FACHINFO-MAGAZIN
MKG
MIT KOLLEGIALEN GRÜßEN

SONDERAUSGABE SPEZIAL SONDERAUSGABE

ffi Verlag
Freie Fachinformationen

Von erfahrenen Praktikern für junge Juristen

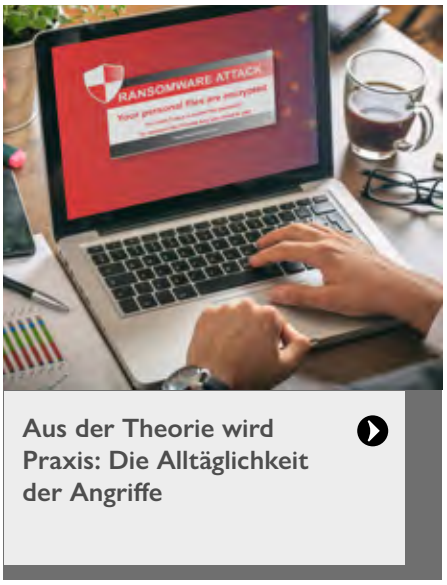
Mai 2019

Dr. Lutz Martin Keppeler

CYBERSCHUTZ IN DER ANWALTSKANZLEI

KOMPAKTER LEITFADEN ÜBER RECHTLICHE ANFORDERUNGEN, IT-SICHERHEIT UND DATENSCHUTZ

Die Digitalisierung in der Anwaltskanzlei ist längst Alltag



Aus der Theorie wird Praxis: Die Alltäglichkeit der Angriffe

Rechtliche Verpflichtungen zur IT-Sicherheit: Anwalt ist in der Pflicht

Welche Anforderungen bestehen nach Art. 32 DSGVO konkret?

Cyberschutzversicherung – möglich und sinnvoll?

Fazit – Gute IT-Sicherheit ist der beste Selbstschutz!

MKG SPEZIAL

INHALT

NEHMEN SIE JETZT AN UNSERER UMFRAGE TEIL!

WELCHE BEDEUTUNG HAT CYBERSICHERHEIT IM KANZLEIALLTAG?

WIE PROFESSIONELL SCHÜTZEN SIE SICH VOR BERUFLICHEN RISIKEN?

BERUFSHAFTPFLICHT-VERSICHERUNG 2.0

ProfessionGuard RSW

DAS VERSICHERUNGSKONZEPT FÜR RECHTSANWÄLTE/STEUERBERATER/WIRTSCHAFTSPRÜFER

Für den professionellen und umfassenden Schutz gegen die Risiken Ihres Berufsalltags haben wir dieses innovative Versicherungskonzept entwickelt.
Die für Rechtsanwälte, Steuerberater und Wirtschaftsprüfer maßgeschneiderte Lösung bündelt Risiken und bietet damit umfänglichen Schutz gegen die Folgen von Vermögensschäden aus:

- der freiberuflich ausgeübten Tätigkeit
- Cyberrisiken wie Hacker-Attacken
- Büroservicetätigkeiten
- der Tätigkeit als externer Datenschutzbeauftragter
- der Ausübung von Fremdmandaten
- der Veruntreuung durch eigene Mitarbeiter

Profitieren Sie von der AIG Kombi-Lösung **ProfessionGuard RSW**. Umfangreicher Versicherungsschutz bei attraktiver Prämie, topaktueller Versicherungsschutz durch kontinuierliche Innovation. AIG steht für ein weltweites Netzwerk, globales Know-how und weitreichende Erfahrung in der Schadenabwicklung.

ERFAHREN SIE MEHR: WWW.AIG.DE

AIG®

DR. LUTZ MARTIN KEPPELER

Dr. Lutz Martin Keppeler (Fachanwalt für Informationstechnologierecht) arbeitet seit 2014 bei Heuking Kühn Lüer Wojtek in Köln im Bereich IT/IP. Zuvor war er bei einer internationalen Kanzlei beschäftigt. Er berät Mandanten zu allen Fragen des IT- und Datenschutzrechts und ist in diesen Bereichen sowohl außergerichtlich als auch forensisch tätig. Herr Dr. Keppeler arbeitet besonders intensiv an der Schnittelle zwischen Technik und Recht woraus sich Spezialgebiete wie das IT-Sicherheitsrecht, das Open Source-Lizenzrecht und das Daten-schutzrecht ergeben.

www.heuking.de

1. EINFÜHRUNG: RECHTLICHE ANFORDERUNGEN AN DEN CYBERSCHUTZ IN DER ANWALTSKANZLEI

Schon in der „guten alten Zeit“ durften keine Informationen abhandenkommen, die dem „Anwaltsgeheimnis“ unterlagen. Doch um die Verschwiegenheitsverpflichtung zu erfüllen, genügte es damals noch, nach Feierabend die Bürotür fest zuzuschließen und nicht über seine Fälle zu sprechen. Das Datenschutzrecht spielte nur eine Rolle für sehr spezialisierte Kollegen, die sich dafür interessierten. Doch dieses „analoge“ Zeitalter ist für Anwälte längst vorbei und die Errungenschaften der Digitalisierung haben auch neue Gefahren mit sich gebracht.

Dieses MkG-Spezial erklärt vor dem Hintergrund der Digitalisierung in Anwaltskanzleien (siehe unter 2.) und den damit einhergehenden Gefahren (siehe unter 3.), welche rechtlichen Anforderungen an die IT-Sicherheit in Anwaltskanzleien bestehen (siehe unter 4.) und weshalb die DSGVO hierbei eine besonders prominente Rolle einnimmt (siehe hierzu unter 5.).

In dem Hauptteil dieser Ausgabe wird erläutert, welche Anforderungen sich an die IT-Sicherheit aus Art. 32 DSGVO ergeben (siehe unter 6.). In diesem Rahmen wird erörtert, weshalb es – angesichts fehlender Konkretisierungen der Generalklauseln in der Rechtsprechung und aufgrund des sehr individuellen Schutzbedarfes in konkreten Kanzleien – kaum allgemein verbindliche Checklisten zur Erfüllung der Anforderungen an die IT-Sicherheit einer Kanzlei geben kann. Es wird aber auch gezeigt, dass jede Kanzlei, die dokumentiert, welcher „Schutzbedarf“ besteht und welche technischen und organisatorischen Schutzmaßnahmen implementiert wurden, und die erkannten Risiken mit vertretbarem Aufwand minimiert, auf der sicheren Seite ist. Zum Schluss folgen kurze Erläuterungen zu Cyber-Versicherungen (siehe unter 7.) und zivilrechtlichen Haftungsrisiken (siehe hierzu unter 8.). Die Spezialausgabe schließt mit einem zusammenfassenden Fazit ab (siehe unter 9.).

Mit kollegialen Grüßen

Dr. Lutz M. Keppeler

2. DIE DIGITALISIERUNG IN DER ANWALTSKANZLEI IST LÄNGST ALLTAG

Auch wenn man gedanklich den Beruf des Anwalts nicht sofort mit dem Silicon Valley verknüpft, haben dennoch viele technologische Neuerungen Einzug in den Arbeitsalltag gehalten. Anstelle des Briefes wird seit mehr als zwei Jahrzehnten die E-Mail als primäres Kommunikationsmittel genutzt. Es wurde sogar ein besonderes elektronisches Anwaltspostfach, kurz: beA von der Bundesrechtsanwaltskammer ins Leben gerufen, mit dem das Ziel verfolgt wurde, eine sichere Kommunikation zwischen Gerichten, Staatsanwälten und Rechtsanwälten zu gewährleisten.

Der feste Schreibtisch und dicke Kommentarliteratur werden immer häufiger durch ein handliches Notebook mit Zugang zu juristischen Online-Datenbanken ersetzt und anstelle eines Diktats, dass von einer/einem Rechtsanwaltsfachangestellten mühselig abgetippt wird, nutzt man heutzutage vermehrt Spracherkennungssoftware, die das gesprochene Wort wie per „Zauberhand" in geschriebene Buchstaben verwandelt und bei Bedarf durch Übersetzungssoftware (inklusive Google Translate) in verschiedene Sprachen übersetzt. Die hieraus entstandenen Schriftsätze verschwinden sodann immer seltener in Regalen mit schweren Aktenordnern, sondern auf der Festplatte des eigenen Kanzlei-Servers oder irgendwo anders auf der Welt bei seriösen Hostern oder im schlimmsten Fall bei freien Cloud-Providern wie Dropbox.

In jüngster Zeit sprießen unter dem Stichwort „Legal Tech" zahlreiche neue (und gut verpackte alte) Innovationen auf den Markt für Rechtsdienstleistungen, welche die Anwaltswelt nachhaltig verändern werden. Diese Digitalisierung bringt zwar großen Effizienznutzen, doch gleichzeitig wachsen auch die Anforderungen an die IT-Sicherheit für jede Anwältin und jeden Anwalt stetig.

3. AUS DER THEORIE WIRD PRAXIS: DIE ALLTÄGLICHKEIT DER ANGRIFFE

Diese neuen Arbeitsformen bringen auch ihre ganz eigenen Gefahrenquellen mit sich. Aus unterschiedlichsten Gründen können Systeme ausfallen und Daten verloren gehen. Die Ursachen hierfür können sowohl intern als auch extern begründet sein. Eine wesentliche Gefahr stellen dabei böswillige und kriminelle Einflüsse von außen dar. Nicht zu unterschätzen ist z. B. ein Schadcode, der oftmals als E-Mail-Anhang oder über manipulierte Internetseiten auf den Computer des Nutzers gespielt wird. Ein unbedachter Mausklick kann dazu führen, dass die gesamten IT-Systeme einer Kanzlei verschlüsselt werden. Kriminelle fordern dann eine Art Lösegeld, nach dessen Zahlung die IT – vermeintlich – wieder entschlüsselt wird. Wird nicht gezahlt, stehen die Chancen, jemals wieder an die Daten zu kommen, äußerst schlecht. Für eine Kanzlei gleicht dies dem Super GAU. Opfer eines solchen Cyber-Angriffs war beispielsweise 2017 die internationale Großkanzlei DLA Piper, die viele Wochen benötigte, um zum „business as usual" zurückzukehren.

Weitere Gefahren können auch Fälle von Identitätsdiebstahl oder sogenanntem Social Engineering sein, mit dessen Hilfe Menschen zur Preisgabe vertraulicher Informationen bewegt werden sollen. Auch ganz „konservative" Gefahren wie der Verlust oder Diebstahl des Notebooks oder Smartphones stellen ein relevantes Risiko dar. Die zuletzt genannten Risiken bestehen hier nicht nur für den Anwalt, sondern vor allem auch für Personen, deren Informationen durch den Anwalt verarbeitet werden, also für Mandanten, Gegner und Dritte. Diese Daten muss der Anwalt zwar auch im eigenen Interesse schützen, primär aber deshalb, weil er hierzu verpflichtet ist (siehe sogleich Ziffer 4). Immer häufiger erfolgen auch gezielte Hackings, um personenbezogene Daten und andere sensible Informationen zu entwenden oder Accounts zu übernehmen. Wie leicht dies heutzutage gehen kann, hat nicht zuletzt das Hacking von zahlreichen Social Media-Accounts von Politikern im Dezember 2018/Januar 2019 gezeigt: Als Täter wurde ein typisches **„Script Kiddy"** identifiziert, ein 20-Jähriger, der aus Verärgerung über Politiker mit sehr begrenzten Ressourcen und Fähigkeiten vorgegangen ist. Was dieser Täter konnte, kann nahezu jeder fünfte Mandant oder Gegner auch oder könnte es sich leicht beibringen (oder hat Kinder oder Freunde, die das besser können).

4. RECHTLICHE VERPFLICHTUNGEN ZUR IT-SICHERHEIT: ANWALT IST IN DER PFLICHT

Doch sind deshalb Anwälte dazu verpflichtet, besondere IT-Sicherheitsmaßnahmen zu treffen? Ansatzpunkte hierzu finden sich in ganz unterschiedlichen Rechtsgebieten:

a. § 203 StGB

- Für das unbefugte Offenlegen fremder Geheimnisse, die einem Rechtsanwalt in dieser Funktion anvertraut wurden, droht eine Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe.
- Eine Strafbarkeit kann auch durch das Unterlassen von notwendigen IT-Sicherheitsmaßnahmen bestehen.

b. § 2 BORA

- Detailliertere Regelungen zur Verschwiegenheitspflicht von Rechtanwälten. Unter anderem enthält § 2 Abs. 7 BORA die Verpflichtung, die zum Schutze des Mandantengeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu schaffen, die risikoadäquat und für den Anwaltsberuf zumutbar sind.

c. § 43a Abs. 2 BRAO

- Hier wird die Verschwiegenheitspflicht als eine der Grundverpflichtungen des Rechtsanwalts definiert.

d. Art. 32 DSGVO

- Art. 32 DSGVO verpflichtet jeden, der personenbezogene Daten verarbeitet, zur Vornahme von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung. Es ist zu beachten, dass der Anwendungsbereich der DSGVO äußerst schnell eröffnet ist, da mittlerweile fast alle Daten einen Personenbezug haben. Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies wird insbesondere auch von der Rechtsprechung sehr weit ausgelegt. Es spielt dabei keine Rolle, ob die Daten einen sensiblen Charakter haben oder völlig trivial erscheinen.

e. § 13 Abs. 4, 7 TMG

- Anbieter von Telemedien haben auch in Bezug auf die angebotenen Dienste technische und organisatorische Vorkehrungen zu treffen, welche die Sicherheit der Dienste garantieren. Dies ist vor allem für den Betrieb der Kanzleiwebseite relevant.

5. DIE DSGVO ALS TREIBER DER AKTUELLEN DEBATTE UM IT-SICHERHEIT

Die Digitalisierung gibt es nicht erst seit gestern und die Debatten um die Verschlüsselung von E-Mails vor dem Hintergrund von § 203 StGB und § 43a Abs. 2 BRAO reichen bis zum Jahr 2001 zurück. Die Ursache dafür, dass diese Thematik gerade jetzt hochkocht, liegt vorwiegend daran, dass seit dem 25.05.2018 die DSGVO anwendbar ist. Damit verbunden sind hohe Sanktionsmöglichkeiten durch die Datenschutzaufsichtsbehörden, die theoretisch Bußgelder von bis zu EUR 10.000 im Falle eines Verstoßes gegen Art. 32 DSGVO erlassen können. In der Praxis liegen die Bußgelder allerdings weit darunter. Soweit ersichtlich wurde in **2018 für einen Verstoß gegen Art. 32 DSGVO** nur ein Bußgeld erlassen. Dieses betrug EUR 20.000 und wurde gegen das Soziale Netzwerk „Knuddels“ erlassen, da diesem eine Vielzahl unverschlüsselter Kundendaten abhandengekommen sind.

Ein weiterer Faktor sind wettbewerbsrechtliche Abmahnungen von Konkurrenten: Es ist nach Einführung der DSGVO bereits vorgekommen, dass Anwaltskanzleien von anderen Anwälten aufgrund vermeintlich mangelhafter Datenschutzerklärungen abgemahnt wurden. Es ist durchaus denkbar, dass sich auch diese Fälle häufen und auch auf Fragen der IT-Sicherheit beziehen werden, wenngleich hierzu einschränkend anzumerken ist, dass die Abmahnfähigkeit von Verstößen gegen die DSGVO umstritten ist. Vor diesem Hintergrund beschäftigt sich diese Spezialausgabe im Folgenden hauptsächlich mit den IT-Sicherheitsanforderungen nach der DSGVO.

6. WELCHE ANFORDERUNGEN BESTEHEN NACH ART. 32 DSGVO KONKRET?

Einleitend ist festzuhalten, dass es keine Liste mit vorgegebenen, pauschalen Maßnahmen zur Erfüllung von Art. 32 DSGVO gibt, ebenso wie es keine Checkliste zur Erfüllung des § 242 BGB im Rahmen von Verträgen geben kann. In beiden Fällen liegt dies an der generalklauselartigen Gestaltung der Norm. Der hier wesentlich relevante Art. 32 DSGVO lautet in seinem maßgeblichen Text wie folgt:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."

Dem Normtext können keine konkreten obligatorischen Maßnahmen entnommen werden. Wenngleich Art. 32 Abs. 1 lit. a)–d) DSGVO Regelbeispiele für bestimmte Maßnahmen nennt, wie z. B. die Verschlüsselung und Pseudonymisierung, lassen sich hieraus dennoch keine nach Art und Umfang konkrete Maßnahmen ableiten. Dabei dürfte man sich Fragen stellen wie:

- Welches Verschlüsselungsverfahren soll in welchem Fall angewendet werden?
- Genügt die Verschlüsselung der Kommunikation oder müssen alle gespeicherten Daten verschlüsselt werden?

Stattdessen muss im Einzelfall geprüft werden, welche konkreten Maßnahmen erforderlich und sinnvoll sind. Dies hängt insbesondere von der jeweils genutzten IT-Infrastruktur, der Sensibilität der verarbeiteten Daten und der diesbezüglichen Risikobewertung ab. In einem ersten Schritt müssen Kanzleien überprüfen, welche konkreten IT-Systeme in der Kanzlei genutzt werden. Im nächsten Schritt muss evaluiert werden, welches Sicherheitsniveau dabei gewährleistet wird. Das bedeutet, dass geprüft werden muss, welche Sicherheitsmaßnahmen bereits etabliert sind und an welchen Stellen keine oder nur schwache Maßnahmen bestehen.

Die Evaluierung der individuell erforderlichen Maßnahmen kann von Kanzlei zu Kanzlei zu sehr unterschiedlichen Ergebnissen führen. Von besonderer Bedeutung ist hierbei u. a. der Tätigkeitsschwerpunkt der jeweiligen Kanzlei. Eine Kanzlei für Strafrecht oder Familienrecht wird aufgrund der Sensibilität der gespeicherten Daten regelmäßig ein höheres Sicherheitsniveau gewährleisten müssen als z. B. eine Baurechtsboutique.

A | BEISPIELMAßNAHMEN FÜR KLEINE KANZLEIEN OHNE SENSIBLE DATEN

Es ist daher denkbar, dass eine Kanzlei, die nur mit weniger sensiblen Daten arbeitet, lediglich allgemeine technische und organisatorische Maßnahmen treffen muss. Zu denken wäre in diesem Fall z. B. an:

- regelmäßige Updates sämtlicher verwendeter Software.
- Verwendung ausreichend komplexer Passwörter (in größeren Kanzleien sichergestellt durch eine „Passwortrichtlinie").
- einmalige Schulung und Sensibilisierung der Mitarbeiter.
- Verschlüsselung von E-Mails per TLS (Bei TLS handelt es sich um eine selbständig ablaufende Verschlüsselung des Transportweges der E-Mail; weit über 95 % der heute in Deutschland gängigen E-Mail-Accounts sind so eingerichtet, dass sie E-Mails automatisch verschlüsseln. Die Abkürzung steht für „Transport Layer Security").
- regelmäßige Backups wichtiger Daten auf externen Festplatten und
- Verschlüsselung gespeicherter Daten bzgl. ganzer Festplatten.

Man sieht, dass diese beispielhaften Sicherheitsmaßnahmen nicht übermäßig schwer umzusetzen wären, sie dürften aber auch nur für kleine Kanzleien ohne sensible Daten und ohne wichtige Geschäftsgeheimnisse der Mandanten ausreichen. Weitere Anregungen für typische technische und organisatorische Maßnahmen können einem Muster des deutschen Anwaltsvereins entnommen werden.

Zum Gratis-Download hier klicken.
Checkliste für technische und organisatorische Maßnahmen der Datensicherheit.

B | BEISPIELMAßNAHMEN FÜR GRÖßERE KANZLEIEN MIT SENSIBLEN DATEN

Eine größere Kanzlei würde etwa zusätzlich noch ein Berechtigungskonzept (also Regelungen darüber, wer auf welche Daten und Akten zugreifen darf) benötigen – was bei einer 1-Mann-Kanzlei naturgemäß nicht nötig wäre. Kanzleien, die wesentlich sensiblere personenbezogene Daten (etwa Vaterschaftstest, Informationen aus intimen Details aus dem Privatleben, Krankenakten oder psychiatrische Gutachten über Personen) müssen solche Daten stärker schützen. Die oben genannten Maßnahmen müssen gegebenenfalls verschärft werden (z. B. durch Mindestanforderung für Passwortlänge; Verschlüsselung der gespeicherten Daten; Ende-zu-Ende-Verschlüsslung in der E-Mail-Kommunikation; Home-Office nur über VPN-Verbindungen und zusätzliche Auflagen an das Ausdrucken und die Mitnahme und Verwendung von ausgedruckten Daten usw.).

C | ANALYSE DER IN EINER KANZLEI VERARBEITETEN DATENKATEGORIEN UND DEREN SCHUTZBEDARF

Welche technischen und organisatorischen Maßnahmen genau umgesetzt werden sollten, kann nur ermittelt werden, wenn klar dokumentiert ist, welcher Schutzbedarf für die durch die Kanzlei verarbeiteten Daten besteht. Welche Daten müssen vor welchen Bedrohungen angesichts welcher Schadenspotentiale geschützt werden? Die Prüfung von Art. 32 DSGVO muss mit der Frage beginnen, vor welchen Risiken die zu implementierenden technischen und organisatorischen Maßnahmen schützen sollen. Dies betonen auch die Datenschutzaufsichtsbehörden in den wenigen veröffentlichten Papieren zu Art. 32 DSGVO und dieser Analyseschrift (in der IT-Fachsprache häufig „Schutzbedarfsanalyse“ genannt). Dies ergibt sich auch aus allen gängigen IT-Sicherheitsstandards, wie den BSI-Grundschutzkatalogen/dem BSI-Kompendium, den Standards der ISO-Normenreihe 27001ff, den „Common Criteria“ oder dem von den Datenschutzaufsichtsbehörden entwickelten „Standard Datenschutz Modell“.

(1) | WELCHE DATEN WERDEN VERARBEITET? – RÜCKGRIFF AUF DAS VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Haben Sie einen Überblick darüber, welche Daten in Ihrer Kanzlei gespeichert und verarbeitet werden? Im Idealfall hat eine Kanzlei bereits im Rahmen der Vorbereitung auf die DSGVO ein so genanntes Verzeichnis der Verarbeitungstätigkeiten erstellt. Dieses Verzeichnis enthält eine Reihe an Details zu allen Datenverarbeitungsvorgängen, die in der jeweiligen Kanzlei konkret vorkommen (also z. B. Verfahren bezüglich der eigenen Mitarbeiter wie „Lohnbuchhaltung“ oder „Personalverwaltung“ oder Verfahren bezüglich Mandanten wie „Verwaltung von Geldern für Mandaten inklusive Geldwäscheprozess“ oder „Führen eines Prozesses im allgemeinen Zivilrecht“ oder „Führen einer familienrechtlichen Streitigkeit“). Gemäß Art. 30 DSGVO ist jeder datenschutzrechtlich Verantwortliche verpflichtet, ein solches Verzeichnis zu führen. Wenn diese Aufgabe sorgfältig erledigt wurde, kann anhand des Verzeichnisses der Verarbeitungstätigkeiten bereits abgelesen werden, welche Daten in einer Kanzlei verarbeitet werden.

(2) | RELEVANTE RISIKEN

Bis hierhin galt die Faustregel: Wer die Anforderungen aus Art. 32 DSGVO erfüllt, erfüllt zugleich auch die Anforderungen der anderen oben genannten Vorgaben des Standesrechts und des Strafrechts bzw. handelt nicht „fahrlässig“ im Sinne sämtlicher denkbarer zivilrechtlicher Anspruchsgrundlagen. Im Hinblick auf die relevanten Risiken für die Daten einer Anwaltskanzlei ist nun zu differenzieren:

Art. 32 DSGVO schützt ausschließlich natürliche Personen vor Bedrohungen wie Identitätsdiebstahl, finanziellem Verlust (einer Person, nicht eines Unternehmens), unbefugter Aufhebung der Pseudonymisierung, Belästigung durch Werbung, Verlust des Zugriff auf Accounts oder anderen wirtschaftlichen oder gesellschaftlichen Nachteilen.

Nicht relevant sind für Art. 32 DSGVO hingegen wirtschaftliche Risiken von Unternehmen wie etwa Geschäftsgeheimnisse, ein unautorisierter Zugriff auf geheime Unterlagen der Forschungsabteilung oder sensible Finanzinformationen. Diese Aspekte sollte ein Anwalt dennoch im Rahmen der Schutzbedarfsanalyse berücksichtigen. Auch wenn dies zur Erfüllung von Art. 32 DSGVO nicht notwendig ist, dient dieser Aspekt zur Erfüllung der anderen oben genannten Normen (z. B. dem Standesrecht und der berufsrechtlichen Verschwiegenheitsverpflichtung aus § 203 StGB).

(3) | PROBLEM DER FAKTISCHEN ERMITTLUNG VON RISIKEN

Im nächsten Schritt ist zu bewerten, wie hoch die Wahrscheinlichkeit ist, dass ein (materieller oder immaterieller) Schaden als Folge einer verwirklichten Gefahr eintritt und wie schwer dieser Schaden sein könnte. Häufig ist hierbei fraglich, auf welcher Informationsgrundlage solche Prognosen vorgenommen werden können. Denn es gibt keine objektiven Langzeitstudien darüber, wie häufig Anwaltskanzleien angegriffen werden, welche Daten hierbei abhandenkommen und zu welchem Schaden dies führt. Die vielfach befürchtete staatliche Wirtschaftsspionage wird für größere Wirtschaftskanzleien eventuell eine Rolle spielen, aber welche Art von „Tätern“ und „Angreifern“ soll sich eine kleinere Kanzlei für Verkehrsrecht vorstellen?

Wenn man aktuelle Studien zur Lage der IT-Sicherheit in Deutschland liest (wie sie etwa vom Bundesamt für Sicherheit in der Informationstechnologie herausgegeben werden: **www.bsi.bund.de**) oder auch nur die Tagespresse durchgeht, könnte man leicht den Eindruck gewinnen, Unternehmen aller Branchen und Größen – und damit auch Anwälte – seien der ständigen Gefahr durch Hacking ausgesetzt. Sucht man hingegen in Kommentierungen von § 203 StGB oder in Juris/Beck-Online nach Verurteilungen von Anwälten wegen Unterlassens der Vornahme einer gebotenen IT-Sicherheitsmaßnahme stellt man fest,

dass – trotz weit vorangeschrittener Digitalisierung – keinerlei relevante Verurteilungen veröffentlicht wurden. Aus dieser Perspektive gewinnt man den Eindruck, dass entweder Cybercrime vorwiegend außerhalb von Anwaltskanzleien stattfindet oder dass die durchschnittlichen Sicherheitsmaßnahmen von durchschnittlichen Anwälten häufig ausreichen. Wie ist diese Diskrepanz in der Beschreibung möglicher Risiken aufzulösen und wie soll ein einzelner Anwalt hierzu in der Lage sein? Von Interesse wären weitere Details, etwa von wem und wie oft E-Mails „mitgelesen" werden oder in welchem Ausmaß versucht wird, eine Transportverschlüsselung oder eine „Ende-zu-Ende"-Verschlüsslung anzugreifen oder zu umgehen.

(4) AUSWAHL DER GEEIGNETEN IT-SICHERHEITSMAßNAHMEN GGF. GEMEINSAM MIT EINEM IT-DIENSTLEISTER; BERÜCKSICHTIGUNG DER SICHERHEIT ALS GESAMTBILD

Trotz dieser Unsicherheit müssen Maßnahmen gewählt werden, welche helfen, die bestehenden Risiken adäquat zu minimieren. In der Regel hilft die Dokumentation der Risiken bei der Auswahl zwischen einer sehr sicheren, aber dafür aufwendigen Maßnahme und einer moderaten, vielleicht aber nicht ganz so sicheren, dafür aber in der Praxis ohne jegliche Änderung der Arbeitsabläufe umsetzbaren Maßnahme. Hierbei ist stets das „Gesamtmaß" an Sicherheit einer Kanzlei zu berücksichtigen, denn die IT-Sicherheit ist stets nur so stark, wie das schwächste Glied der Kette. Anders ausgedrückt: Wenn die Haustüre gut verschlossen ist, aber die Fenster alle sperrangelweit geöffnet sind, nützt es wenig, die Schlösser der Eingangstür zu verstärken. So ist dies auch im Bereich der IT-Sicherheit und dies wird häufig übersehen. Tatsächlich wird aktuell die Stärke und Methode der E-Mail-Verschlüsslung intensiv diskutiert. Teilweise wird sehr pauschal und ohne konkrete Schutzbedarfsanalyse eine aufwendige Ende-zu-Ende-Verschlüsslung gefordert – ohne zu berücksichtigen, ob Privatpersonen als Mandanten hiermit überfordert sein könnten. Die beste Ende-zu-Ende-Verschlüsslung nützt aber nichts, wenn es sehr leicht ist, von außen oder innen auf die Festplatten der Arbeitsplatzrechner und Server zuzugreifen, etwa weil:

- Zugänge nur sehr unzureichend mit Passwörtern gesichert sind,
- diese beispielsweise seit Jahren nicht geändert wurden (und auch zahlreichen Ex-Angestellten bekannt sind).

Diese Argumentation soll vor allem davor schützen, punktuelle übertriebene Investitionen zu tätigen. Bevor viel Geld in eine neue teure „Firewall" gesteckt wird, sollte man selbst oder mithilfe eines IT-Sicherheitsexperten kurz überlegen, durch welche Standardmaßnahmen (z. B. den oben genannten) das Gesamtmaß an Sicherheit wesentlich kostengünstiger erhöht werden kann.

(5) DOKUMENTATION „PLAUSIBLER" SCHUTZBEDARFSANALYSE UND ERGRIFFENER MAßNAHMEN ALS „RETTUNG"

Aus der Ungewissheit über die konkret bestehenden Risiken und die Wirkung und Angemessenheit spezifischer Maßnahmen entsteht zweifellos ein großer Auslegungs- und Prognosespielraum. Gerade diese Unwägbarkeiten haben Anwälte in der Vergangenheit dazu veranlasst, erst gar keine Schutzbedarfsanalyse vorzunehmen und diese zu dokumentieren, auch weil Sanktionen oder andere Nachteile in der Praxis bislang kaum drohten.

Angesichts der DSGVO sollte sich jedoch jeder Anwalt fragen, ob dieses Verhalten für die Zukunft noch richtig ist. Denn gemäß Art. 5 Abs. 2 und Art. 24 DSGVO besteht eine umfassende Nachweispflicht für die Einhaltung der Vorgaben der DSGVO. Bei einer Nachfrage der Datenschutzaufsichtsbehörde muss der Anwalt nachweisen können, dass er ausreichende Sicherheitsmaßnahmen getroffen hat, um Art. 32 DSGVO zu erfüllen. Einen solchen Nachweis kann nur erbringen, wer die oben genannten Schritte für sich intern dokumentiert hat.

Im Rahmen der Anfertigung der Dokumentation sollte man sich folgenden Leitgedanken vor Augen halten: Fehlt eine Dokumentation völlig und wurde in keiner Weise verschriftlicht, welcher Schutzbedarf für Daten besteht (und welche Daten überhaupt verarbeitet werden), so stellt dies ohne jeden Zweifel einen Verstoß gegen Art. 32 i.V.m. Art. 5 Abs. 2 und Art. 24 DSGVO dar. Eine komplizierte Prüfung bleibt einer Datenschutzaufsichtsbehörde so erspart. Zwar ist die Wahrscheinlichkeit der verdachtsunabhängigen Prüfung durch eine Datenschutzaufsichtsbehörde nicht sehr hoch, doch die hohe Anzahl an Beschwerden bei Aufsichtsbehörden, welche typischerweise genaue Prüfungen nach sich ziehen, sollte zu denken geben:

Was ist, wenn der unzufriedene Mandant, der enttäuschte Gegner oder der frustrierte Kollege sich bei der Datenschutzaufsichtsbehörde mit der Behauptung beschweren, die Daten seien bei Ihnen nicht sicher?

Eine Datenschutzaufsichtsbehörde hat dann keine andere Wahl und wird eine Anwaltskanzlei nach der Umsetzung von Art. 32 DSGVO fragen müssen. Bei Fehlen jeglicher Dokumentation wird es dann mühsam und riskant.

Umgekehrt gilt jedoch: Sobald „plausibel" und „in sich schlüssig" dokumentiert wurde, dass sich jemand auf Basis einer Übersicht aller gespeicherten Datenkategorien Gedanken um den Schutzbedarf gemacht und darauf aufbauend technische und organisatorische Schutzmaßnahmen implementiert hat, wird es für eine Datenschutzaufsichtsbehörde sehr schwierig, zu argumentieren, dass die konkreten Maßnahmen nicht ausreichen. Zumindest Bußgelder werden in einem solchen Fall kaum erlassen werden können – schon allein, weil das Rechtstaatsgebot für schwer sanktionierte Verbote wesentlich präzisere Tatbestände verlangt, als dies in Art. 32 DSGVO umgesetzt wird. Solange keine detaillierte Rechtsprechung zu Art. 32 DSGVO existiert, wird es daher genügen, wenn eine Dokumentation der Auswahl der technischen und organisatorischen Maßnahmen „plausibel" und „in sich schlüssig" erscheint; nahezu unabhängig davon, welche konkreten Maßnahmen genau gewählt wurden. Dies ist gewissermaßen die Kehrseite der Medaille der tatsächlichen und rechtlichen Unsicherheit über die Handhabung von Art. 32 DSGVO.

Häufig wird man in kleineren Kanzleien feststellen, dass Standardmaßnahmen wie das regelmäßige Ändern von Passwörtern und das regelmäßige Updaten von Software bereits intuitiv vorgenommen werden (oder die Software es mittlerweile automatisch so vorsieht). Dann muss nichts weiter veranlasst werden, als diese Maßnahme zu dokumentieren und anhand des Schutzbedarfs der Kanzlei zu argumentieren, dass diese Maßnahmen ausreichen.

(6) ZERTIFIZIERUNG NACH IT-SICHERHEITSNORMEN

Angesichts der enormen Unsicherheit über die Frage, wann das Maß einer „ausreichenden" IT-Sicherheit gegeben ist, gehen viele Unternehmen dazu über, die eigene IT-Sicherheit durch einen externen Auditor begutachten zu lassen, mit dem Ziel, ein Zertifikat darüber zu erlangen. Schließlich, so wird argumentiert, kann sich ein Geschäftsführer, IT-Sicherheitsbeauftragter oder Datenschutzbeauftragter trotz der Unsicherheit der Materie nichts mehr vorwerfen lassen, wenn ein seriöser und anerkannter externer Spezialist, die IT-Sicherheit für zertifizierungswürdig gehalten hat. Insbesondere das Sicherheitsmanagement kann nach der sehr verbreiteten ISO 27001 Norm zertifiziert werden.

Die Durchführung eines entsprechenden Audits und vor allem dessen Vorbereitung sind jedoch ohne spezialisierte Experten in diesem Bereich nicht zu schaffen. Deswegen sind Anwälte bislang kaum dazu übergegangen, die eigene Kanzlei zertifizieren zu lassen. Leichter möglich ist es allerdings für einen Anwalt, Teile der IT-Infrastruktur auf einen Dienstleister auszulagern, der seinerseits entsprechend zertifiziert ist. Bei der Auswahl eines geeigneten Cloud-Service-Providers sollte also auf entsprechende Zertifikate geachtet werden. So ist etwa der vom DAV empfohlene Hoster TeamDrive Systems GmbH entsprechend ISO 27001 zertifiziert.

7. CYBERSCHUTZVERSICHERUNG – MÖGLICH UND SINNVOLL?

Auch Versicherer haben seit ein paar Jahren erkannt, dass keinem Unternehmen und keinem Anwalt eine hundertprozentige Vermeidung von Hackings und anderen IT-Sicherheitsproblemen gelingen kann. Nachdem zunächst in den USA entsprechende Versicherungsprodukte entstanden, boomt nun seit zwei bis drei Jahren auch in Deutschland der Markt für sogenannte Cyber-Policen, die im Versicherungsfall häufig nicht nur für Schäden aufkommen, sondern auch Assistance-Leistungen, wie die Zurverfügungstellung spezialisierter IT-Forensiker, Hilfe durch Kommunikationsagenturen für die Außendarstellung und Hilfe durch spezialisierte Anwälte für Fragen von Meldepflichten und möglichen Regressansprüchen im Zusammenhang mit IT-Sicherheitsverstößen bieten. Da der Markt für Cyber-Policen noch relativ jung ist und sich noch kein Standard-Wording für Versicherungsbedingungen vollständig durchgesetzt hat, lohnt es sich gerade für kleinere Unternehmen und Anwaltskanzleien, mehrere Anbieter von Cyber-Policen um Angebote zu bitten oder einen spezialisierten Makler zu konsultieren.

Wichtig ist im vorliegenden Zusammenhang allerdings Folgendes:
Die Versicherungsbedingungen werden stets vorsehen, dass der Versicherte gewisse Obliegenheiten im Bereich der IT-Sicherheit erfüllen muss.

Insbesondere muss der Versicherungsnehmer ein gewisses Maß an IT-Sicherheitsmaßnahmen treffen. Auch hierfür hat sich in der Praxis noch kein einheitlicher Standard durchgesetzt.

Klar ist jedenfalls: Wenn man nach einem Hacking die Versicherung in Anspruch nehmen will und keinerlei Dokumentation über die eigene IT-Sicherheit geführt hat, so hat man auch schlechte Karten gegenüber der Versicherung.

Besteht hingegen die oben beschriebene Dokumentation der IT-Sicherheitsmaßnahmen, bestehen gute Chancen, im Schadensfall die Versicherung auch in Anspruch nehmen zu können. Hat man bereits bei Vertragsabschluss eine ordentliche Dokumentation vorzuweisen, kann es sogar gelingen, die Gebühren für die Versicherung nach unten zu verhandeln und mit der Versicherung abzuklären, ob die getroffenen und dokumentierten IT-Sicherheitsmaßnahmen nach Ansicht der Versicherung ausreichen, um die Obliegenheiten zu erfüllen. Welche Fragen eine Versicherung typischerweise vor Abschluss einer Cyber-Police stellt, geht aus einem Muster-Fragekatalog hervor, welcher von dem Gesamtverbund der Deutschen Versicherungswirtschaft (GDV) online kostenlos zur Verfügung gestellt wird: **Musterbedingungen.**

Zudem wird folgender Katalog an Mindest-IT-Sicherheitsmaßnahmen von der GDV empfohlen: **Diesen IT-Schutz sollten alle Unternehmen haben.**

8. RATING AKTUELLER CYBER-VERSICHERUNGEN – DIE BESTEN TARIFE

Die Ratingagentur Franke und Bornberg hat ein Rating für gewerbliche Cyber-Policen im deutschen Markt veröffentlicht. Untersucht wurden 35 Tarife und Bausteinlösungen von 28 Anbietern. Noch sind die Leistungsunterschiede groß und es gibt nur wenige Top-Tarife.

Westfälische Provinzial **Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall, Stand 04.2019** **FFF** **sehr gut (1,5)**	**Provinzial Nord** **Cyber-Versicherung mit Bausteinen Haftpflicht, Eigen-, Vertrauensschaden, Ertragsausfall, Stand 04.2019** **FFF** **sehr gut (1,5)**	**AIG EUROPE** **CyberEdge online 3.0, Stand 08.2018** **FF+** **gut (1,7)**	**HISCOX** **CyberClear, Stand 01.2018, Cyber-Diebstahl, Stand 01.2018, Betriebsunterbrechung durch Cloud-Ausfall, Stand 01.2018** **FF+** **gut (1,7)**
Markel **Markel Pro Cyber, 01.2018, Cyber-Haftpflicht, 01.2018, Cyber-Forderung, 01.2018, Cyber-Zahlungsmittel, 01.2018, Cyber-Vertrauensschaden, 01.2018, Cyber-Betriebsunterbrechung, 01.2018** **FF+** **gut (1,8)**	**Basler** **Cyber-Police mit Betriebsunterbrechung wegen Ausfall des Dienstleisters und Sublimit-Anhebung, Stand 01.2019** **FF+** **gut (1,8)**	**Gothaer** **Cyber-Versicherung für Gewerbekunden, Stand 10.2018, Erhöhung der Sublimits auf 20% der Versicherungssumme, Stand 10.2018** **FF+** **gut (2,4)**	**HDI** **Cyberversicherung für Firmen und Freie Berufe, Stand 10.2018, Internet-Diebstahl, Stand 10.2018, Betriebsunterbrechung durch Cloud-Ausfall, Stand 10.2018, Leistungs-Update-Garantie, Stand 10.2018, Cyber-Spionage, Stand 10.2018** **FF+** **gut (2,5)**

Quelle: Franke & Bornberg

Das gesamte Rating für Cyber-Versicherungen mit weiteren Versicherungsanbietern finden Sie auf franke-bornberg.de

Für Hintergrundinfos zum Rating hier klicken

Notensystem		Anzahl der mit dieser Note bewerteten Tarife
FFF	sehr gut	2
FF+	gut	6
FF	befriedigend	11
F+	ausreichend	8
F	mangelhaft	4
F-	ungenügend	5

ÜBER FRANKE UND BORNBERG

Franke und Bornberg analysiert seit 1994 Versicherungsprodukte und Versicherungsunternehmen. Die für die Analysen verwendeten Daten werden dabei vom in Hannover ansässigen Unternehmen eigenständig recherchiert. Franke und Bornberg ist fachlich und wirtschaftlich unabhängig.

9. HAFTUNG FÜR IT-SICHERHEITSVORFÄLLE: GENAUE DOKUMENTATION SCHÜTZT VOR HAFTUNG

Kommt es in einer Kanzlei zu einem IT-Sicherheitsvorfall und entsteht einem Betroffenen dadurch ein Schaden, kann die Kanzlei für den Schaden haftbar gemacht werden. Neben dem vertraglichen Schadensersatzanspruch nach § 280 Abs. 1 BGB und dem deliktischen Anspruch aus § 823 Abs. 1 BGB kommt auch ein spezieller deliktischer Schadensersatzanspruch gemäß Art. 82 Abs. 1 DSGVO in Betracht. Letzterer beinhaltet nicht nur eine Verschuldensvermutung, sondern auch den Ersatz von immateriellen Schäden.

Dabei ist zu berücksichtigen, dass die Haftung nach Art. 82 Abs. 1 DSGVO nicht nur gegenüber dem eigenen Mandanten, sondern gegebenenfalls auch gegenüber Dritten (z. B. der gegnerischen Partei) entstehen kann, wohingegen die Haftung nach § 280 Abs. 1 BGB lediglich auf den eigenen Mandanten beschränkt ist. Des Weiteren ist zu berücksichtigen, dass Art. 82 DSGVO eine gesamtschuldnerische Haftung von Verantwortlichen und Auftragsverarbeitern vorsieht, sodass auch beim Einsatz von Dienstleistern entsprechende Sorgfalt einzuhalten ist.

Es liegt auf der Hand, dass eine Exkulpation im Rahmen der Haftung von Art. 82 DSGVO häufig nur gelingen kann, wenn eine ausreichende Dokumentation vorliegt, die belegt, dass die Vorgaben der DSGVO – insbesondere die des Art. 32 DSGVO – erfüllt waren.

10. FAZIT – GUTE IT-SICHERHEIT IST DER BESTE SELBSTSCHUTZ! ZUSAMMENFASSEND KANN FOLGENDES FESTGEHALTEN WERDEN:

- ☛ Anwälte sind schon länger aufgrund von Standesrecht und strafrechtlichen Vorgaben dazu verpflichtet, ein ausreichendes Maß an IT-Sicherheit zu gewähren, um die Verschwiegenheitsverpflichtung zu wahren. Neu ist, dass seit dem 25.05.2018 ein Verstoß gegen die IT-Sicherheitsvorgaben aus Art. 32 DSGVO mit einem Bußgeld von bis zu EUR 10.000.000 geahndet werden kann.

- ☛ Anlassunabhängige Aktivitäten von Datenschutzaufsichtsbehörden werden zwar nicht mit einer hohen Wahrscheinlichkeit flächendeckend erwartet, aber Behörden werden derzeit umfangreich bei Beschwerden von Betroffenen tätig (Betroffener kann der eigene Mandant, der Gegner, der gegnerische Anwalt oder ein beliebiger Dritter sein, dessen Daten in einer Anwaltskanzlei gespeichert werden).

- In Zeiten der Digitalisierung sind Anwälte theoretisch und praktisch vielfältigen Gefahren ausgesetzt. Großkanzleien (mit eigener IT-Abteilung) wurden bereits Opfer von Hacking, gerade für kleine Kanzleien verbleibt eine große Unsicherheit, wie gefährdet ihre IT wirklich ist.

- Vor diesem Hintergrund ist es empfehlenswert, zumindest gewisse „Standardmaßnahmen" der IT-Sicherheit umzusetzen und diese Umsetzung zu dokumentieren. Zudem sollte im Rahmen einer Schutzbedarfsanalyse geprüft (und dokumentiert) werden, mit welchen Risiken für die Betroffenen die Verarbeitung der Daten in der Kanzlei einhergeht. Darauf aufbauend sollte dokumentiert werden, dass die getroffenen Maßnahmen angesichts der Schutzbedarfsanalyse ausreichend sind, um den identifizierten Risiken zu begegnen.

- Viele Anwälte werden sich dies zu Recht nicht alleine zutrauen und sollten in diesem Fall auf einen externen IT-Sicherheitsspezialisten zurückgreifen.

- Angesichts der Unsicherheit über die konkreten Vorgaben aus Art. 32 DSGVO bzw. der Frage, welche IT-Sicherheitsmaßnahmen als „ausreichend" betrachtet werden können, versuchen viele Unternehmen, Ihre IT nach anerkannten IT-Sicherheitsstandards (wie etwa ISO 27001) zu zertifizieren. Für Kanzleien ist der hierfür erforderliche Aufwand jedoch regelmäßig zu groß, so dass entsprechende Zertifizierungen für Anwälte bislang Einzelfälle sind. Soweit man die eigene IT oder Teile davon auslagert, empfiehlt es sich jedenfalls, ein zertifiziertes Rechenzentrum zu wählen, um auch in der eigenen Dokumentation auf dieses Zertifikat verweisen zu können.

- Es lohnt sich auch für Anwälte, sich auf dem jungen Markt der Cyber-Versicherungen umzusehen. Eine gut dokumentierte IT-Sicherheit hilft sowohl beim Abschluss eines Versicherungsvertrages als auch der Verhandlung der Versicherungsprämie. Zudem könnte die Versicherung bestätigen, dass die gegenwärtig dokumentierte IT-Sicherheit ausreichend ist.

CHECKLISTE DER WICHTIGSTEN SICHERHEITSVORKEHRUNGEN IN DER ANWALTSKANZLEI

BITTE BERÜCKSICHTIGEN SIE:
Vor dem oben geschilderten Hintergrund müssen sich die konkreten IT-Sicherheitsmaßnamen auf den spezifischen Schutzbedarf in einer Kanzlei beziehen. Die Checkliste bietet einen Anhaltspunkt für durchschnittliche Kanzleien, sie sollte aber nicht unhinterfragt auf jede Kanzlei angewendet werden. Der Bedarf an Schutzmaßnahmen sollte für jede Kanzlei individuell ermittelt werden.

- ✔ **Starke Passwörter**
  Achten Sie darauf, dass Sie das Beste aus Ihrer bisherigen Infrastruktur rausholen. Hierzu gehören die Verwendung von starken anstelle von schwachen Passwörtern und die regelmäßige Änderung wichtiger Passwörter.

- ✔ **Software-Updates**
  Verwenden Sie nur solche Software, die einen gewissen Sicherheitsstandard aufweist und die regelmäßig auch mit Updates unterstützt wird. Nur durch eine schnelle Beseitigung von Sicherheitslücken seitens des Softwareherstellers ist es Ihnen möglich, Ihre Daten erfolgreich zu schützen. Hier gilt auch das Prinzip Qualität vor Quantität: Nutzen Sie deshalb lieber weniger und qualitativ hochwertige Software als viele verschiedene Tools von einer Vielzahl von Anbietern (hierdurch steigt nämlich das Risiko von Sicherheitslücken).

- ✔ **Verschlüsselung von Datenbeständen**
  Zur Verschlüsslung von Daten auf Festplatten stehen kostenlose Softwaretools wie etwa „Veracrypt“ oder auch Standard-Windows-Funktionen zur Verfügung. Diese sollten genutzt werden. Professionelle Kanzleisoftware sollte eigene Verschlüsselungsmechanismen aufweisen.

- ✔ **Vermeidung der Nutzung derselben Geräte/Software für berufliche und private Zwecke**
  Stellen Sie sich die Frage, ob private Hardware/Software beruflich und berufliche Hardware/Software privat genutzt wird, da durch die Doppelnutzung regelmäßig ein gesteigertes Sicherheitsrisiko begründet wird.

- ✔ **Zugangsberechtigung**
  Auf analoger und digitaler Ebene sollten verschiedene Ebenen der Zugangsberechtigung erstellt werden. Desto weniger Personen Zugriff auf Daten haben, desto geringer sind auch die Sicherheitsrisiken.

- ✔ **Fernzugriff**
  Falls Sie auf Ihre Daten auch außerhalb des Büros zugreifen möchten, ist es wichtig, dass diese externen Zugriffe einen hinreichenden Schutz aufweisen. So sollte bei empfindlichen Daten regelmäßig mit einer VPN-Verbindung gearbeitet werden.

- ✔ **Backup-System**
  Achten Sie darauf, hinreichende externe Backups von Daten zu erstellen, um so den Verlust von Daten präventiv zu vermeiden.

- ✔ **Zumindest „Transportverschlüsselung“ von E-Mails**
  Verschlüsselung von E-Mails per TLS wird empfohlen. Die Abkürzung TLS steht für „Transport Layer Security“. Bei TLS handelt es sich um eine selbständig ablaufende Verschlüsselung des Transportweges der E-Mail. Die meisten E-Mail-Server verwenden TLS automatisch. Dies gilt auch für E-Mail-Server von Anbietern wie gmx.de oder web.de. Fragen Sie Ihren IT-Dienstleiter, ob auch Ihre E-Mails automatisch per TLS verschlüsselt werden (und lassen sie sich von Mandanten in Ihrer Mandatsvereinbarung bestätigen, dass diese Verschlüsslung dem Mandanten genügt und dass auch der Web-Server des Mandanten die TLS-Verschlüsselung beherrscht).

- ✔ **Mitarbeiterschulung**
  Häufig ist der Mensch das „schwächste Glied“ in der Kette der IT-Sicherheit. Es ist also wichtig, dass die Mitarbeiter ein Sicherheitsbewusstsein entwickeln. Häufig fehlt es schlicht an der Kenntnis über den Themenbereich. Achten Sie darauf, dass Mitarbeiter Schulungen in IT-Sicherheit erhalten, die unter anderem die oben genannten Themen umfassen.

MKG

HIER GEHT ES ZU
MKGONLINE
FACHINFO-MAGAZIN

IMPRESSUM

FFI-Verlag
Verlag Freie Fachinformationen GmbH
Leyboldstraße 12
50354 Hürth

Ansprechpartnerin
für inhaltliche Fragen im Verlag:
Bettina Taylor
02233 80575-14
taylor@ffi-verlag.de
www.ffi-verlag.de

Bestellungen
ISBN: 978-3-96225-034-8
Über jede Buchhandlung und beim Verlag. Abbestellungen jederzeit gegenüber dem Verlag möglich.

Erscheinungsweise
6 Ausgaben pro Jahr, nur als PDF, nicht im Print. Für Bezieher kostenlos.

Bildquellen
- Frau am PC: Adobe Stock/Africa Studio
- Laptop mit „Ransomware Attack“: Adobe Stock/Rawf8
- Schwebende Paragraphen: Adobe Stock/sdecoret
- Weltkugel mit DSGVO: Adobe Stock/Stockwerk-Fotodesign
- Business Man mit „Cyber Risk Insurance“: Adobe Stock/Coloures-Pic
- Taste mit Schloss-Symbol: Adobe Stock/Maksim Kabakou
- Cyber-Schlüssel: Adobe Stock/pickup

Partnerunternehmen für junge Rechtsanwälte

EVENTS ZUM THEMA CYBERSICHERHEIT UND IT-RECHT VON DER DAVIT (ARBEITSGEMEINSCHAFT INFORMATIONSTECHNOLOGIE IM DEUTSCHEN ANWALTVEREIN)

- **19.–20.09.2019, Köln**
  9. NRW IT-Rechtstag
- **26.09.2019, Köln**
  Mobile Apps – Rechtliche Anforderungen und aktuelle Entwicklungen
- **17.10.2019, München**
  18. Bayerischer IT-Rechtstag 2019

Noch aktuellere News gibt es auf mkg-online.de

BESUCHEN SIE UNS AUF MKG-ONLINE.DE

Verpassen Sie keine Ausgabe! Hier geht es zum Newsletter-Abo: mkg-online.de/abo

Folgen Sie uns auch auf facebook!