von der BRAK bekommen, in der erläutert wird, woher Sie Ihre beA-Karte bekommen und wie die Erstregistrierung im beA-System erfolgt. Diese Erstregistrierung ist wichtig, denn erst dann sind Sie in der Lage, auf Ihr Postfach zuzugreifen und damit zu arbeiten. Aber: Auch ohne Erstregistrierung können an Ihr Postfach Nachrichten geschickt werden. Von den Gerichten nach § 174 Abs. 3 ZPO und von jenen Kollegen, die auf das beA als den sicheren elektronischen Übermittlungsweg setzen. Der ein oder andere mag jetzt einwenden, dass in seinem Bundesland die Gerichte noch nicht am elektronischen Rechtsverkehr teilnehmen und daher kein Grund zur Sorge beziehungsweise zum Handeln in Form der Erstregistrierung besteht. Aber können Sie wirklich mit einhundertprozentiger Sicherheit ausschließen, dass Ihnen ein Gericht in einem Bundesland mit ERV-Teilnahme – Berlin, Brandenburg, Sachsen und Hessen – oder ein Kollege relevante Dokumente zusendet? Dann etwas zu verpassen kann möglicherweise haftungsrechtliche Folgen nach sich ziehen.

Sie sollten daher die – vielleicht etwas ruhigeren – Spätsommertage nutzen und sich um Ihr beA kümmern. Bestellen Sie bei der Bundesnotarkammer, die mit der Herstellung und dem Vertrieb beauftragt wurde, Ihre beA-Karte. Und machen Sie sich Gedanken über Ihre Büroorganisation im beA-Zeitalter: Wie viele Mitarbeiter sollen/dürfen auf mein Postfach zugreifen? Welcher Kollege oder welche Kollegin soll mich vertreten, wenn ich im Urlaub oder krankheitsbedingt abwesend bin? Von welchen Orten brauche ich einen Zugriff auf das beA? Im Büro, Zuhause, unterwegs? Die Antworten auf diese Fragen bestimmen auch die notwendige technische Ausstattung, beispielsweise die Art und Anzahl der Sicherheitsmittel für Ihr Postfach.

Vor einem Jahr hieß es noch: „beA kommt". Jetzt steht beA vor der Einfahrt. Alle Signale sind auf grün. Steigen Sie ein!

IT-SICHERHEIT IN DER KANZLEI

Rechtsanwalt Alfred Gass, Ass. jur. Iris Speiser, Europäische EDV-Akademie des Rechts gGmbH

Mit der verpflichtenden Einführung des besonderen elektronischen Anwaltspostfachs (beA) wird mit Beginn des Jahres 2016 ein wesentlich größerer Teil der Kommunikation zwischen Anwälten und Gerichten elektronisch ablaufen als dies in den meisten Kanzleien bisher der Fall war. Das beA soll hohe Sicherheitsstandards erfüllen und eine vertrauliche Kommunikation gewährleisten. Doch die Kette ist natürlich nur so stark wie das schwächste Glied – sprich: das Sicherheitskonzept kann nur funktionieren, wenn auch die übrigen in der Kanzlei eingesetzten IT-Komponenten hohe IT-Sicherheitsstandards erfüllen.

Für die Netzwerke großer Kanzleien stellt dies regelmäßig keine größeren Probleme dar, da bedingt durch deren Größe oftmals Fachpersonal vorhanden ist, das sich hauptamtlich um die Betreuung der Kanzleinetzwerke kümmert – auch wenn dies die Kanzleiinhaber natürlich nicht von ihrer rechtlichen Verantwortung für die IT entbindet. Anders sieht es oft in kleineren Kanzleien aus, in denen die Betreuung der IT-Infrastruktur oftmals von Mitgliedern der Kanzlei nebenamtlich oder aber durch externe Dienstleister wahrgenommen wird. Ausgehend von dem Szenario einer kleineren Kanzlei sollen hier einige typische Problemfelder im Bereich der IT-Sicherheit aufgezeigt werden.

RECHTEMANAGEMENT UND ZUGRIFFSKONTROLLE

Der naheliegendste Aspekt der IT-Sicherheit wird leider oft vergessen, obwohl er an erste Stelle stehen sollte: Der Anwender. Das beste IT-Sicherheitskonzept ist wertlos, wenn nicht alle Anwender dieses Konzept konsequent in ihre tägliche Arbeit integrieren – symptomatisch sei hier das berühmte auf der Unterseite der Tastatur oder unter der Schreibunterlage notierte Passwort genannt. Der erste Schritt eines IT-Sicherheitskonzepts sollte daher aus „Awareness Rising" bestehen, der Schaffung eines Sicherheitsbewusstseins. Gerade in einer kleinen Kanzlei mit einer überschaubaren Anzahl an Nutzern sollte das Konzept daher unter Einbeziehung aller Anwender erarbeitet werden. Es empfiehlt sich, unter anderem folgende Aspekte zu beachten:

Ein Angreifer, der auf ein System unbefugt Zugriff auf den Account eines Nutzers erlangt, wird zunächst nicht mehr Rechte erlangen können, als dieser Nutzer. Sind die Zugriffsrechte dieses Nutzers auf den Umfang beschränkt, der zur Erfüllung der Arbeitsaufgaben benötigt wird, beschränkt dies auch den Zugriff eines Dritten, der den Account des Mitarbeiters „hackt"

Sensible Papiere finden regelmäßig nach Feierabend den Weg in verschließbare Aktenschränke und Archivräume. Entsprechendes sollte auch für PCs, Server und Datenträger gelten. Insbesondere laufende Systeme sollten niemals unbeaufsichtigt bleiben und auch bei kurzfristigem Verlassen des Arbeitsplatzes gesperrt werden. Große Bedeutung kommt hier auch den USB-Schnittstellen von PCs zu, über die leicht Daten kopiert oder über USB-Sticks Schadsoftware eingeschleust werden kann. Es ist daher zu überlegen, nicht benötigte USB-Schnittstellen zu deaktivieren oder gar physisch unbrauchbar zu machen.

Schwer räumlich begrenzen lassen sich die Daten drahtloser Netzwerke. Es stellt sich daher zunächst die grundsätzliche Frage, ob in der Kanzlei ein WLAN tatsächlich benötigt wird. Will man jedoch auf den Komfort der Unabhängigkeit von einer Netzwerkdose nicht verzichten, so sollte durch geeignete Aufstellung des WLAN-Routers darauf hingewirkt werden, dass die eigenen Kanzleiräume optimal versorgt werden und nicht die Straße davor. Außerhalb der Geschäftszeiten kann das drahtlose Netzwerk komplett deaktiviert werden. Schon allein um eventuellen Haftungsansprüchen wegen illegaler Aktivitäten im Netz vorzubeugen sollten alle durch den Router unterstützten Sicherungsmöglichkeiten, insbesondere zur Verschlüsselung genutzt werden. Der bewusste Zugang für Dritte („Gast-WLAN") sollte nicht gewährt werden. Zudem ist zu empfehlen, den Zugriff auf Netzwerkressourcen mit einem zusätzlichen Passwort zu sichern, so dass unbefugte Personen – sollte es ihnen gelingen, unberechtigt auf das WLAN Zugriff zu erlangen – nicht automatisch

auch Daten auf den Rechnern in der Kanzlei einsehen können.

MOBILE GERÄTE

In unserer digitalen Gesellschaft spielen mobile Geräte eine immer wichtigere Rolle. So begeben sich auch Anwälte zunehmend nicht mehr mit dem Aktenstapel, sondern mit dem Notebook auf den Weg zum Mandanten oder zu Gericht. Das Smartphone dient längst nicht mehr nur zum Telefonieren, sondern ist mobile Kommunikationszentrale und dient zum Management von Terminen.

Mobile Geräte sind in einem erhöhten Maße der Gefahr von Diebstahl ausgesetzt. Es sollte daher zunächst über geeignete Maßnahmen zur Diebstahlsicherung nachgedacht werden. Dies kann von sicherheitsbewusstem Verhalten (Smartphone nicht offen auf den Tisch legen) bis zu Maßnahmen wie dem Anbringen von so genannten Kensington-Schlössern zur Sicherung von Notebooks und Tablet-PCs reichen. Teil eines Sicherheitskonzepts für Mobilgeräte ist aber auch, den Zugriff auf die Geräte zu beschränken. So kann eine Sperre bei bereits kurzer Inaktivität (z.B. kennwortgesicherter Bildschirmschoner, PIN-gesicherter Sperrbildschirm auf dem Smartphone) verhindern, dass Unbefugte bei kurzer Abwesenheit Zugriff erlangen, während die Verschlüsselung von Festplatten und Speicher des Smartphones die Daten auf den Geräten auch im Falle eines Diebstahls effektiv schützen können

Sinnvoll, aber oftmals aus Gründen der Bequemlichkeit nur schwer zu realisieren, ist die Trennung von beruflich und privat genutzten Geräten. Neben der Tatsache, dass Anwälte bereits aus berufsständischen Gründen streng auf eine getrennte Datenhaltung zwischen privaten und beruflichen Daten achten sollen, so stellen auch Familienangehörige, die Geräte im privaten Bereich mitnutzen, eine erhebliche Schwachstelle im IT-Sicherheitskonzept dar. Wenn sich eine solche duale Nutzung nicht vermeiden lässt, so sollten zumindest getrennte Zugangskennungen und Datenbereiche für beide Anwendungsszenarien eingerichtet werden. Einige Smartphones bieten inzwischen sogar die Möglichkeit, einen besonders gesicherten Bereich für besonders schützenswerte Daten einzurichten.

AKTUALITÄTSMANAGEMENT

Die Entwicklung von Schadsoftware und Software, die diese abwehren soll, ist ein stetiger Wettlauf. Zwar mögen die Schadsoftwareentwickler immer einen Schritt voraus sein – das Gros der

Schadsoftware die praktisch zum Einsatz kommt, ist bereits bekannt und kann von den aktuellen Versionen der auf dem Markt befindlichen Sicherheitssoftware auch abgewehrt werden. Voraussetzung ist allerdings, dass sich sowohl diese, als auch Betriebssystem und Anwendungssoftware auf dem jeweiligen Rechner auf aktuellem Stand befinden. An dieser Stelle kommt es jedoch gelegentlich zum Konflikt zweier Sicherheitsstrategien. Einerseits sollten die Nutzer eines Systems bei der täglichen Arbeit nicht über Administrationsrechte verfügen, da dies das System im laufenden Betrieb angreifbar macht. Andererseits werden für die Aktualisierung des Systems regelmäßig Administrationsrechte benötigt – insbesondere Anwendungssoftware unterstützt zwar oftmals automatischen Updateroutinen, verlangt jedoch die aktive Eingabe eines Administratorpasswortes. Um derartige Systeme dennoch auf aktuellem Stand zu halten, bedarf es der Aufstellung eines Updateplans, der regelmäßig durch einen Administrator abgearbeitet werden muss.

AUSFALLSICHERHEIT

Auf den ersten Blick ist das Thema Ausfallsicherheit keine Frage der IT-Sicherheit. IT-Sicherheit sollte aber auch die Sicherheit hinsichtlich der Verfügbarkeit der IT-Infrastruktur umfassen. Daher soll an dieser Stelle auf einige typische Ausfallszenarien und mögliche Lösungsansätze hingewiesen werden:

Datensicherheit beginnt bei der Datensicherung. Ab einer gewissen Datenmenge kann eine Datensicherung nicht mehr in kurzen Zeitabständen manuell auf einen externen Datenträger erfolgen; es bedarf einer Backup-Strategie. Regelmäßige Datensicherungen können im Haus auf ein Backup-System erfolgen (z.B. NAS-Server) oder aber außer Haus auf Systemen eines Dienstleis-

ters. Beides hat Vor- und Nachteile. Backups im eigenen Haus sind schnell verfügbar, bieten aber – z.B. im Falle eines Brandes – eine geringere Sicherheit. Backups außer Haus in der „Cloud" bergen hingegen ein potentielles Datenschutzrisiko. Insbesondere bei Anbietern im Ausland stellt sich das Problem der Auftragsdatenverarbeitung im Ausland. Im Falle einer Backup-Strategie, die auf einen Cloud-Anbieter setzt, sollte daher auf jeden Fall in inländischer, zertifizierter Anbieter ausgewählt werden, bei dem zusätzlich eine verschlüsselte Übertragung und Speicherung der Daten gewährleistet ist. Von Diensten mit Serverstandort im Nicht-EU-Ausland, die keine Verschlüsselung bieten (in diese Kategorie fällt leider auch der recht beliebte und komfortable Dienst „Dropbox") ist dagegen dringend abzuraten. Auf der sicheren Seite bewegt man sich, wenn man auf zertifizierte, speziell auf Anwälte zugeschnittene Angebote zurückgreift

Korrespondierend zur Planung des Backups ist auch an eine Wiederherstellungsstrategie zu denken. Insbesondere die Neuinstallation und Rücksicherung nach dem Ausfall von Hardwarekomponenten wird im Gegensatz zum Backup gelegentlich vernachlässigt, was im Schadensfall zu langen Ausfallzeiten führt, die den Betrieb einer Kanzlei empfindlich stören kann.

Während Hardwareausfälle zum Glück selten sind, sind kurzfristige Ausfälle der Netzinfrastruktur ein häufigeres Problem, das oftmals außerhalb der eigenen Einflusssphäre liegt. Gerade bei Umstellung auf den elektronischen Rechtsverkehr kann ein Ausfall der Internetverbindung kurz vor Fristablauf fatal sein – auch wenn Fristversäumnisse oftmals über Wiedereinsetzungsanträge abgefangen werden können. Bei der Auswahl des Internetanbieters sollte daher auf hohe Verfügbarkeit und ggf. das Vorhandensein alternativer Zugangsmethoden geachtet werden.

Natürlich kann dieser Artikel nur einen kleinen Auszug der Aspekte aufzeigen, mit denen sich die Inhaber einer Anwaltskanzlei im Hinblick auf ihre IT beschäftigen sollten. Vielfach werden sich die Verantwortlichen in einem Dilemma wiederfinden: Je komfortabler IT-Lösungen sind, um so unsicherer sind die tendenziell. Ein Mehr an Sicherheit geht hingegen regelmäßig mit höheren Kosten einher. Hier den optimalen Kompromiss zu finden, ist ohne professionelle Beratung – insbesondere für den wenig IT-affinen Anwalt – nur schwer zu leisten.

DAI Deutsches Anwaltsinstitut e.V.

FACHINSTITUT FÜR ARBEITSRECHT

27. Jahresarbeitstagung Arbeitsrecht

6. bis 7. November 2015
Köln

Neueste Entwicklungen im Kündigungsschutz
Stephanie **Rachor,** Richterin am Bundesarbeitsgericht, Erfurt

Alles rund um die Mitbestimmung nach § 87 BetrVG
Dr. Barbara **Reinhard,** Rechtsanwältin, Fachanwältin für Arbeitsrecht, Frankfurt am Main

Arbeitsvertrag – Werkvertrag – freie Mitarbeit – aktuelle Rechtsprechung und praktische Probleme
Waldemar **Reinfelder,** Richter am Bundesarbeitsgericht, Pressesprecher des Bundesarbeitsgerichts, Erfurt

Befristung und Leiharbeit im Spannungsfeld deutscher und europäischer Regulierung
Prof. Dr. Gregor **Thüsing,** LL.M., Universitätsprofessor, Rheinische Friedrich-Wilhelms-Universität Bonn

Aktuelles zum GmbH-Fremdgeschäftsführer aus arbeitsrechtlicher Sicht
Prof. Dr. Stefan **Lunk,** Rechtsanwalt, Fachanwalt für Arbeitsrecht, Hamburg

Mindestlohngesetz – erste Rechtsprechung und praktische Erfahrung
Dr. Mark **Lembke,** LL.M. (Cornell), Rechtsanwalt, Fachanwalt für Arbeitsrecht, Attorney-at-Law (New York), Frankfurt am Main

Leitung:	Bernd **Ennemann,** Rechtsanwalt und Notar, Fachanwalt für Arbeitsrecht, Soest
Zeitstunden:	10 – mit Nachweis zur Vorlage nach § 15 FAO (Arbeitsrecht)
Kostenbeitrag:	525,– € (USt.-befreit)
Nr.:	012251

Fortbildungsplus zur 27. Jahresarbeitstagung Arbeitsrecht
5. November 2015 · Köln · Nr. 012660

Die Jahresarbeitstagung und das Seminar ermöglichen Fachanwältinnen und Fachanwälten, ihre Pflichtfortbildung (15 Zeitstunden – § 15 FAO) an einem Termin wahrzunehmen.

Leitung:	Bernd **Ennemann,** Rechtsanwalt und Notar, Fachanwalt für Arbeitsrecht, Soest
Referenten:	Prof. Dr. Stefan **Greiner,** Universitätsprofessor, Rheinische Friedrich-Wilhelms-Universität Bonn
	Prof. Dr. Claudia **Schubert,** Universitätsprofessorin, Ruhr-Universität Bochum
	Werner **Ziemann,** Vors. Richter am Landesarbeitsgericht, Hamm
Zeitstunden:	5 – mit Nachweis zur Vorlage nach § 15 FAO (Arbeitsrecht)
Kostenbeitrag:	345,– € (USt.-befreit)
Paketpreis:	725,– € (USt.-befreit) für beide Veranstaltungen

Deutsches Anwaltsinstitut e.V. · Universitätsstr. 140 · 44799 Bochum
Tel. 0234 970640 · Fax 0234 703507 · arbeitsrecht@anwaltsinstitut.de

Das DAI ist eine Einrichtung von Bundesrechtsanwaltskammer, Bundesnotarkammer, Rechtsanwaltskammern und Notarkammern.

WWW.ANWALTSINSTITUT.DE

DAS ELEKTRONISCHE SCHUTZSCHRIFTENREGISTER

Rechtsanwalt Christopher Brosch, BRAK Berlin

Am 1. Januar 2016 wird nicht nur das besondere elektronische Anwaltspostfach (beA) empfangsbereit sein. Das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten sieht mit der Einrichtung eines elektronischen Schutzschriftenregisters eine weitere Neuerung vor, die Auswirkungen auf die Arbeitsweise von Rechtsanwältinnen und Rechtsanwälten haben wird.

HINTERGRUND

Bislang ist die Schutzschrift gesetzlich nicht geregelt, sie ist ein von der Praxis entwickeltes und gewohnheitsrechtlich etabliertes Rechtsmittel. § 945a Absatz 1 Satz 2 ZPO wird ab dem 1. Januar 2016 erstmals eine Definition der Schutzschrift enthalten: „Schutzschriften sind vorbeugende Verteidigungsschriftsätze gegen erwartete Anträge auf Arrest oder einstweilige Verfügung."

Ein „fliegender Gerichtsstand" führt dazu, dass ein Antrag auf Arrest oder einstweilige Verfügung bei sehr vielen Gerichten gestellt werden kann. Entsprechend muss eine Schutzschrift auch bei vielen Gerichten vorliegen, um zuverlässig ihre Wirkung entfalten zu können. Auch bei der Justiz entsteht durch die derzeitige Verfahrensweise hoher Aufwand; jede Schutzschrift muss zunächst registriert werden und in ein Verzeichnis eingetragen werden, obwohl zu den meisten Schutzschriften niemals ein entsprechender Verfügungsantrag eingeht.

REGISTER WIRD VERBINDLICH

Seit dem Jahr 2007 existiert ein privat betriebenes elektronisches Register, das gegen Zahlung einer Gebühr die Hinterlegung einer Schutzschrift ermöglicht und diese dann teilnehmenden Gerichten zum Abruf bereitstellt. Nach diesem Vorbild wird der neue § 945a ZPO zum 1. Januar 2016 die Einrichtung eines zentralen, länderübergreifenden elektronischen Registers für Schutzschriften vorsehen und damit erstmals eine gesetzliche Grundlage für ein Register schaffen. Über Verweisungen in § 62 Absatz 2 und § 85 Absatz 2 ArbGG wird das Schutzschriftenregister auch im arbeitsgerichtlichen Verfahren zur Anwendung kommen. Eine Schutzschrift gilt nach Absatz 2 der neuen ZPO-Vorschrift als bei allen ordentlichen Gerichten der Länder eingereicht, sobald sie in das Schutzschriftenregister eingestellt ist. Schutzschriften werden sechs Monate nach ihrer Einstellung in das Register gelöscht.

Besondere Bedeutung für Rechtsanwältinnen und Rechtsanwälte erhalten die Regelungen über das Schutzschriftenregister dadurch, dass zum 1. Januar 2017 mit § 49c BRAO eine berufsrechtliche Nutzungspflicht für das Schutzschriftenregister vorsehen werden wird. Rechtsanwältinnen und Rechtsanwälte werden verpflichtet sein, Schutzschriften ausschließlich zum Schutzschriftenregister nach § 945a ZPO einzureichen; eine Einreichung in Papierform ist demnach ausgeschlossen.

RECHTSVERORDNUNG

Einzelheiten des Betriebs des Schutzschriftenregisters sollen in einer Rechtsverordnung nach § 945b ZPO geregelt werden. Das Bundesministerium der Justiz und für Verbraucherschutz hat am 27. Februar 2015 den Entwurf einer entsprechenden Rechtsverordnung übersandt. Die BRAK hat in ihrer Stellungnahme Nr. 11/2015 die Einrichtung eines Schutzschriftenregisters ausdrücklich begrüßt, an einzelnen Bereichen des Verordnungsentwurfs jedoch Kritik geübt. Das Verordnungsgebungsverfahren ist derzeit noch nicht abgeschlossen.

TECHNISCHE UMSETZUNG

In technischer Hinsicht wird sich die Einreichung zum Schutzschriftenregister nicht wesentlich von anderen Bereichen des elektronischen Rechtsverkehrs unterscheiden. Dementsprechend ist die Regelung über die möglichen Einreichungswege zum Register in dem Entwurf der Rechtsverordnung jedenfalls stark an die künftige Vorschrift in der ZPO angelehnt. Eine Einreichung von Schutzschriften an das Schutzschriftenregister soll über das beA jedenfalls mit Inkrafttreten der berufsrechtlichen Nutzungspflicht am 1. Januar 2017 möglich sein; das Schutzschriftenregister soll über das beA wie ein Gericht adressiert werden können.

beA – Digital. Einfach. Sicher.

Ihr digitales Anwaltspostfach ab 2016.

Das besondere elektronische Anwaltspostfach beA ist der Zugang der Anwaltschaft zum elektronischen Rechtsverkehr.

Jeder Rechtsanwalt und jede Rechtsanwältin wird zum 1.1.2016 von der BRAK ein eigenes beA erhalten. Die Sicherheit hat bei der Entwicklung des beA oberste Priorität, denn Verschwiegenheit ist als Kernwert der anwaltlichen Tätigkeit fundamental für unseren Beruf. Ein besonders gesicherter Zugang zum Postfach und die Ende-zu-Ende-Verschlüsselung sämtlicher Nachrichten gewährleisten, dass nur die jeweiligen Absender und Empfänger beziehungsweise die von ihnen ausdrücklich befugten Personen erfahren können, welche Inhalte versendet wurden.

Alle Informationen zum beA im Web unter
www.bea.brak.de

FRISTSACHE!
01.01.2016
Jetzt informieren!

beA
Digital. Einfach. Sicher.

BUNDESRECHTSANWALTSKAMMER

beA – sicher

Die Sicherheitsarchitektur des beA

Rechtsanwalt Christopher Brosch, Rechtsanwältin Peggy Fiebig, BRAK, Berlin

Auf Grund des durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten in die BRAO eingefügten § 31a richtet die Bundesrechtsanwaltskammer zum 1. Januar 2016 für jeden Rechtsanwalt und jede Rechtsanwältin ein besonderes elektronisches Anwaltspostfach (beA) ein. Spätestens im Jahr 2022 verpflichtet das Gesetz überdies auch zur aktiven Nutzung des elektronischen Rechtsverkehrs.

Entsprechend den gesetzlichen Voraussetzungen wurde das beA mit einem besonders hohen Sicherheitsstandard entwickelt: Die Nachrichtenübertragung und auch das Postfach selbst sind gegen unbefugte Zugriffe geschützt.

Die Enthüllungen von Edward Snowden über die Aktivitäten verschiedener Geheimdienste, Berichte über Computerspionage im Deutschen Bundestag und auch die neuen Pläne zur Einführung einer Vorratsdatenspeicherung haben zu Fragen im Hinblick auf die Sicherheit elektronischer Kommunikation geführt. Nachfolgend soll daher ein Überblick über die Sicherheitsarchitektur des beA gegeben werden.

Ende-zu-Ende-Verschlüsselung

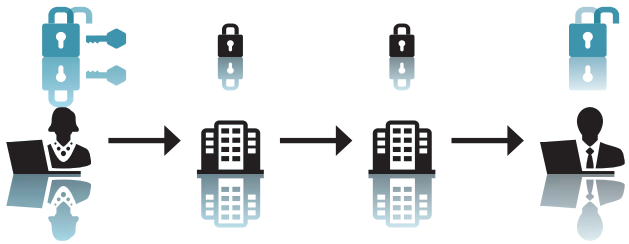
Entscheidend für die Vertraulichkeit der Übertragung von Nachrichteninhalten im beA ist eine durchgehende („Ende-zu-Ende“) Verschlüsselung – vom Webbrowser bzw. der Kanzleisoftware des Absenders bis zur Entschlüsselung durch den Empfänger. So gibt es keine Zwischenstationen, in denen die Nachrichten im Klartext vorliegen.

Verschlüsselt werden die zu übertragenden Nachrichten durch eine Kombination aus einem symmetrischen und einem asymmetrischen Verschlüsselungsverfahren. Beim symmetrischen Verfahren erfolgen Ver- und Entschlüsselung mit ein und demselben Schlüssel, der nicht öffentlich gemacht und deshalb auch nicht ungeschützt

dem Empfänger übertragen werden darf. Bei der asymmetrischen Verschlüsselung dagegen werden zwei Schlüssel – ein öffentlicher und ein privater – benötigt. Mit dem öffentlichen Schlüssel wird verschlüsselt, mit dem privaten entschlüsselt.

Da asymmetrische Verschlüsselungsverfahren erheblich mehr Rechenleistung benötigen und dadurch deutlich langsamer sind, wird beim beA die Nachricht selbst symmetrisch verschlüsselt, und lediglich der dazu verwendete Nachrichtenschlüssel wird asymmetrisch chiffriert.

Ende-zu-Ende-Verschlüsselung



Die Entschlüsselung der Nachrichten erfolgt dann direkt auf dem Computer des Empfängers. Von dieser Ende-zu-Ende-Verschlüsselung ausgenommen sind lediglich einzelne für den Nachrichtentransport erforderliche Metadaten wie die Angabe des Absender- und des Empfängerpostfachs. Aber auch diese Informationen werden bei der Übertragung durch das Internet mit einer Transportverschlüsselung geschützt und in verschlüsselten Datenbanken abgelegt.

Sichere Rechteverwaltung

Zur Abbildung einer Kanzleiorganisation aus mehreren Rechtsanwälten sowie Mitarbeitern stellt das beA eine umfassende Rechteverwaltung zur Verfügung, die es dem Postfachinhaber u.a. ermöglicht, anderen Personen Zugriff auf Nachrichten in seinem Postfach zu gewähren. Hierfür kommt ein sogenanntes Hardware Security Module (HSM) zur Anwendung. Ein HSM ist ein Gerät, das nur spezielle, vorab definierte kryptographische Funktionen ausführen kann und das gegen jede Art der Manipulation sowie gegen Abhören geschützt ist.

Durch das HSM wird der verschlüsselte Nachrichtenschlüssel nach Prüfung der Berechtigung für einen Leser – Mitarbeiter oder Postfachinhaber – „umgeschlüsselt"; dieser kann ihn anschließend mit seinem privaten Schlüssel entschlüsseln und mit dem nun im Klartext vorliegenden Nachrichtenschlüssel die Nachricht entschlüsseln. Durch Einsatz des HSM kann eine Nachricht im beA mehreren Personen zum Lesen bereitgestellt werden, ohne dass sie zu irgendeinem Zeitpunkt unverschlüsselt im System vorliegt. Die Standorte der beA-Rechenzentren einschließlich der HSM befinden sich in Deutschland – der genaue Ort wird als eine weitere Sicherheitsmaßnahme nicht öffentlich genannt.

Sicherer als Post und Fax

Es lohnt sich, im Vergleich zu der Nachrichtenübermittlung im beA einen kurzen Blick auf die anderen Kommunikationswege mit der Justiz, die bisher zur Verfügung stehen, zu richten: Ein gewöhnliches Telefax wird unverschlüsselt über öffentliche Telefonnetze übertragen; eine Kenntnisnahme Dritter kann daher nicht ausgeschlossen werden. Das Öffnen eines Briefes durch Dritte hinterlässt in der Regel zwar Spuren – einen Schutz gegen ein unbefugtes Lesen bietet der Papierbrief jedoch nicht. Absolute Vertraulichkeit ist nur schwer zu erreichen. Doch so viel steht fest: Gegenüber der Kommunikation mittels Telefax oder Brief bedeutet das beA einen gewaltigen Sprung nach vorn.

Doppelt hält besser

Lediglich ein Schutz der Datenübertragung wäre nicht ausreichend zur Gewährleistung der Vertraulichkeit. Auch vor und nach Ende der Datenübertragung zwischen zwei Postfächern müssen unberechtigte Zugriffe auf das beA verhindert werden. Entsprechend der gesetzlichen Vorgaben ist für den Zugriff auf das beA eine sichere Anmeldung unter Verwendung zweier voneinander unabhängiger Sicherungsmittel erforderlich. Durch diese so genannte Zwei-Faktor-Authentifizierung wird ein weit höheres Maß an Sicherheit erreicht als lediglich durch ein Passwort.

Zwei-Faktor-Authentifizierung

Vorgesehen ist, dass für jeden Zugriff auf das beA neben einer PIN (Wissen) entweder eine Chipkarte oder ein Softwarezertifikat (Besitz) verwendet werden muss. Dies gilt für Rechtsanwälte und – nach der Vergabe der entsprechenden

Berechtigungen – für Mitarbeiter gleichermaßen. Für Rechtsanwälte bietet es sich an, eine Chipkarte mit Signaturfunktion zu erwerben, denn nur so ist nicht nur der Zugriff auf das Postfach, sondern auch der Versand von Nachrichten möglich: Das ERV-Gesetz sieht bis Ende 2017 vor, dass Dokumente, die elektronisch bei Gericht eingereicht werden, qualifiziert elektronisch signiert sein müssen. Ab 2018 entfällt dieses Erfordernis, wenn die Dokumente vom Rechtsanwalt selbst (nicht von einem Mitarbeiter oder Vertreter) aus seinem beA-Postfach versandt wurden. Auch hierfür ist dann für die Anmeldung eine Chipkarte erforderlich, ein Softwarezertifikat wird voraussichtlich nicht genügen.

Wo Anwalt draufsteht, ist Anwalt drin

Damit sichergestellt wird, dass nur Rechtsanwälte ein beA besitzen, ist eine von der BRAK herausgegebene beA-Karte erforderlich, die jeder Rechtsanwalt und jeder Rechtsanwältin aus diesem Grund erwerben muss (Näheres zum Bestellverfahren siehe gegenüberliegende Seite). Die Karte enthält die eindeutige Bezeichnung des Postfachs und wird dem Rechtsanwalt bzw. der Rechtsanwältin getrennt von der dazugehörigen PIN übermittelt. Nur so lässt sich eine sichere Zuordnung eines Postfachs zum jeweiligen Besitzer gewährleisten. Zugleich wird das Risiko eines Missbrauchs von Zugangsinformationen ausgeschlossen, denn nur die Benutzung von Karte und PIN ermöglichen den Zugriff auf ein Postfach. Selbst wenn eine Karte bei ihrem Versand abgefangen würde, fehlt die getrennt versandte PIN.

Das beA basiert auf einem sicheren Verzeichnisdienst, der von der Bundesrechtsanwaltskammer betrieben wird. Nur wer hier eingetragen ist, wird ein beA-Postfach erhalten. Gespeist wird der Verzeichnisdienst aus den elektronischen Registern der Rechtsanwaltskammern nach § 31 Absatz 1 BRAO. Diese Daten werden in einem sicheren Verfahren von den Rechtsanwaltskammern an die Bundesrechtsanwaltskammer übertragen – eine elektronische Signatur der Rechtsanwaltskammer schließt dabei Manipulationen bei der Übertragung aus.

Das beA ermöglicht eine Kommunikation nur mit definierten und in die Verzeichnisse eingetragenen Postfächern. Während bei der E-Mail-Kommunikation die angezeigte E-Mail-Adresse sowie der Name frei bestimmt werden können und man sich daher – sofern nicht zusätzlich eine qualifizierte elektronische Signatur verwendet wird – nie sicher sein kann, dass der Kommunikationspartner, Absender oder Empfänger einer Nachricht, der ist, der er zu sein scheint, gilt beim beA: Wo Anwalt drauf steht, ist auch Anwalt drin.

Geht nicht, gibt's nicht

Für die anwaltliche Tätigkeit ist eine ununterbrochene Verfügbarkeit des beA-Systems von großer Bedeutung. Systemausfälle müssen verhindert werden und dürfen gerade auch kurz vor Ablauf eines Tages nicht vorkommen. Bereits bei der Konzeption wurde daher Wert darauf gelegt, dass technische Störungen, die sich nie vollständig ausschließen lassen werden, möglichst keine Auswirkungen auf den Betrieb des beA haben: Das beA-System wird in zwei örtlich getrennten Rechenzentren betrieben. An beiden Orten befindet sich dieselbe Hard- und Software. Neben der Lastverteilung dient dies der Ausfallsicherheit. Zusätzlich sind auch in jedem der beiden Rechenzentren Redundanzen vorhanden, die die Last und das Ausfallrisiko verteilen.

© Max Bauermann - Fotolia.com

Ergebnis

Zusammenfassend ausgedrückt: Das beA ist sicher. Die BRAK stellt jeder Rechtsanwältin und jedem Rechtsanwalt ein höchsten Anforderungen genügendes Kommunikationssystem zur Verfügung.
Ein wesentlicher Baustein der IT-Sicherheit ist jedoch auch das Verhalten der Anwender. Die dargestellten Maßnahmen verlieren an Wert, wenn etwa unberechtigte Personen Zugriff auf beA-Karte und PIN haben oder das beA von einem Computer (etwas in einem öffentlichen Internetcafe) genutzt wird, bei dem das Vorhandensein von Viren und Spionagesoftware nicht ausgeschlossen werden kann.

Wie bekomme ich mein beA?

Rechtsanwältin Peggy Fiebig, BRAK, Berlin

Alle Rechtsanwälte in der Bundesrepublik werden zum 1.1.2016 ein empfangsbereites beA-Postfach besitzen. Um es nutzen zu können, ist eine so genannte Erstregistrierung mit einer von der Bundesnotarkammer im Auftrag der BRAK herausgegebenen beA-Karte notwendig.

beA-Karte – der Schlüssel zum Postfach

Im August werden, nach den derzeitigen Planungen, alle Rechtsanwälte in der Bundesrepublik von der BRAK und der Bundesnotarkammer angeschrieben und über die beA-Karte informiert. Diese Karte stellt sicher, dass nur dazu befugte Personen Zugriff auf die jeweiligen Postfächer erhalten. Und es wird gewährleistet, dass ausschließlich Rechtsanwälte ein beA erhalten. Denn sie ist nur für jene erhältlich, die im Bundesweiten Amtlichen Anwaltsverzeichnis eingetragen sind. Auf dem Chip der beA-Karte ist sowohl der Name des jeweiligen Rechtsanwalts als auch die Postfachnummer enthalten, deshalb kann eine sonstige Signaturkarte zur Erstregistrierung nicht verwendet werden. Die beA-Karte ist jedoch anschließend auch für die tägliche Anmeldung am Postfach verwendbar und kann nach Wunsch mit einer Signierfunktion zur Erstellung einer qualifizierten elektronischen Signatur (qeS) aufgeladen werden.

Bestellung der beA-Karte

Mit der Herstellung und Ausgabe der beA-Karte wurde die Bundesnotarkammer beauftragt, die dazu eine Internetseite eigerichtet hat: www.bea.bnotk.de. Für den Bestellprozess ist eine eindeutige Identifikationsnummer erforderlich, die die BRAK jedem Rechtsanwalt in einem persönlichen Brief im August mitgeteilt. Sollten Sie das Schreiben bis Anfang September nicht erhalten haben, wenden Sie sich bitte an die Bundesnotarkammer. Die Kontaktdaten finden Sie am Ende dieses Artikels.

Die beA-Karte ist als beA-Karte Basis erhältlich, die für die Erstregistrierung und die tägliche Anmeldung verwendet werden kann. Außerdem besteht die Möglichkeit die Basiskarte mit einem Signaturzertifikat auszustatten, so dass darüber hinaus auch das Signieren von Dokumenten möglich ist (beA-Karte Signatur). Die beA-Karte Basis wird 29,90 Euro kosten, die beA-Karte Signatur 49,90 Euro, jeweils zzgl. Mehrwertsteuer. Für die Bestellung ist die Erteilung einer SEPA-Einzugsermächtigung erforderlich, außerdem muss für die weitere Kommunikation eine gültige E-mail-Adresse angegeben werden. Über die Bundesnotarkammer können auch Kartenlesegeräte und weitere Chipkarten zum Zugriff auf das beA-Postfach, beispielswiese für Mitarbeiter erworben werden.

Kartenversand und Erstregistrierung

Herstellung und Versand der beA-Karten Basis beginnen im Oktober. Es gilt dabei das „first come first served"-Prinzip – eine frühzeitige Bestellung lohnt also. Ab Mitte November wird der Zugriff auf die beA-Postfächer möglich sein, Karteninhaber können sich dann erstmalig am System registrieren. Erforderlich dafür sind neben einem internetfähigen Computer die beA-Karte und ein entsprechendes Kartenlesegerät. Ab 1.1.2016 kann das beA zum Versand und Empfang von Nachrichten genutzt werden. In den ersten Monaten des kommenden Jahres werden dann entsprechend den Bestellungen die qualifizierte elektronische Signatur zum Nachladen auf die Karte sowie die Mitarbeiterkarten und Softwarezertifikate zur Verfügung gestellt.

beA-Service

Für Fragen zum Bestellverfahren und zu den beA-Karten hat die Bundesnotarkammer eine E-Mail-Adresse bea@bnotk.de und für Eilfälle eine Telefonnummer 0800 - 3550 100 eingerichtet. Informationen zum beA selbst stehen Ihnen unter www.bea.brak.de zur Verfügung.

SIGNATUR UND SIGNIERVORGANG – FÜR ANWÄLTE

Walter Büttner, MBA (USQ) ist IT-Direktor der Bundesnotarkammer und Geschäftsführer der NotarNet GmbH.

Die qualifizierte elektronische Signatur ist ein eindeutiger digitaler „Schlüssel", der durch Anwendung sicherer kryptographischer Verfahren so mit Nutzdaten verknüpft und diesen beigefügt wird, dass eine nachträgliche Veränderung dieser Nutzdaten erkannt werden und über ein Verzeichnis, ähnlich Einträgen in einem Telefonbuch, die Urheberschaft an diesen langfristig überprüft werden kann. Spätestens wenn mit dem beA Schriftsätze an das Gericht versendet werden sollen, muss der Rechtsanwalt wissen, wie signiert wird.

RECHTLICHER RAHMEN UND HINWEISE

In der elektronischen Welt kann die handgeschriebene Unterschrift mit der qualifizierten elektronischen Signatur nach dem Signaturgesetz ersetzt werden. Schriftformäquivalenz wird nach § 126a BGB dadurch erreicht, dass das elektronische Dokument den Namen des Erklärenden enthält und es qualifiziert elektronisch signiert ist. Für Erklärungen im Verwaltungsverfahren gilt § 3a VwVfG entsprechend. Außerdem sehen die wesentlichen Prozessordnungen dauerhaft die Nutzungsmöglichkeit qualifiziert signierter Verfahrenserklärungen vor.

Zu beachten ist insbesondere, dass nach § 130a Abs. 3 ZPO (u.a.) mittels besonderen elektronischen Anwaltspostfachs (beA) ab 1.1.2018 nur Verfahrenserklärungen, nicht aber materiellrechtliche schriftformgebundene Erklärungen ohne qualifizierte Signatur abgegeben werden können. Umgekehrt ist für elektronisch erreichbare Gerichte bereits ab sofort die Übermittlung von qualifiziert signierten Schriftsätzen per EGVP und ab 1.1.2016 via beA zulässig. Die qeS ersetzt damit formelle und materielle Schriftform, soweit dies (im Ausnahmefall) nach § 126 Abs. 3 BGB nicht explizit ausgeschlossen ist.

SIGNATURVORGANG

Der Ablauf eines Signierprozesses ist denkbar einfach:

a) Dokument(e) laden
   Nach dem Scannen von Dokumenten oder dem Umwandeln von Word in z.B. PDF/A-Dokumenten können diese in der Signatursoftware (z.B. in beA bei der Zusammenstellung einer Nachricht) geladen werden.
b) Sichten
   Das Signaturgesetz gibt vor, dass alle zu signierenden Dokumente in einem sicheren Viewer angezeigt werden, damit der Signierende genau weiß, was er elektronisch unterzeichnet.
c) Signieren
   Nach der Sichtung wird durch Klick auf den Signieren-Button die (Stapel-) Signatur ausgelöst. Der Nutzer wird aufgefordert, seine PIN auf dem Kartenlesegerät bei gesteckter Signaturkarte einzugeben. Kommt es auf den Zeitpunkt der Signatur an, kann zusätzlich ein sog. Zeitstempel aufgebracht werden. Der Bildschirm zeigt an, wann der Signaturprozess abgeschlossen ist.
d) Verwenden
   Signierte Dokumente und dazugehörige Signaturdateien (im Regelfall im Format .pkcs7) können zusammen verwendet werden, z.B. für eine Übermittlung via EGVP. Dokumente sollen nach Wunsch der Justiz möglichst nicht „inline" signiert werden (PDF-interne Signatur), sondern mit separaten Signaturdateien. Außerdem sollen Dokumente und nicht die Nachricht selbst qualifiziert signiert werden. Der Empfänger kann damit prüfen, ob die übermittelten Daten unversehrt und welchen Ursprungs sie sind. Außerdem weist die Signaturprüfung bei Gericht aus, ob die verwendete Signaturkarte gültig, abgelaufen oder gesperrt war. Bei Verwendung eines Zeitstempels wird zusätzlich beweissicher angezeigt, zu welcher verbindlichen Zeit signiert wurden.

Die Signatur des Anwalts benötigt kein Berufsträgerattribut („Rechtsanwalt in ..., Rechtsanwaltskammer ..."). Stellvertretung bei der Aufbringung der Signatur ist nicht zulässig.

ELEKTRONISCHE KOMMUNIKATION MIT DEM MANDANTEN

Dr. Hendrik Schöttle, Fachanwalt für IT-Recht, Mitglied im Ausschuss Datenschutzrecht der BRAK

Spätestens seit der Snowden-Affäre ist das Thema Sicherheit bei elektronischer Kommunikation wieder in den Vordergrund gerückt. Für den Datenaustausch von Anwalt zu Anwalt oder zu den Gerichten wird es künftig das beA geben – wie aber erfolgt die Kommunikation mit den Mandanten? Einfach per E-Mail? Oder ist gerade sie nicht vielmehr so unsicher wie – ja, dieser Vergleich muss jetzt kommen – eine Postkarte? Für den Rechtsanwalt stehen immerhin seine berufsrechtliche Verschwiegenheitspflicht auf dem Spiel und das Risiko, gegen die aus dem Mandatsvertrag erwachsende Pflicht zur Interessenwahrung zu verstoßen.

E-MAILS UND TRANSPORTVERSCHLÜSSELUNG

Der Großteil aller in Deutschland versandten E-Mails geht unverschlüsselt über das Netz; unverschlüsselte E-Mails sind zudem vor einer unbefugten Kenntnisnahme strafrechtlich nicht geschützt. Damit ist der Blick in eine E-Mail nicht besser geschützt, als der auf eine Postkarte. So, in Kurzform, die Argumentation hinter dem Postkarten-Vergleich. Der Vergleich mag immer noch seinen Charme haben, die zugrunde gelegten Fakten sind allerdings überholt.

Nach einer Statistik eines Berliner E-Mail-Providers aus dem Jahr 2015 gingen bei diesem knapp 60% aller E-Mails verschlüsselt ein; über 86% aller ausgehenden E-Mails konnten zudem verschlüsselt zugestellt werden. Seit der Snowden-Affäre bieten viele E-Mail-Provider nicht nur verschlüsselte E-Mail-Kommunikation an, die vier größten deutschen E-Mail-Provider haben unverschlüsselte Kommunikationsschnittstellen zu ihren Kunden sogar komplett abgeschaltet – die Kunden sind also gezwungen, E-Mails verschlüsselt zu übermitteln. Das Bayerische Landesamt für Datenschutzaufsicht hat zudem im September 2014 mehr als 3.500 E-Mail-Server automatisiert auf das Vorhandensein von Verschlüsselung überprüft und in (nur) 750 Fällen eine fehlende Verschlüsselung beanstandet.

Um mögliche Missverständnisse gleich auszuräumen, sei klargestellt: Bei der hier genannten Verschlüsselung handelt es sich um sogenannte Transportverschlüsselung (Vielen unter den Abkürzungen TLS oder SSL ein Begriff). Das heißt, die E-Mail ist auf dem Weg vom Absender zum Empfänger verschlüsselt. Auf den Servern von Absender und Empfänger liegt sie unverschlüsselt. Sie ist damit einer Kenntnisnahme durch den Betreiber des Webservers und potenziell auch Strafverfolgungsbehörden ausgeliefert. Soll dieses Risiko ausgeschlossen werden, ist eine Ende-zu-Ende-Verschlüsselung erforderlich, siehe dazu unten.

Nicht nur die Technik hat aufgeholt, gleichzeitig hat auch der Gesetzgeber nachgebessert: So wurde 2007 mit § 202b StGB der Straftatbestand des Abfangens von Daten in das StGB eingeführt, der das bis dahin straflose unbefugte Mitlesen unverschlüsselter Daten unter Strafe stellt. Daneben greift außerdem das Telekommunikationsgeheimnis nach § 88 TKG.

Damit ist die E-Mail sowohl technisch als auch rechtlich besser vor unbefugter Kenntnisnahme geschützt als noch vor zehn Jahren. Was bedeutet das für den Rechtsanwalt? Er sollte auf jeden Fall sicherstellen, dass sein E-Mail-Server (bzw. der E-Mail-Server seines Providers) Transportverschlüsselung anbietet, damit er derart verschlüsselte E-Mails empfangen kann. Er selbst sollte mit seinem E-Mail-Server nur unter Einsatz von Transportverschlüsselung kommunizieren. Das Bayerische Landesamt für Datenschutzaufsicht hält im Übrigen eine solche Transportverschlüsselung inzwischen für rechtlich geboten.

ENDE-ZU-ENDE-VERSCHLÜSSELUNG VON E-MAILS

Bei einer Transportverschlüsselung von E-Mails besteht nach wie vor das Risiko eines unbefugten Zugriffs auf die E-Mails auf den Servern von Absender und Empfänger. Soll auch dieses Risiko ausgeschlossen werden, bleibt letztlich nur eine Ende-zu-Ende-Verschlüsselung von E-Mails. Hier haben sich insbesondere S/MIME und OpenPGP als Standards etabliert. Bei beiden Verfahren wird die E-Mail auf dem Rechner des Absenders verschlüsselt und erst wieder auf dem Rechner des Empfängers entschlüsselt – und zwar erst dann, wenn sie tatsächlich gelesen wird. Der Vorteil einer durchgehenden Verschlüsselung wird allerdings mit einigen organisatorischen Nachteilen erkauft, wie etwa einer fehlenden Durchsuchbarkeit des E-Mail-Accounts.

Der größte Nachteil einer Ende-zu-Ende-Verschlüsselung ist die zwingende Mitwirkung des Mandanten. Nur dann, wenn auch der Mandant über die notwendige Technik verfügt, kann ihm der Rechtsanwalt überhaupt eine verschlüsselte Nachricht zuschicken. Dies ist jedoch der Ausnahmefall.

Eine weniger aufwändige Alternative stellt das Verwenden von passwortgeschützten Containerdateien dar. Sie erlaubt zumindest den verschlüsselten Versand von Daten in Richtung Mandant. Dabei wird der Inhalt der E-Mail vor Versenden in einem verschlüsselten Dateicontainer abgelegt. Dem Empfänger muss dann lediglich ein Link zum Download der Entschlüsselungssoftware sowie das Passwort auf einem gesonderten Kanal übermittelt werden. An dieser Stelle sei jedoch zur Vorsicht gemahnt: Ein Versand des Passworts in einer gesonderten E-Mail kommt in der Praxis immer wieder vor – ist jedoch grob fahrlässig, da das Risiko eines Zugriffs auf das Postfach des Mandanten dadurch gerade nicht beseitigt wird. Denn wer Zugriff auf die verschlüsselte E-Mail hat, der kann auch auf die kurz davor oder danach versandte E-Mail mit dem Passwort zugreifen.

Ein entsprechender Schutz kann im Einzelfall auch durch die Verwendung eines Passwortschutzes bei Standard-Dateiformaten erreicht werden. Der Nutzer muss keine zusätzliche Software installieren und kann die Datei direkt öffnen. Allerdings ist auch hier Vorsicht geboten: Einige Programme bieten zwar für Standard-Dateiformate einen Passwortschutz, dieser lässt sich allerdings in vielen Fällen mit einfachsten Mitteln aushebeln.

INSTANT MESSAGING

Ein letztes Wort sei der stetig zunehmenden Inanspruchnahme von Instant Messaging Services und Nachrichtendiensten auf Social-Media-Seiten gewidmet. Die Sicherheitsstandards dieser Dienste sind überaus heterogen und für den Anwender meist nur schwer nachvollziehbar. Da es sich selten um offene Systeme handelt, bei denen die Sicherheitsarchitektur klar ist, sollten diese Techniken in der Kommunikation mit Mandanten nur dann eingesetzt werden, wenn die Sicherheit gewährleistet ist.

ERGEBNIS

Wer Ende-zu-Ende-Verschlüsselung anbietet, der dürfte aus rechtlicher Sicht auf der sicheren Seite sein. Was gilt, wenn – derzeit der Regelfall – eine solche Verschlüsselung fehlt? Rechtsprechung zur Frage, ob der Rechtsanwalt E-Mail ohne Ende-zu-Ende-Verschlüsselung kommunizieren darf, existiert ebenso wenig wie eindeutige Meinungen, die eine Kommunikation per E-Mail generell für unzulässig halten. Wer auf der sicheren Seite sein will und keine Ende-zu-Ende-Verschlüsselung anbietet, sollte die Einwilligung des Mandanten einholen. Diese kann in der Mandatsvereinbarung geschehen oder auch konkludent erfolgen. Eine konkludente Einwilligung dürfte dann erteilt sein, wenn der Mandant von sich aus vertrauliche Daten mittels unverschlüsselter E-Mail an den Rechtsanwalt übermittelt. Weicht jedoch die IT-Infrastruktur des Rechtsanwalts vom Stand der Sicherheitstechnik nach unten ab, sollte der Mandant davon unterrichtet werden, da von einer konkludenten Einwilligung immer nur auf Basis der Einhaltung aktueller IT-Sicherheitsstandards ausgegangen werden sollte.

So beständig sich der Vergleich der E-Mail mit der Postkarte hält, so wenig sind die Risiken der beiden Medien vergleichbar. Jeder Rechtsanwalt sollte sich die Frage stellen, ob und wie seine E-Mail-Kommunikation gesichert ist. Er sollte unbedingt Transportverschlüsselung einsetzen. Der Einsatz passwortgeschützter Container kann dabei eine Option für zusätzliche Sicherheit sein. Eine Einwilligungsklausel in der Mandatsvereinbarung reduziert das Risiko weiter.

Fit für den Wettbewerb:

Materialien für Anwälte

Unser Leitfaden als kostenloses E-Book

01 Kanzleistrategie
Der Weg zu einem klaren Kanzleiprofil

Download: www.anwaltverlag.de/BRAK-Leitfaden

Für Sie als Anwalt

10 Fitmacher für den Wettbewerb

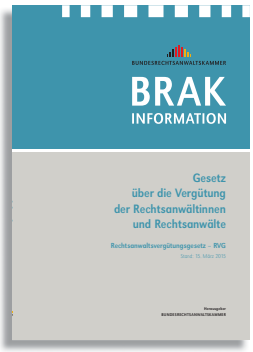
Kleine Schritte, große Wirkung

Die Broschüre unterbreitet zehn konkrete, leicht umsetzbare Vorschläge, wie Sie Ihre Kanzlei auf den Wettbewerb vorbereiten können. Das ist natürlich nur der Anfang. Zu jeder Idee finden Sie ergänzende Anregungen und Materialien auf der Internetseite der Initiative.

8 Seiten, DIN A5.
Download: www.anwaelte-im-markt.de

Rechtsanwaltsvergütungsgesetz

Auf einen Blick



Aus dem Inhalt:

- Gesetzestext RVG
- Rechtsanwaltsgebühren nach § 13 RVG
- Gebührentabelle
- Gebühren in Strafsachen
- Gebühren in Bußgeldsachen
- Gerichtsgebührentabelle
- Kostenrisikotabelle
- Stichwortverzeichnis

108 Seiten, DIN A5.
3,90 € / Stück *

Für Ihre Mandanten

Akquiseflyer

Empfehlen Sie sich – bei Ihren Mandanten und bei jenen, die es werden sollen. Der Flyer informiert über die Markenzeichen der Anwaltschaft: Unabhängigkeit, Verschwiegenheit, Loyalität. Drei gute Gründe, um miteinander ins Gespräch zu kommen.

6 Seiten, DIN A6, gefaltet.
Liefereinheit 50 Stück im Paket.
Schutzgebühr 9,95 € / 50er Paket *

Broschüre „Ihr Anwaltsbesuch“

Der Gang zum Anwalt ist für viele Mandanten ungewohnt. Sie fühlen sich verunsichert und haben zahlreiche Fragen, von der richtigen Vorbereitung über den Ablauf bis zu den Kosten der Beratung. Die Broschüre gibt Antworten auf diese Fragen – und damit Sicherheit.

12 Seiten, DIN A5.
Liefereinheit 25 Stück im Paket.
Schutzgebühr 19,95 € / 25er Paket *

Wörterbuch für Ihren Anwaltsbesuch

Rechtsberatung ist Vertrauenssache – und eine Frage von Verständnis. Mandantenfreundlich erklärt das Wörterbuch 130 grundlegende Rechtsbegriffe und vermittelt Wissenswertes rund um den Anwaltsbesuch. Zum Verschenken an Ihre Mandanten.

64 Seiten, DIN A6.
1,95 € / Stück *

Und so bestellen Sie

Bestellformular faxen an: 030 / 28 49 39-11 (BRAK)

Hiermit bestelle ich die eingetragene Anzahl der Publikationen:

- ☐ **Rechtsanwaltsvergütungsgesetz** _____ Stück
- ☐ **Akquiseflyer** _____ Pakete
- ☐ **Broschüre „Ihr Anwaltsbesuch“** _____ Pakete
- ☐ **Wörterbuch für Ihren Anwaltsbesuch** _____ Stück

Vorname _____

Name _____

BUNDESRECHTSANWALTSKAMMER

Kanzleistempel / Adresse

* Schutzgebühr jeweils inkl. MwSt. und zzgl. Versand.

Auslieferung und Rechnungsstellung durch Deutscher Anwaltverlag GmbH · Rochusstraße 2-4 · 53123 Bonn
Tel. 0228 / 91911-0 · Preisänderungen / Irrtum vorbehalten.

IT-RECHT – EIN RECHTSGEBIET IM RASANTEN WANDEL

2. JAHRESARBEITSTAGUNG IT-RECHT DES DEUTSCHEN ANWALTSINSTITUTS E. V.

Professor Dr. Jochen Marly, TU Darmstadt, Leiter der Jahresarbeitstagung IT-Recht

Die überaus stürmische Weiterentwicklung im Bereich der Informationstechnologie führt dazu, dass sich das IT-Recht ständig anpassen und fortentwickeln muss, wobei das hierfür notwendige Tempo geradezu atemberaubend ist. Allein das Thema des Handels mit sogenannter „Gebrauchtsoftware" rund um den Erschöpfungsgrundsatz der §§ 69c Nr. 3 S. 2, 17 Abs. 2 UrhG beschäftigt die Gerichte seit Jahren, ohne dass ein Ende der Diskussion absehbar wäre – und dies trotz mittlerweile dreier Entscheidungen des BGH sowie einer Entscheidung des EuGH. Während es zu Beginn der Diskussion noch um die eher einfach gelagerte Frage der Weiterveräußerung von Computersoftware ging, die auf einem Permanent-Datenträger erworben wurde (Software in der Box), kamen sehr schnell weitere Varianten hinzu wie die Weitergabe von im Wege des Downloads bezogener Software, Client-Server-Software, Software, die im Rahmen von Volumenlizenzen überlassen wurde oder gar nicht dem Anwender übermittelt wird, sondern lediglich zur Online-Nutzung bereit gestellt wird, etwa „in der Cloud".

Als gesichert kann mittlerweile festgehalten werden, dass Software in der Box vom Ersterwerber weiterveräußert werden darf, sofern verschiedene vom BGH aufgestellte Bedingungen eingehalten werden (BGH, Urt. v. 11.12.2014, I ZR 8/13), die im Wesentlichen darauf zurückzuführen sind, dass eine Weiternutzung durch den Ersterwerber unterbleibt. Auch die sogenannte Aufspaltung von Volumenlizenzen in Einzellizenzen ist zulässig, soweit sich die Volumenlizenz auf die Nutzung eigenständiger Kopien des Computerprogramms bezieht. Da dies alles aber nur für auf Dauer überlassene Standardsoftware gilt, bleiben mannigfaltige Fragen offen. Vielfach wird die Weitergabe nur unter Bedingungen erlaubt oder die Nutzung an die Einrichtung eines Nutzer-Accounts geknüpft, dessen Übertragbarkeit ausgeschlossen wird. Verstärkt sind in den letzten Jahren auch Mietmodelle der Softwareüberlassung auf dem Markt, bei denen der Erschöpfungsgrundsatz von vornherein nicht eingreift. Der Diskussionsbedarf bleibt dementsprechend auch für die Zukunft groß, zumal die Möglichkeiten der Weitergabe digitaler Güter etwa bei Musik, E-Books, Fotos und Filmen nicht nur beständig zunehmen, sondern auch noch der juristischen Aufarbeitung harren.

Weitere Themen der Jahresarbeitstagung werden etwa die sogenannte Industrie 4.0 sein, deren technische Grundlagen erörtert (Dr. Ulrich Springer, Frauenhofer-Institut für Software- und Systemtechnik) und deren juristische Probleme in Hinblick auf Datensicherheit und Datenschutz (Isabell Conrad, Rechtsanwältin) vorgestellt werden. Darüber hinaus werden die Themen „Aktuelle Rechtsprechung zum Internetrecht" (Dieter Kehl, Vors. Richter am Landgericht), „Aktuelle vergaberechtliche Rechtsprechung mit Bezug zu IT-Beschaffungen der öffentlichen Hand – agile Softwareentwicklung vs. Vergaberecht" (Günther Pinkenburg, LL.M., Rechtsanwalt), „Urheberrechtliche und vertragsrechtliche Probleme bei Apps für Smartphones" (Professor Dr. Jochen Marly, TU Darmstadt), „Aktuelle BGH-Rechtsprechung zum IT-Recht" (Dr. Thomas Koch, Richter am Bundesgerichtshof) sowie „Datenmigration – Qualität von Daten im Nutzungskontext – Was bedarf der rechtlichen Regelung aus technischer Sicht?" (Dipl.-Ing. Wiegand Liesegang, öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung) behandelt. Damit bietet die Jahresarbeitstagung IT-Recht einen Überblick sowohl über technische Entwicklungen als auch über die aktuelle juristische Diskussion und bietet allen Kolleginnen und Kollegen die Möglichkeit, in dieser schnelllebigen Materie auf dem Laufenden zu bleiben. Neben dem fachlichen Erfahrungsaustausch besteht selbstverständlich auch Raum für die Pflege persönlicher Kontakte.

2. JAHRESARBEITSTAGUNG IT-RECHT

9. bis 10. Oktober 2015 · München

Weitere Informationen und Anmeldung:
Deutsches Anwaltsinstitut e. V.
Tel. 0234 970640
info@anwaltsinstitut.de
www.anwaltsinstitut.de

Großmacht

NEU

Lützenkirchen **Mietrecht** Kommentar. *Bearbeitet von RiLG Dr. Dr. Andrik Abramenko; RA, FA MietR/WEG Dr. Marc Dickersbach; RA, FA MietR/WEG Dr. Klaus Lützenkirchen. 2., neu bearbeitete Auflage 2015, 2.672 Seiten Lexikonformat, gbd. 149,– €. ISBN 978-3-504-45078-6*

Pünktlich zum Inkrafttreten der *Mietpreisbremse* tritt auch Lützenkirchen wieder auf den Plan. Mit einer nagelneuen Auflage des anwaltsorientierten Großkommentars zu Wohn- und Gewerberaummiete, mit Heizkosten- und Wärmelieferverordnung.

Erstklassige Autoren. Erläuterungen der Extraklasse, mit Beispielen, Tabellen und überzeugender Begründungstiefe. Für Gestaltungsaufgaben und Schriftsätze auf höchstem Niveau.

Mit allen Änderungen der Mietrechtsnovelle 2015. Mit dem Gesetz zur Umsetzung der Verbraucherrechterichtlinie. Mit neuester Rechtsprechung und Literatur. Bis hin zu den jüngsten BGH-Entscheidungen zur Unwirksamkeit von Quotenabgeltungs- und Vornahmeklauseln bei Schönheitsreparaturen oder zum eingeschränkten Minderungsrecht des Mieters bei Lärmbelästigungen.

Lützenkirchen, Großkommentar zum Mietrecht. Jetzt Probe lesen und bestellen bei **www.otto-schmidt.de/gkm2**

ottoschmidt

Als Rechtsanwalt wissen Sie: Für den Erfolg Ihrer Mandanten vor Gericht stehen Sie. Für den wirtschaftlichen Erfolg Ihrer Kanzlei gibt es Unterstützung. Mit der Software DATEV Anwalt classic pro und dem Fachwissen von TeleLex profitieren Sie von einem Rundum-Angebot speziell für Anwälte – von der Organisation der Abläufe in der Kanzlei bis hin zu aktuellem Fachwissen und Online-Seminaren nach § 15 FAO.

Informieren Sie sich auf www.datev.de/anwalt oder unter 0800 3283872.

DATEV

Zukunft gestalten. Gemeinsam.