01 | 2015

schweitzerthema

Praxiswissen für Ihre Steuerberater-Kanzlei | Datenschutz

Datenschutz in der Steuerberaterkanzlei: Heute und in Zukunft!

Wie Steuerberater heute sicher elektronisch kommunizieren können – Die verschlüsselte E-Mail und ihre Alternativen

In ihrer Informationsbroschüre »Verschlüsselung von E-Mails« stellt die DATEV fest, dass »die E-Mail der Briefpost [im Geschäftsleben] längst den Rang abgelaufen« hat. Der IT-Sachverständige Dr. Lenhard führt aus, »der oft gewählte Vergleich der E-Mail mit der Postkarte« sei »zutreffend – es fehl[e] selbst an der ›Minimalsicherung‹ eines verschlossenen Umschlags wie bei der postalischen Kommunikation« (Kazemi/Lenhard, Datenschutz in der Rechtsanwaltskanzlei, 2014, S. 31). Als Rechtsanwalt will ich an dieser Stelle nicht versuchen, die genauen technischen Hintergründe dieses Phänomens zu beschreiben. Wer hier mehr wissen will, dem sei das Studium der Ausführungen von Herrn Dr. Lenhard empfohlen. Fest steht jedoch: Die einfache, »aus dem Outlook« heraus versandte E-Mail ist unsicher, weil unverschlüsselt; sie kann mit relativ einfachen Mitteln von unbefugten Dritten mitgelesen und – dies ist vielleicht sogar noch gravierender – ohne Erkennbarkeit auf ihrem Weg vom Absender zum Empfänger inhaltlich verändert werden. Dennoch gaben 56 % der Befragten einer DsiN-Studie zur Sicherheitslage im Mittelstand 2013 an, sich nicht um die Sicherheit Ihres E-Mail-Verkehrs zu kümmern. Dies mag daran liegen, dass die Probleme nicht bekannt oder ihre »Lösung« als zu kompliziert empfunden wird. Den Mandanten hier jedoch im Unklaren zu lassen, ist sicherlich die schlechteste Vorgehensweise zur Problemlösung. Daher ist der Mandant jedenfalls auf die Gefahren der »unverschlüsselten« elektronischen Kommunikation hinzuweisen.

Die (unsichere) E-Mail ist heute Alltag!

Die einfache E-Mail kann mitgelesen und unbemerkt verändert werden!

Einwilligung des Mandanten erforderlich

Der bloße Hinweis reicht allerdings nicht aus: Mit Blick auf die Möglichkeit des unberechtigten Mitlesens der Kommunikation und § 203 StGB ist vielmehr eine konkrete Einwilligung des Mandanten in diese Kommunikationsform einzuholen. Dies kann im Rahmen der Mandatsannahme erfolgen und in beispielsweise wie folgt geschehen: *»Wenn der Auftraggeber der Kanzlei eine E-Mail-Adresse mitteilt, willigt er ein, dass die Kanzlei ihm ohne Einschränkung per E-Mail mandatsbezogene Informationen zusendet. Dem Auftraggeber ist bekannt, dass E-Mails Viren enthalten können, dass andere Internetteilnehmer von dem Inhalt Kenntnis nehmen können und dass nicht sichergestellt ist, dass E-Mails tatsächlich von dem Absender stammen, der*

Mit dieser Mustereinwilligung sind Sie sicher

angegeben ist. Der Auftraggeber wird hiermit auf die Möglichkeit hingewiesen, die vorgenannten Risiken zumindest teilweise durch eine verschlüsselte E-Mail-Kommunikation auszuschließen. Soweit der Auftraggeber eine verschlüsselte E-Mail-Kommunikation wünscht, bedarf es hierzu der Vereinbarung eines Verschlüsselungscodes mit der Kanzlei.«

DE-Mail und E-Post-Brief als Alternativen?

Wer hier nicht auf die »unsichere« Kommunikation setzen und dem Mandanten ein Mehr an Sicherheit bieten will, der sucht am Markt nach Alternativen. DE-Mail und ePost-Brief scheinen hier auf den ersten Blick eine gute und sichere Alternative. Bereits 2014 hatten wir diese Kommunikationslösungen in den Blick genommen und damals vor allem die fehlende Ende-zu-Ende-Verschlüsselung kritisiert. Sowohl die DE-Mail-Anbieter als auch die ePost haben hierauf reagiert und bieten seit 2015 auch die Möglichkeit der sicheren und hoch verschlüsselten Ende-zu-Ende-Kommunikation an (siehe hierzu Artikel bezüglich DE-Mail und betreffend ePost). Fest steht also, beide Varianten beseitigen die bestehenden Unsicherheiten; gleichwohl beinhalten sie auch praktische Nachteile. Einer ist sicherlich in dem umständlichen Registrierungsvorgang und dem Umstand zu sehen, dass DE-Mail und ePost-Brief nur deutschen Kunden offenstehen; ein im Ausland sitzender Mandant kann damit nicht erreicht werden. Die Registrierung ist zudem zeitaufwändig und für viele Mandanten daher keine echte Alternative. Aus Sicht des Steuerberaters sehe ich ein erhebliches Problem darin, dass die E-Mail-Kommunikation nicht mehr über die »eigene Domäne«, sondern über den jeweiligen Anbieter erfolgt. Wir tun uns hingegen schwer damit, die Endung »@steuerberaterxyz.de« durch »@epost.de« oder »@de-mail.de« zu ersetzen. Hierdurch geht ein zentraler Indentitätsfaktor verloren, weswegen wir uns in unserer Rechtsanwaltskanzlei gegen den Einsatz dieser Technik entschieden haben.

DE-Mail und E-Post haben reagiert…

…machen aber an den deutschen Grenzen halt.

Elektronische Aktenführung mit Mandantenzugriff

»Goodbye E-Mail – Welcome elektronisches Mandantenpostfach!« So bewirbt beispielsweise die Firma e.Consult aus Saarbrücken seine Kommunikationslösung »WebAkte« gegenüber Rechtsanwälten.

Die »WebAkte« ist keine E-Mail-Lösung, sondern eine Kommunikationsalternative. Die Kanzlei legt hierbei für ihren Mandanten eine »elektronische Akte« an, auf deren Inhalt der Mandant in der Folge zugreifen und hier sowohl vom Steuerberater bereitgestellte Dokumente herunterladen als auch eigene Dokumente zum Abruf durch den Steuerberater hochladen kann. Die »eAkte« ist dabei zwar vor allem bei Rechtsanwälten beliebt, ihre Nutzung steht indes auch den Steuerberatern offen. Auch andere Anbieter im Markt, wie beispielsweise die Firma polargold aus Hamburg bieten ähnliche Lösungen an.

Die Vorteile: Selbst große Dateien lassen sich so bequem dem Mandanten übermitteln, ohne auf Postfachbeschränkungen des jeweiligen E-Mail-Anbieters Rücksicht nehmen zu müssen. Up- und Download der Dateien erfolgen über verschlüsselte

Die Cloud der »WebAkte« hat Vor- und Nachteile!

Verbindungen.
Die Nachteile: Die Kommunikation mit dem Mandanten ist nicht so unkompliziert wie bei der Nutzung einer E-Mail, da sämtliche Dokumente und Nachrichten erst in die eAkte eingestellt werden müssen. Für die schnelle Kommunikation von unterwegs ist dies sicherlich ein Problem. Die Weboberfläche der »WebAkte« ist auf den deutschen Mandanten ausgerichtet, sodass sich Mandanten aus dem Ausland hier nur schwer zurechtfinden. Die Kommunikation ist nicht gänzlich von der Kenntnisnahme Dritter abgeschlossen, denn die Anbieter dieser Lösungen lassen sich oft weitreichende Administrationsrechte einräumen, die den Zugriff auf den jeweiligen Aktenінhalt ermöglichen. Hierauf ist vor dem Einsatz derartiger Produkte zu achten und in jedem Fall eine vorherige und konkrete Einwilligung des Mandanten in diese Administrationen einzuholen. Wer gleichwohl über den Einsatz elektronischer (Online-)Akten nachdenkt, der sollte bei der Auswahl des Dienstleisters auf die gebotene Sicherheit achten. Zwingend sind dabei

- der Einsatz deutscher oder im EU-Ausland belegener Server durch den Dienstleister,
- die Gewährleistung organisatorischer und technischer Maßnahmen zum Schutz Ihrer Daten durch den Dienstleister, deren Nachweis über entsprechende Zertifikate oder sonstige Prüfunterlagen erfolgen sollte,
- der Ausschluss unerlaubter Zugriffe auf die für für das Angebot genutzten technischen Einrichtungen und
- die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens beim Aufbau der Verbindung zu dem Server des Anbieters (bspw. SSL-Verschlüsselung).

Werden diese Kriterien eingehalten, bietet eine elektronische (Online-)Akte sicherlich ein Mehr an Sicherheit innerhalb der Mandantenkommunikation und ist gegenüber der einfachen und unverschlüsselten E-Mail klar im Vorteil.

DATEV E-Mail-Verschlüsselung

Eine gute Alternative zur einfachen E-Mail

Eine weitere Möglichkeit bietet der von der DATEV angebotene Service »DATEV E-Mail-Verschlüsselung«, der auf dem Angebot »DATEVnet« basiert und eine entsprechende Integration in die bestehenden E-Mail-Programme bietet. Die Verschlüsselung der E-Mails findet dabei nicht in der Kanzlei selbst, sondern auf den Servern der DATEV statt, zu denen die E-Mail mittels verschlüsselter Verbindung transportiert und dort entsprechend verschlüsselt wird. Der Vorteil dieser Lösung besteht klar darin, dass sich die Art der Verschlüsselung den technischen Gegebenheiten bei den Empfängern der E-Mails anpasst, denn die DATEV-Software prüft automatisch, ob der Mandant bereits über eine DATEV-SmartCard, mIDentity oder über ein vergleichbares System verfügt. Ist dies der Fall, erfolgt die Zustellung mittels S/MIME oder OpenPGP. Verfügt der Mandant nicht über eine entsprechende Lösung, wird die E-Mail automatisch in ein PDF-Dokument umgewandelt und dieses mit einem Kennwort verschlüsselt. Die Dateianhänge der E-Mail werden im Originalformat an das PDF-Dokument übergeben. Das Kennwort wird an den Steuerberater als Absender verschickt und kann dann per Telefon an den Mandanten übermittelt werden.

Weitere Anbieter am Markt

Eine ähnliche Lösung bietet der Anbieter Connectware mit seinem Angebot »Cryptshare« an. Weitere Anbieter derartiger Lösungen sind beispielsweise der Anbieter IntelliSecure, das System iQ.Suite Crypt Pro (welches eine serverbasierte E-Mail-Verschlüsselung ermöglicht) oder der Einsatz eines sog. SEPPMail-Servers, der einen sehr hohen Sicherheitsstandard bietet, aber auch mit erheblichen Kosten verbunden ist. Letztgenanntes System wird unter anderem zur Kommunikation im schweizerischen Gesundheitswesen verwandt. Die Aufzählung an dieser Stelle ist, dies sei noch mal hervorgehoben, keinesfalls abschließend und keine Empfehlung in die ein oder andere Richtung. Sie soll lediglich verdeutlichen, dass bereits heute zahlreiche Möglichkeiten existieren, um die elektronische Mandantenkommunikation sicher oder zumindest sicherer zu machen.
Den Leserinnen und Lesern sei daher empfohlen, sich hier genauer zu informieren. Dies dient nicht nur dem eigenen Schutz, sondern auch dem Mandanteninteresse!

Elektronische Kommunikation in der StB-Kanzlei

1. Überprüfen Sie jetzt die Sicherheit Ihrer elektronischen Kanzlei-Kommunikation.
2. Machen Sie Schluss mit der unverschlüsselten E-Mail ohne Mandanteneinwilligung – entweder
   - einigen Sie sich mit Ihrem Mandanten auf eine Verschlüsselung oder
   - Sie holen sich bei Ihrem Mandanten die Einwilligung (siehe Mustertext oben) zur »unverschlüsselten« elektronischen Kommunikation ein.
3. Alternativen wie ePost, DE-Mail, »DATEV E-Mail-Verschlüsselung« oder Cryptshare können datenschutzrechtlich zulässig eingesetzt werden, erfordern jedoch im Vergleich zur E-Mail z.T. erhebliche Umstellungen in der Kanzleikommunikation.

Rechtsanwalt Dr. Kazemi ist Autor zahlreicher Fachpublikationen zum Datenschutzrecht, unter anderem des im Jahre 2011 erschienen Werkes »Datenschutz in der anwaltlichen Beratung«.
Er veröffentlichte auch die kostenlose E-Broschüre »Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei« (Hier herunterladen, 5,6MB).

Dr. Robert Kazemi

Überblick Die Schweitzer Themen-Reihe »Datenschutz in der Steuerberaterkanzlei: Heute und in Zukunft!«

Teil 1: Wie Steuerberater schon heute sicher elektronisch kommunizieren können – Die verschlüsselte E-Mail und ihre Alternativen

Teil 2: Die häufigsten Datenschutz-Probleme in Steuerberaterkanzleien und wie man sie vermeidet! Erscheint ca. Oktober 2015.

Wir freuen uns auf Ihre Fragen, Anregungen und Diskussionsbeiträge.

Mit freundlichen Grüßen,
Barbara Mahlke
Programmleitung Recht & Beratung
b.mahlke@schweitzer-online.de

02|2015

schweitzerthema

Praxiswissen für Ihre Steuerberater-Kanzlei | Datenschutz

Datenschutz in der Steuerberaterkanzlei: Heute und in Zukunft!

Die fünf häufigsten Datenschutzprobleme im Büro des Steuerberaters

Vorwort

In diesem Artikel sollen Sie als Steuerberater nicht ein weiteres Mal lesen müssen, welche Gesetze zum Schutz der Mandantendaten von Ihnen beachtet werden müssen. Vielmehr möchte ich Ihnen im Folgenden die häufigsten Fallstricke erläutern, die sich organisatorisch sowie technisch ergeben und die manchmal trotz aller Bemühungen die Sicherheit von Daten im Büro des Steuerberaters gefährden.

Technische und organisatorische Maßnahmen

Daten nicht nur gegen illegalen Zugriff, sondern auch gegen Verlust schützen!

Datenschutz und Datensicherheit sind nicht nur auf das Verhindern von Zugriffen durch unberechtigte Dritte auf personenbezogene Daten beschränkt. Vielmehr geht es auch darum, Konsistenz und Wahrheitsgehalt der Daten zu gewährleisten. Die Daten müssen gegen ungewollte Manipulation ebenso gesichert sein wie gegen Verlust. Zwar relativiert § 9 Satz 2 BDSG die erforderlichen Maßnahmen dahin gehend, dass »die Maßnahmen nur erforderlich sind, wenn der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht«, jedoch kann davon ausgegangen werden, dass Mandantendaten generell als derart schutzbedürftig eingestuft werden, dass die Umsetzung grundlegender technischer und organisatorischer Maßnahmen obligatorisch für den Umgang damit ist. Zu derartigen Maßnahmen zählt auch die Datensicherung.

Datensicherung

Ein defekter Rechner kann den Fortbestand des Steuerbüros bedrohen!

Software und Hardware verursachen Kosten. Speziell im Steuerbüro ist das Wissen um kaufmännisches Handeln und effizientes Wirtschaften besonders ausgeprägt. Das wird häufig aber dahin gehend missverstanden, dass die Infrastruktur für Datensicherungen gänzlich eingespart wird. Risiken werden häufig unterschätzt. Was wäre aber, wenn der Server oder der zentrale Bürorechner ausfällt? Soweit die Daten nicht wiederhergestellt werden können, könnte ein derartiger Defekt u.U. den Fortbestand eines Steuerbüros bedrohen. Datenträger sind i.d.R. nicht unbegrenzt nutzbar. Es stellt sich also nicht die Frage, ob eine Festplatte irgendwann ihren Dienst versagt, sondern nur, wann dies geschehen wird. Häufig werden Datensicherungen

von einem Softwaresystem zwar periodisch erstellt, dabei aber auf die lokale Festplatte geschrieben. Fällt diese Festplatte dann aus, sind damit auch die Datensicherungen verloren. Diese sollten sicher außerhalb des Steuerbüros aufbewahrt werden oder zumindest in einem Tresor untergebracht sein, der auch einen gewissen Schutz gegen Feuer bietet.

Manchmal kommt es nach einem Havariefall (z.B. Blitzschlag) trotz einer intakten Datensicherung zu Problemen. Üblicherweise verwendet eine Software für Steuerberater eine Datenbank, deren Inhalt gesichert werden soll. Ist jedoch das entsprechende Programm nicht verfügbar, so ist die Datensicherung i.d.R. nutzlos. Im Rahmen der Notfallplanung sollten also auch Installationsressourcen oder Image-Sicherungen erstellt werden, mit denen das vollständige System im Notfall auch auf einem anderen Rechner wiederhergestellt werden kann. Schließlich reicht es nicht, täglich Datensicherungen[1] zu erstellen, wenn diese nicht auch auf Ihre Brauchbarkeit hin getestet werden.

Eine funktionierende Datensicherung kann essentiell für den Fortbestand eines Steuerbüros sein[2].

Checkliste Datensicherung

Daher sollten ein paar Eckpunkte beachtet werden:

- Stellen Sie sicher, dass Ihre Daten regelmäßig gesichert werden.
- Überprüfen Sie regelmäßig die Datensicherung.
- Stellen Sie auch die (schnelle) Wiederherstellung des Basissystems sicher.
- Bewahren Sie die Datensicherungen stets an einem sicheren Ort auf.

WLAN

WLAN-Netze sind für Hacker-Angriffe anfälliger als kabelbasierte Netze

Der Zugang zu einem kabelgebundenen Netzwerk ist i.d.R. ungleich sicherer als das Verwenden von WLAN-Technologien. Ein WLAN ist ein Funknetz, dessen Empfangsbereich sich räumlich nicht exakt eingrenzen lässt. Daher bietet es eine breitere Basis für Angriffe durch Hacker als eine Netzwerkverkabelung. Das häufigste Problem bei WLAN besteht darin, dass die Technik nicht mehr hinterfragt wird, sobald das Netzwerk einmal eingerichtet ist. Im Bereich der WLAN-Router gibt es grundlegende technische Unterschiede, die sich direkt auf das Sicherheitsniveau des Netzwerks auswirken. So ist z.B. Firewall längst nicht gleich Firewall. Es ist erforderlich, Geräte einzusetzen, die für den professionellen Bereich geeignet sind. Es sollten auch regelmäßig Sicherheitsupdates in die Router eingespielt werden. Außerdem sollte die Netzwerk-ID nicht für jedermann sichtbar sein. Die Verschlüsselungsverfahren WEP und WPA entsprechen nicht mehr dem Stand der Technik. Derzeit sollte zumindest der Standard WPA2 verwendet werden. Schließlich sollte auch kein Gastzugang zu Ihrem Netzwerk vorhanden sein. Folgende Checkliste fasst die vorstehenden Ausführungen zusammen:

1 BSI-Grundschutzhandbuch, Maßnahmenkatalog M 6.32 Regelmäßige Datensicherung, abrufbar hier.
2 Kazemi / Lenhard, Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei, Deutscher Anwaltsverlag, 2014.

Checkliste für sicheres WLAN-Netz

Folgende Checkliste fasst die vorstehenden Ausführungen zusammen:

- Verwenden Sie nur WLAN-Router, die für den professionellen Einsatz geeignet sind.
- Achten Sie darauf, dass sich die Firewall-Funktionalitäten nicht nur auf eine Paket-Filterung beschränken.
- Verwenden Sie ausschließlich Verschlüsselungsvarianten, die dem jeweiligen Stand der Technik entsprechen, und lassen Sie im WLAN keine Netzwerk-ID anzeigen.
- Lassen Sie nicht zu, dass sich Gäste mit ihren mobilen Geräten über Ihr Kanzlei-Netzwerk mit dem Internet verbinden.

E-Mail

Unverschlüsselte E-Mails sind für die Kommunikation zwischen Anwalt und Mandant ungeeignet

Das Internet ist ein öffentliches Netz. Prinzipiell kann alles, was darüber übertragen wird, auch mitgelesen werden. Soweit eine E-Mail nicht verschlüsselt ist, werden die Daten im Klartext in Datenpaketen übertragen. An jedem denkbaren Knotenpunkt zwischen Sender und Empfänger können solche Pakete mitprotokolliert, gelesen oder nach Manipulation weiterversendet werden. Im Übrigen funktioniert das Mitprotokollieren auch bei Internet-Telefonie[3]. Da unverschlüsselte E-Mails keinerlei Schutz gegen unbefugtes Mitlesen bieten, sind diese grundsätzlich für die Kommunikation zwischen Steuerberater und Mandant ungeeignet. Allerdings ist die E-Mail mittlerweile ein allgemein genutztes Kommunikationsmittel, das aus den meisten Steuerbüros nicht mehr wegzudenken ist. Daher könnten im Steuerbüro spezielle E-Mail-Verfahren, wie z.B. DE-Mail, zum Einsatz kommen, bei denen eine Ende-zu-Ende-Verschlüsselung sichergestellt ist. Allerdings funktioniert das nur dann, wenn auch beide Seiten, d.h. Steuerberater und Mandant, dasselbe System verwenden. Der Markt bietet verschiedene Verschlüsselungsvarianten an, welche die Sicherheit der Nachrichtenübermittlung auf ein ausreichendes Niveau erhöhen können. Eine alternative Methode zur E-Mail wäre die Benutzung von serverbasierten Diensten mit Ende-zu-Ende-Verschlüsselung (sog. Webakten).

Schweitzer Thema: Wie Steuerberater heute sicher elektronisch kommunizieren können – Die verschlüsselte E-Mail und ihre Alternativen.

Mangelnde technische Absicherung von Servern

Der Kanzleiserver – das unterschätzte Risiko

Oft wird gefragt, was im Bezug auf Computersysteme denn schon passieren könnte. Mangels entsprechender Erfahrungen wird dann die Absicherung gegen Überspannung und Stromausfall ebenso vernachlässigt wie der Schutz gegen Gefährdungen wie Wasser, Feuer, Diebstahl oder mutwillige Zerstörung.

Die meisten Programme für Steuerberater arbeiten mit Datenbanken. Eine Datenbank ist ein komplexes Gebilde, dessen Systeme i.d.R. ein kontrolliertes Beenden erfordern, bevor ein Server ausgeschaltet wird. Fällt der Server durch einen Strom-

3 Vgl. L. L. Iacono; Abhören von IP-Telefonaten – Rote Telefone, Artikel auf Heise Online, iX-Magazin für professionelle Informationstechnik, abrufbar hier.

ausfall aus, so kann das u.U. eine Datenbank zerstören. Festplatten und andere Komponenten eines Rechners können bei Stromausfällen ebenfalls beschädigt werden. Wichtige Systeme sollten daher durch unterbrechungsfreie Stromversorgungen abgesichert werden. Darüber hinaus sollten Server so untergebracht sein, dass ein ausreichender Schutz gegen Gefährdungen, wie z.B. Feuer oder Wasser (z.B. Rohrbruch, Hochwasser), gegeben ist.
Da Server üblicherweise permanent in Betrieb sind, sollte ausschließlich für den Dauerbetrieb geeignete Hardware zum Einsatz kommen. Gespiegelte Festplatten (sog. RAID-Laufwerke) sind dabei ebenso obligatorisch wie redundante Netzteile.
Weiterhin ist es unverzichtbar, dass alle Server und Rechner des Steuerbüros über aktuelle Antiviren-Software verfügen und das Netzwerk zum Internet hin durch eine professionelle Firewall gesichert ist.

Checkliste zur Absicherung von Servern

Folgende Checkliste mag hierzu dienlich sein:

- Setzen Sie für Server nur Hardware ein, die für den Dauerbetrieb geeignet ist.
- Sichern Sie Server stets durch unterbrechungsfreie Stromversorgung ab.
- Vermeiden Sie ein Steckerleisten-Chaos!
- Bringen Sie Ihre Server an einem trockenen, sicheren Ort unter. Beachten Sie dabei, dass gegebenenfalls eine enorme Abwärme entsteht.
- Sichern Sie das Netzwerk zum Internet hin durch eine professionelle Firewall, für die es regelmäßige Sicherheitsupdates gibt.

Fehlende Schulung der Mitarbeiter

Brauche ich einen Datenschutzbeauftragten?

Aus gutem Grund hat der Gesetzgeber den Datenschutzbeauftragten die Pflicht auferlegt, Mitarbeiter für einen sicheren Umgang mit personenbezogenen Daten zu sensibilisieren. Ein entsprechender Mangel ist oft der Tatsache geschuldet, dass das Steuerbüro keinen ordentlich bestellten Datenschutzbeauftragten hat. Soweit mehr als neun Mitarbeiter mit der Bearbeitung personenbezogener Daten (das wäre bereits der Zugriff auf ein E-Mail-Verzeichnis) befasst sind, besteht eine gesetzliche Pflicht, einen Datenschutzbeauftragten zu bestellen. Sie sollten dabei aber nicht eine lapidare ein- bis dreitägige Schulung als ausreichende Qualifikation ansehen, sondern einen Experten damit beauftragen. Schließlich bleiben Sie immer verantwortlich für die Sicherheit personenbezogener Daten in Ihrem Steuerbüro.
Selbst wenn Sie nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, sollten Sie dennoch dafür Sorge tragen, dass Ihr Personal geschult ist.
Ansonsten tauchen zuweilen vermeidbare Probleme auf. Dazu gehört z.B. der Befall mit Computerviren. Zu einer derartigen Infektion kann es bereits durch das Anklicken eines E-Mail-Anhangs kommen. Viele Virenbefälle wären vermeidbar, wenn mit verringerten Rechten (Standardbenutzer) gearbeitet würde und Administratorkonten nur verwendet würden, wenn Software installiert wird oder Konfigurationsänderungen durchgeführt werden. Viele Viren können ein System nämlich nur befallen, wenn sie unter einem Benutzerkonto mit Administratorrechten aktiv sind.
Besonders gefährliche Bot-Viren konnten u.a. schon deshalb entdeckt werden, weil

Der Faktor Mensch – das Risiko Mensch

sensibilisierten Mitarbeitern ungewöhnliche Aktivitäten der Festplatten aufgefallen sind.

Nicht sensibilisierte Mitarbeiter nutzen zuweilen private USB-Sticks, um Ihren Kollegen Urlaubsbilder zu präsentieren. Dabei werden dann gleich auch diverse Viren ins System eingeschleppt. Die Schulung der Mitarbeiter bezieht sich aber auch auf Themen wie Identitätsdiebstahl oder Social Hacking, bei denen per E-Mail oder telefonisch versucht wird, an Daten zu gelangen.

Mitarbeiterschulungen sind elementar für den Datenschutz im Steuerbüro

Hier ein paar einfache Maßnahmen als Checkliste:

- Soweit mehr als 9 Personen für Ihr Büro tätig sind, bestellen Sie einen externen Spezialisten zum Datenschutzbeauftragten.
- Schulen Sie regelmäßig das gesamte Personal hinsichtlich Datenschutz und Datensicherheit.
- Vermeiden Sie die Nutzung privater Wechseldatenträger (z.B. USB-Stick). Eventuell kann hierzu auch eine technische Lösung eingesetzt werden.
- Nutzen Sie nur Benutzerkonten mit Administratorrechten, wenn das unbedingt erforderlich ist.

Beheben Sie die fünf häufigsten Datenschutzprobleme in Ihrem Steuerberaterbüro!

1. Überprüfen Sie jetzt Ihre Datensicherung.
2. Setzen Sie bei WLAN nur Geräte für den professionellen Bereich ein.
3. Informieren Sie sich über die verschlüsselte E-Mail und ihre Alternativen.
4. Beheben Sie mangelnde technische Absicherung von Servern.
5. Schulen Sie Ihre Mitarbeiter im sicheren Umgang mit personenbezogenen Daten.

Dr. Thomas H. Lenhard

Dr. Thomas H. Lenhard

Dr. Thomas H. Lenhard ist Geschäftsführer der medi-ip dataprotect UG in Bonn. 2011 wurde Dr.Lenhard vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein als Sachverständiger für IT-Produkte (technisch) akkreditiert. In den Jahren 2014 und 2015 folgten die Anerkennungen als Sachverständiger für das Europäische Datenschutzsiegel und für das Datenschutzsiegel Mecklenburg-Vorpommern. Er ist u.a. Co-Autor der kostenlosen E-Broschüre »Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei« (Hier herunterladen, 5,6MB).

Ausblick

Ausgabe 1/2016: Marketing Strategie für klassisches Marketing und Online-Marketing
Ausgabe 2/2016: Sichtbarkeit steigern durch Empfehlungsmarketing
Ausgabe 3/2016: Mit Mandanten in Kontakt kommen und bleiben

Wir freuen uns auf Ihre Fragen, Anregungen und Diskussionsbeiträge.

Mit freundlichen Grüßen,
Barbara Mahlke
Programmleitung Recht & Beratung
b.mahlke@schweitzer-online.de