Hinweise[1] der Bundessteuerberaterkammer zur Einhaltung der Verschwiegenheit, der Datensicherheit, des Datenschutzes und anderer Rechtsvorschriften bei Nutzung des Internet in der Steuerberaterpraxis

Beschlossen vom Präsidium der Bundessteuerberaterkammer am 10. September 2002

Inhaltsverzeichnis

Vorbemerkungen 2

1. Gefahren der Internetnutzung 2

2. Maßnahmen zur Minimierung des Sicherheitsrisikos 3

2.1 Personal 3

2.2 Sicherheitsmaßnahmen am Rechner 3

2.3 Disketten und andere Datenträger 4

2.3.1 Eingehende Disketten und andere Datenträger 4

2.3.2 Ausgehende Disketten und andere Datenträger 4

2.4 E-Mail-Verkehr und Eingabe von Daten auf Internetseiten 5

2.5 Verschlüsselung und elektronische Signatur 5

2.5.1 Verschlüsselung 6

2.5.2 Elektronische Signatur 6

2.5.3 Interoperabilität von elektronischen Signaturen und Verschlüsselungen 6

3. Homepage des Steuerberaters 7

3.1 Informationspflichten gem. Teledienstgesetz 7

3.2 Berufsrechtliche Regelungen 8

4. Maßnahmen bei Computerviren 9

Glossar 10

[1] Die Hinweise haben keinen verbindlichen Charakter. Sie sollen zu bestimmten Sachverhalten oder Problemkreisen Anregungen zu eigenverantwortlichen Lösungen geben und somit die Praxisarbeit unterstützen.

Vorbemerkungen

Die Nutzung von Datenverarbeitungssystemen und des Internet schaffen nicht nur Arbeitserleichterungen, sondern beschleunigen auch die Kommunikationsabläufe und ebnen den Weg zum papierlosen Büro. Daneben ist die Nutzung des Internet zu Zwecken der raschen Informationsbeschaffung, der elektronischen Abwicklung des Rechts- und Geschäftsverkehrs oder der Selbstdarstellung mittels einer eigenen **Homepage** mit einem enormen Einsparpotential verbunden.

Der Gesetzgeber hat dieser Entwicklung mit der Schaffung der Initiative „BundOnline 2005" Rechnung getragen. Danach sollen bis zum Jahr 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung online verfügbar sein und die elektronische Kommunikation ermöglicht werden.

Da die Nutzung des Internet neben den Chancen auch Risiken für das eigene DV-System birgt, werden in diesen Hinweisen Maßnahmen vorgestellt, die zur Minimierung des Sicherheitsrisikos beitragen sollen. Darüber hinaus wird über die Vorschriften für das Einrichten und Betreiben einer **Homepage** durch den Steuerberater informiert.

Weitere Hinweise sowie Erläuterungen zu den durch Fettdruck hervorgehobenen Begriffen befinden sich im Glossar.

1. Gefahren der Internetnutzung

Das Internet als Medium der Selbstdarstellung, Informationsbeschaffung oder Kommunikation mit Mandanten, Kollegen oder Behörden birgt erhebliche Risiken für Datenschutz und Datensicherheit. So lassen sich z.B. Daten, die offen über das Internet übertragen werden, wie E-Mails oder auf Formularen im Internet eingegebene Daten, von jedem, der Zugang zu einem benutzten Netz hat, unbemerkt mitlesen, kopieren oder verfälschen. Angriffe durch **Hacker**, **Computerviren**, **Trojanische Pferde** und **aktive bzw. ausführbare Inhalte** gefährden das eigene DV-System. Andere Belästigungen können z.B. durch die Versendung von Massen-E-Mails mit Werbebotschaften oder durch gefälschte Warnmeldungen über neue **Computerviren** entstehen.

Mandanten vertrauen darauf, dass ihr Steuerberater geeignete Maßnahmen zum Datenschutz und zur Datensicherheit getroffen hat. **Computerviren**, **Hacker**, **Trojanische Pferde** und **ausführbare Inhalte** führen daher nicht nur zur Schädigung der eigenen bzw. mandantenbezogenen Daten, zur Beeinträchtigung der Arbeit sowie zu finanziellen Schäden durch Betriebsausfälle, Folgeschäden oder Kosten für die Wiederherstellung der Daten, sondern können auch einen erheblichen Image- und Vertrauensschaden anrichten. Dies gilt umso mehr, wenn z.B. virenbefallene Dateien per E-Mail an Man-

danten versandt werden, dort den Rechnerbetrieb lahm legen oder wichtige Unternehmensdaten zerstören.

Im Folgenden werden daher einzelne Hinweise zur Minimierung des Sicherheitsrisikos gegeben:

2. Maßnahmen zur Minimierung des Sicherheitsrisikos

2.1 Personal

Die umfassende Information des Personals und die Sensibilisierung für Sicherheitsrisiken bieten den wichtigsten Schutz gegen Angriffe. Hierzu empfiehlt es sich, verbindliche **Sicherheitsregeln** (z.B. Passwortgenerierung, Zugriffschutz) und verbindliche **Richtlinien zur Nutzung der betrieblichen EDV** (z.B. Regelungen zur privaten Internetnutzung) aufzustellen und in schriftlichen Vereinbarungen mit den Mitarbeitern verbindlich niederzulegen.

2.2 Sicherheitsmaßnahmen am Rechner

Die Anbindung des Praxisnetzes an das Internet sollte über eine aktuelle und stets gewartete **Firewall** erfolgen. Die Firewall ist kein Virenschutzprogramm, sondern sie entscheidet darüber, welche Daten oder Dateien von außen nach innen gelangen dürfen. Die Firewall sollte so eingestellt sein, dass nach einer bestimmten Anzahl von fehlgeschlagenen Versuchen, die Firewall zu überwinden, der Zugang automatisch gesperrt wird.

Auf allen Rechnern der Steuerberaterpraxis sollte ein aktuelles Virenschutzprogramm installiert sein. Die Überprüfung von Hard- und Software sollte regelmäßig erfolgen. Durch ein stets aktualisiertes Virenschutzprogramm (Virensuchprogramme können nur bekannte Viren finden) kann die Abwehr von Viren größtenteils gewährleistet werden. Der Steuerberater sollte sich daher bei seinem Provider vergewissern, ob der Virenscanner regelmäßig aktualisiert wird. Wichtig ist auch, ob das Virenschutzprogramm in der Lage ist, alle Dateiformate zu scannen. Ein Problem bilden verschlüsselte E-Mails, da das Virenschutzprogramm auf diese aufgrund der Verschlüsselung nicht zugreifen kann. Verschlüsselte E-Mails und verschlüsselte Anhänge müssen daher vor dem Öffnen erst entschlüsselt, und auf Viren geprüft werden.

Bei vernetzten Rechnern empfiehlt es sich, die Schreib- bzw. Leserechte der Anwender auf dem Server einzustellen. Auf die Festplatte des Servers kann ein Computervirus nur im Rahmen der Rechte des Anwenders zugreifen. Bestehen nur Lese- und Ausführungsrechte bei den Programmdateien, wird bei Infektion eines Rechners die Gefahr der Übertragung des Virus über den Server auf andere Rechner deutlich reduziert.

Beim Internetbrowser können verschiedene Sicherheitsstufen eingestellt werden. Durch eine entsprechende **Browsereinstellung** kann z.B. die Ausführung von aktiven Inhalten unterbunden werden.

Jeder Arbeitsplatz benötigt einen Passwortschutz für den Rechnerzugang. Dies gilt auch für Notebooks, die nicht ständig in das Netzwerk eingebunden sind. Sensitive Daten der Steuerberaterpraxis sollten zusätzlich mit einem Passwort geschützt werden. Passworte sind so auszuwählen, dass sie nicht leicht zu erraten sind. D.h. Trivialpassworte, wie z.B. der eigene Vorname oder das Geburtsdatum, bilden keinen ausreichenden Passwortschutz. Liegen die Administratorrechte beim Steuerberater, so kann dieser mit Hilfe des Administratorpasswortes den Mitarbeitern einzelne Passworte zuordnen oder diese ändern. Hat ein Dritter die Administratorrechte sollte auf die Protokollierung aller Nutzungen und Tätigkeiten mit dem Administratorpasswort geachtet werden. Weiter empfiehlt es sich, für den Notfall die Passworte der Mitarbeiter an vertraulicher Stelle zu hinterlegen, um durch den Ausfall einzelner Mitarbeiter nicht den ganzen Betrieb lahm zu legen.

Eine weitere Möglichkeit zum Schutz gegen die Gefahren des Internet bildet die Einrichtung eines Einzelplatzrechners, der ausschließlich für Zwecke der Internetnutzung verwendet wird und auf dem weder Mandantendaten noch Daten der Praxis verarbeitet werden. Daten von diesem PC sollten – wenn überhaupt – nur nach vorheriger Virenprüfung auf andere Rechner übertragen werden. Ist eine Internetnutzung nur von einem einzigen Rechner in der Steuerberaterpraxis möglich, werden die Vorteile der Informationsbeschaffung und Kommunikation über das Internet aufgegeben. Die Einrichtung eines Einzelplatzrechners für die Internetnutzung wird daher eher als Sonderfall eingestuft.

2.3 Disketten und andere Datenträger

2.3.1 Eingehende Disketten und andere Datenträger

Disketten, CD´s oder andere Datenträger sollten nur aus seriösen Quellen bezogen und vor jedem Einsatz auf Viren geprüft werden.

2.3.2 Ausgehende Disketten und andere Datenträger

Werden ausgehende Disketten erstellt, sollte zunächst der Rechner, auf dem die Diskette zusammengestellt wird, mit Hilfe eines aktuellen Virenschutzprogramms überprüft werden. Es empfiehlt sich, die Diskette neu zu formatieren und die Dateien fortlaufend auf die Diskette zu kopieren. Müssen bereits kopierte Dateien gelöscht und durch andere ersetzt werden, sollte der gesamte Erstellungsprozess mit der Formatierung der Diskette neu begonnen werden. Nach Fertigstellung der Diskette sollte diese mit dem **Hardwareschutz** versehen und vor dem Versand auf Viren geprüft werden. Es empfiehlt sich, dieses Prüfprotokoll aufzuheben.

2.4 E-Mail-Verkehr und Eingabe von Daten auf Internetseiten

Wird eine E-Mail-Adresse öffentlich bekannt gemacht, muss der E-Mail-Eingang regelmäßig überwacht werden, da anderenfalls ein Verstoß gegen die gewissenhafte Berufsausübung gem. § 57 Abs. 1 StBerG vorliegen kann (siehe etwa § 63 StBerG). Für die Archivierung der mandatsbezogenen Korrespondenz gelten die gleichen Grundsätze wie für die Korrespondenz mit Schriftgut.

Weitere Hinweise zum E-Mail-Verkehr befinden sich im Glossar unter dem Stichwort **„Sicherheitsregeln“**.

Die Eingabe von Daten auf Internetseiten unterliegt den allgemeinen Pflichten des Steuerberaters zur Verwendung von Daten. Dabei ist zu beachten, dass bei Eingaben in ungeschützten Bereichen nicht sichergestellt ist, dass nur der rechtmäßige Empfänger diese Daten auslesen kann.

2.5 Verschlüsselung und elektronische Signatur

Die Steuerberaterkammern sind bemüht, den Berufsangehörigen auf höchstem Sicherheitsniveau die modernste Technologie für die Verschlüsselung und elektronische Signatur bereitzustellen. Aus diesem Grund haben sich die Steuerberaterkammern frühzeitig auf dem Gebiet engagiert und sind führend in dieser Technologie.

Einige Steuerberaterkammern sind inzwischen **akkreditierte Zertifizierungsdiensteanbieter** und erfüllen somit die Anforderungen der höchsten Sicherheitsstufe für elektronische Signaturen nach dem Signaturgesetz. Mit Hilfe der von den Steuerberaterkammern ausgegebenen Signaturkarte und Software kann ein elektronisches Dokument oder eine Datei mit der **qualifizierten elektronischen Signatur mit Anbieterakkreditierung** unterzeichnet werden. E-Mails können mit der **fortgeschrittenen elektronischen Signatur** versehen werden. In allen Fällen ist zusätzlich eine Verschlüsselung möglich.

Das Verfahren der elektronischen Signatur befindet sich noch in der Erprobungsphase und unterliegt ständigen Fortentwicklungen. In vielen Bereichen wurde der elektronische Rechts- und Geschäftsverkehr vom Gesetzgeber bereits geregelt, z.B. § 87a AO, § 3a VwVfG, § 126a BGB, § 14 Abs. 4 UStG, § 130a ZPO, § 77a FGO.

2.5.1 Verschlüsselung

Für den Versand von vertraulichen E-Mails und deren Anlagen ist eine Verschlüsselung unerlässlich, um zu verhindern, dass Unbefugte durch Mitlesen von dem Inhalt Kenntnis erlangen.

Die elektronische Signatur ist unabhängig von einer Verschlüsselung. D.h. ein mit einer elektronischen Signatur versehenes Dokument bleibt lesbar, sofern es nicht zusätzlich verschlüsselt wird. Für die Verschlüsselung wird ähnlich der elektronischen Signatur ein Schlüsselpaar verwendet. Der Absender verschlüsselt die Nachricht oder das Dokument mit dem öffentlichen Schlüssel des Empfängers. Die verschlüsselte Nachricht bzw. das verschlüsselte Dokument kann nur mit dem geheimen privaten Schlüssel des Empfängers entschlüsselt, d.h. wieder lesbar gemacht, werden.

Eine Verschlüsselungssoftware wird von den Zertifizierungsdiensteanbietern, wie den Steuerberaterkammern, zusammen mit der Chipkarte für die elektronische Signatur bereitgestellt.

2.5.2 Elektronische Signatur

Nach dem neuen Signaturgesetz, in dem die EU-Richtlinie 1999/93/EG umgesetzt wurde, gibt es drei Formen von elektronischen Signaturen, die sich hinsichtlich des Grades an Sicherheitsanforderungen unterscheiden. Die **(einfache)** und die **fortgeschrittene elektronische Signatur** unterliegen keinen Regulierungen. Die **qualifizierte elektronische Signatur** ersetzt im elektronischen Rechts- und Geschäftsverkehr die eigenhändige Unterschrift und ist als Beweismittel vor Gericht zugelassen. Im Unterschied zur fortgeschrittenen elektronischen Signatur beruht die qualifizierte Signatur auf einem zum Zeitpunkt ihrer Erzeugung gültigen **Zertifikat**, auch „qualifiziertes Zertifikat“ genannt, das nur einer natürlichen Person zugeordnet werden kann. Die Verbindung zu der juristischen Person, z.B. der Steuerberatungsgesellschaft XY, oder der Berufsbezeichnung, z.B. „Steuerberater“, kann über die **Pseudonymisierung** bzw. das **Attributzertifikat** hergestellt werden. Die qualifizierte elektronische Signatur unter einem Dokument kann mit dem (qualifizierten) **Zeitstempel** des Zertifizierungsdiensteanbieters versehen werden. Anhand des Zeitstempels kann festgestellt werden, ob die qualifizierte elektronische Signatur und z.B. das Attribut „Steuerberater“ zum Zeitpunkt der Vertragsunterzeichnung oder der Unterzeichnung einer E-Mail gültig waren.

2.5.3 Interoperabilität von elektronischen Signaturen und Verschlüsselungen

Derzeit sind die Produkte der verschiedenen Zertifizierungsdiensteanbieter zur Signierung und Verschlüsselung von Nachrichten und Dokumenten noch nicht interoperabel (siehe auch im Glossar unter **Interoperabilität**). Die elektronische Signatur kann gegen den Verzeichnisdienst nur geprüft werden, wenn der Empfänger eines elektronischen Dokumentes über dieselbe Software verfügt wie der Absender. Die meisten Trustcenter bieten auf ihrer Homepage eine kostenlose Version ihrer Software an, mit deren Hilfe die elektronische Signatur geprüft werden kann. Weiter benötigt der Absender ei-

ner verschlüsselten Nachricht die Verschlüsselungssoftware sowie den öffentlichen Schlüssel des Empfängers.

3. Homepage des Steuerberaters

3.1 Informationspflichten gem. Teledienstgesetz

Das neue Teledienstgesetz begründet umfangreiche Informationspflichten für alle geschäftsmäßigen Teledienstanbieter. Zu diesen zählen auch Steuerberater, Steuerbevollmächtigte und Steuerberatungsgesellschaften, die eine **Homepage** eingerichtet haben. Ein Verstoß gegen die allgemeinen Informationspflichten gem. § 6 S. 1 Teledienstgesetz n.F. stellt eine Ordnungswidrigkeit dar und kann gem. § 12 Abs. 2 Teledienstgesetz n.F. mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Um den Anforderungen an die allgemeinen Informationspflichten gem. § 6 S. 1 Teledienstgesetz n.F. genüge zu leisten, müssen Steuerberater, Steuerbevollmächtigte und Steuerberatungsgesellschaften auf ihrer **Homepage** die nachstehenden Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar halten. Es empfiehlt sich, die geforderten Angaben in einen gesonderten Hauptmenüpunkt „Impressum“ einzustellen.

1. Name, Anschrift (kein Postfach), bei juristischen Personen zusätzlich den Vertretungsberechtigten
2. Telefon, Fax, E-Mail-Adresse
3. bei Steuerberatungsgesellschaften die Angabe des Handelsregisters und die Registernummer, bei Partnerschaftsgesellschaften - unabhängig von ihrer Anerkennung als Steuerberatungsgesellschaft - die Angabe des Partnerschaftsregisters und die Registernummer
4. Zuständige Aufsichtsbehörde, d.h. zuständige Steuerberaterkammer
5. Gesetzliche Berufsbezeichnung "Steuerberater" sowie den Zusatz „Die gesetzliche Berufsbezeichnung Steuerberater wurde in der Bundesrepublik Deutschland verliehen.“
6. Angabe der berufsrechtlichen Regelungen und das Zugänglichmachen dieser Regelungen:
   „Der Berufsstand der Steuerberater unterliegt im Wesentlichen den nachstehenden berufsrechtlichen Regelungen:
   (a) Steuerberatungsgesetz (StBerG)
   (b) Durchführungsverordnung zum Steuerberatungsgesetz (DVStB)
   (c) Berufsordnung (BOStB)
   (d) Steuerberatergebührenverordnung (StBGebV)“
7. Angabe der Umsatzsteueridentifikationsnummer, sofern gem. § 27a UStG vorhanden

Der Informationspflicht über die Zugänglichkeit der unter Punkt 6 genannten berufsrechtlichen Regelungen in ihrer jeweils aktuellen Fassung kann gem. der Begründung zu dem o.g. Gesetz wie folgt genüge geleistet werden:

1. Hinweis: „Die berufsrechtlichen Regelungen können bei der zuständigen Steuerberaterkammer (Name, Anschrift, Tel./Fax) eingesehen werden."

oder

2. Die Homepage des Steuerberaters wird mit der Startseite der Homepage der zuständigen Steuerberaterkammer bzw. der Bundessteuerberaterkammer (www.bstbk.de) verlinkt und der Steuerberater gibt auf seiner Homepage die entsprechende Rubrik an, unter der die berufsrechtlichen Regelungen auf der Homepage der zuständigen Steuerberaterkammer bzw. der Bundessteuerberaterkammer zu finden sind.

oder

3. Die Homepage des Steuerberaters wird mit der entsprechenden Seite der Homepage der zuständigen Steuerberaterkammer bzw. der Bundessteuerberaterkammer (www.bstbk.de) direkt verlinkt. Aufgrund der Dynamik des Internet erscheint eine Direktverlinkung auf Unterrubriken nicht empfehlenswert, da bei Veränderungen des Internetauftritts der Steuerberaterkammern bzw. der Bundessteuerberaterkammer dieser Link ins Leere läuft.

Aufgrund der Dynamik im Internet sollte der Steuerberater von Zeit zu Zeit

a) bei Verlinkung auf die Startseite der Homepage der zuständigen Steuerberaterkammer bzw. der Bundessteuerberaterkammer die Aktualität der auf der eigenen Homepage angegebenen Rubrik überprüfen

bzw.

b) bei der Direktverlinkung auf Unterrubriken die Linksetzung überprüfen.

3.2 Berufsrechtliche Regelungen

Nach den Vorschriften der Berufsordnung der Steuerberater ist die Darstellung in elektronischen Medien grundsätzlich erlaubt. Die Nutzung elektronischer Medien, Netze und Netzdienste unterliegt den Vorschriften der §§ 10 bis 21 BOStB i.V.m. §§ 57, 57a StBerG.

Hinsichtlich der Einrichtung und des Betreibens einer **Homepage** gelten § 57 Abs. 1 StBerG, das Bundesdatenschutzgesetz sowie andere Datenschutzgesetze[2], die den Steuerberater zur Einhaltung der Verschwiegenheit, der Datensicherheit und des Datenschutzes verpflichten. D.h. der Steuerberater muss auch in der virtuellen Steuerberaterpraxis alle organisatorischen Vorkehrungen treffen, um

[2] Vgl. Hinweise der Bundessteuerberaterkammer zur Verschwiegenheitspflicht, zur Datensicherheit und zum Datenschutz in der Steuerberaterpraxis

einen Verstoß gegen die Verschwiegenheitspflicht oder die o.g. Datenschutzgesetze zu unterbinden. Dies betrifft z.B. die sorgfältige Auswahl eines zuverlässigen Providers oder ggf. den Einsatz einer **Firewall** und eines Virenscanners. Der einwandfreie Betrieb der Homepage, ein virenfreier Download von Dokumenten der Homepage, die Versendung von vertraulichen Nachrichten durch verschlüsselte E-Mail sollten sichergestellt werden.

Die Auswahl des Domainnamens richtet sich nach den berufs- und wettbewerbsrechtlichen Bestimmungen für die Namensvergabe einer Steuerberaterpraxis. Gattungsbezeichnungen, wie z.B. www.steuerberater.de, sind grundsätzlich unzulässig. Um Konflikte bei Namensgleichheit zu vermeiden, empfiehlt es sich, den Namen um einen Ortszusatz zu erweitern (z.B. www.thomas.schulz-stb-paderborn.de, www.thomas.schulz-stb-berlin.de) und ggf. die verschiedenen Variationsmöglichkeiten auszuschöpfen (www.th.schulz-stb-paderborn.de, www.th.schulz-steuerberater-paderborn.de) oder auf andere Endungen für Web-Adressen, wie z.B. *.com oder *.pro, auszuweichen.

Beispiele für zulässige bzw. unzulässige Inhalte und Gestaltungen einer Homepage befinden sich im Glossar unter dem Stichwort „**Homepage**“.

Bei der Einrichtung und Gestaltung von Webseiten sollte auf Qualität, Aktualität der Informationen sowie auf die Einhaltung der aktuellen Rechtsvorschriften zum Berufsrecht und zum Datenschutz sowie auf die Entwicklung der Rechtsprechung geachtet werden.

4. Maßnahmen bei Computerviren

Bei ungewöhnlichen Reaktionen des PC wird häufig ein Virus als Ursache vermutet. Oft beruhen die Störungen des Rechners aber auf einer fehlerhaften Bedienung, technischen Defekten oder Fehlmeldungen des Virenschutzprogramms.

Bei Verdacht auf einen Virusbefall sollte nicht überstürzt gehandelt, sondern die Arbeit zügig und wie gewohnt beendet werden. Viele Viren sind während des Rechnerbetriebs - ohne Wissen des Nutzers – aktiv. D.h. sie haben in dieser Phase eine weitgehende Kontrolle über den Rechner, können sich weiter verbreiten und unterbinden Maßnahmen zur Virenentfernung bzw. infizieren gesäuberte Datenträger von neuem. Bei Virusverdacht muss der Computer daher zunächst heruntergefahren und ausgeschaltet werden. Es empfiehlt sich, das Personal über Verhaltensregeln bzw. Maßnahmen bei Verdacht auf Virenbefall zu informieren (siehe Glossar unter **Sicherheitsregeln**).

Mit der Analyse der Störungsursache bzw. mit der Virenentfernung sollte ein Experte beauftragt werden.

Glossar

Akkreditierter Zertifizierungsdiensteanbieter

Zertifizierungsdiensteanbieter können bei der Regulierungsbehörde für Post und Telekommunikation (RegTP) einen Antrag auf Akkreditierung stellen. Die Akkreditierung ist ein Gütezeichen, das die RegTP dem Zertifizierungsdiensteanbieter ausstellt, wenn eine umfassende Prüfung der verwendeten technischen Komponenten und des Sicherheitskonzeptes zu einem positiven Ergebnis geführt hat. Die auf einem qualifizierten **Zertifikat** beruhende **qualifizierte elektronische Signatur**, ausgestellt durch einen Zertifizierungsdiensteanbieter mit Anbieterakkreditierung, wird auch **qualifizierte elektronische Signatur mit Anbieterakkreditierung** genannt und entspricht der höchsten Sicherheitsstufe bei den elektronischen Signaturen. Diejenigen Steuerberaterkammern, die als Zertifizierungsdiensteanbieter tätig sind, sind akkreditiert und erfüllen somit die Anforderungen der höchsten Sicherheitsstufe.

Aktive bzw. ausführbare Inhalte/Programme

Da die Möglichkeiten, mit normalen HTML-Seiten ein dynamisches und benutzerorientiertes Internetangebot zu schaffen, begrenzt sind, werden Internetangebote zunehmend von ausführbaren Programmcodes unterstützt, die eine nahezu unbegrenzte Funktionsvielfalt bieten. Derartige Internetangebote sind ohne das Herunterladen und Ausführen von Programmen auf dem lokalen Rechner gar nicht oder nur mit Einschränkung nutzbar. Durch aktive bzw. ausführbare Inhalte auf Web-Seiten (z.B. Java, ActiveX) kommen Programme auf dem Rechner des Benutzers zur Ausführung, von denen dieser nicht unbedingt vorher weiß, was sie tun. Häufig ist beim Anklicken eines Links nicht klar ersichtlich, dass damit ein Programm gestartet wird. Durch aktive Inhalte können im eigenen DV-System Daten zerstört, übermittelt oder verändert werden. So können z.B. vertrauliche Daten des Steuerberaters ausgespäht und über bestehende Internetverbindungen direkt übertragen oder bei nicht bestehender Internetverbindung an einem geheimen Ort gespeichert und zu einem späteren Zeitpunkt übermittelt werden. Datenveränderungen durch ausführbare Inhalte können z.B. in der Infektion von Programmen mit einem **Computervirus** oder in der Veränderung von Datenbankeinträgen bestehen. Auch kann der Rechner des Steuerberaters zu Angriffen auf weitere Rechner genutzt werden.

Attributzertifikat

Das qualifizierte **Zertifikat** kann auf Verlangen des Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person, z.B. Geschäftsführer der Steuerberatungsgesellschaft XY, sowie berufsbezogene, z.B. Steuerberater, oder sonstige Angaben zu seiner Person enthalten (§ 5 Abs. 2 S. 1

SigG). Diese zusätzlichen Angaben (Attributzertifikat) werden bei geschäftlichen Vorgängen mitgesendet. Bei privater Nutzung kann das Attributzertifikat unterdrückt werden. Voraussetzung für die Aufnahme der o.g. Attribute in das Zertifikat ist, dass diese Angaben von der zuständigen Stelle gegenüber dem Zertifizierungsdiensteanbieter bestätigt werden.

Boot-Viren

Boot-Viren können sich im Bootsektor einer Diskette, im Bootsektor[3] der Festplatte oder im Partitionssektor[4] der Festplatte befinden und werden beim Starten der Diskette bzw. Festplatte aktiv. Besondere Probleme bestehen, wenn einzelne Ordner oder Dokumente auf der Festplatte durch ein Passwort oder eine Verschlüsselung geschützt sind. Für den Kaltstart mit der Systemdiskette zum Zwecke der Virenentfernung wird eine spezielle Systemdiskette mit der Schutzsoftware benötigt. Ist diese nicht vorhanden, muss die Virenbeseitigung u.U. im infizierten System erfolgen. Bei einem Befall der Festplatte durch einen Boot-Virus ist die gesamte Verwaltung der Festplatte durch das Betriebssystem betroffen. Änderungen in diesem Bereich können zum Verlust der gesamten gespeicherten Daten führen. Boot-Viren auf Disketten können durch eine Neu-Formatierung der befallenen Diskette beseitigt werden.

Browsereinstellungen

- Im Internet-Browser können verschiedene Sicherheitsstufen eingestellt werden. Grundsätzlich sollte eine möglichst hohe Sicherheitsstufe gewählt werden. So kann z.B. durch die Deaktivierung von **aktiven Inhalten** (ActiveX, Java, JavaScript) und Skript-Sprachen (z.B. Visual Basic Script, VBS) die Ausführung von aktiven Inhalten verhindert werden. Wird der Browser auf die höchste Sicherheitsstufe eingestellt, ist jedoch eine uneingeschränkte Internetnutzung nicht mehr möglich: Bei der Deaktivierung von JavaScript können z.B. verschiedene Websites nicht bzw. nicht vollständig angezeigt werden; so wird z.B. das Home-Banking nicht mehr unterstützt. Aufgrund der Funktionseinschränkungen empfiehlt sich die Installation einer **Firewall** sowie der Einsatz eines aktuellen Virenschutzprogramms anstelle der Einstellung des Browsers auf die höchste Sicherheitsstufe. Zusätzlich kann auch angedacht werden, beim Internet-Browser grundsätzlich die höchste Sicherheitsstufe einzustellen und die Rechner einiger für die Gefahren des Internet besonders sensibilisierter Mitarbeiter hiervon auszunehmen.
- Die gängigen Browser erlauben ein automatisches Update ohne Zutun des Benutzers aus dem Internet. Es kann jedoch nicht davon ausgegangen werden, dass die neue Version fehlerfrei ist. Darüber hinaus können die Konfigurationen, die der Anwender ausgewählt hat, überschrieben werden. Bei einem Update über das Internet besteht zudem die Gefahr, dass ein Rechner die Identität des Update-Servers vortäuscht, und auf diesem Weg einen böswilligen Pro-

[3] Sektor der Festplatte, in den beim Starten des Rechners das Betriebssystem (z.B. Windows, DOS) mit Hilfe des in diesem Sektor befindlichen Ladeprogramms geladen wird.
[4] Sektor der Festplatte, der eine Tabelle mit der logischen Organisation der Festplatte sowie ein Programm zur Auswertung der Tabelle enthält.

grammcode in das eigene DV-System einschleust. Es empfiehlt sich daher, dass automatische Update des Browsers abzustellen.

- Eine Internetseite, wie z.B. das Eingabeformular einer Bank für den Zutritt zum Homebanking, kann von einem Unberechtigten nur vorgegaukelt werden, um die Zugangsdaten des Nutzers auszuspähen. Seriöse Anbieter, wie z.B. Banken, **sichern** ihre Internetseiten mittels Zertifikaten ab, um zu verhindern, dass Unberechtigte ihre Internetseiten dem Nutzer vortäuschen. Der Internet-Browser kann so eingestellt werden, dass er die Echtheit von Zertifikaten stets überprüft, vor ungültigen Site-Zertifikaten warnt, den Wechsel zwischen dem sicheren und dem nicht sicheren Modus anzeigt und vor der Umlenkung von Formulardaten warnt.
- Um den Besuch von bestimmten Websites (z.B. Gewalt oder Sex) auszuschließen, kann durch eine entsprechende Einstellung des Internet-Browsers ein Filter zur Kontrolle der Internetinhalte aktiviert werden (beim Internet-Explorer unter Extras → Internetoptionen → Inhalt → Inhaltsratgeber).
- **Checkliste für einige wichtige Browsereinstellungen:**
  - Hohe Sicherheitsstufe auswählen
  - „**Proxyserver** verwenden“ kann eingestellt werden, „Proxyserver für lokale Adressen umgehen“ einstellen
  - ActiveX-Steuerelemente wegen der hohen Sicherheitsrisiken deaktivieren bzw. nur nach Eingabeaufforderung ausführen
  - Scripting deaktivieren bzw. für einzelne, für die Gefahren von ausführbaren Inhalten sensibilisierte Mitarbeiter aktivieren
  - Für den Aufruf von externen Programmen zur Darstellung von Dateien „Eingabeaufforderung“ einstellen
  - Automatisches Starten von heruntergeladenen Programmen abstellen
  - Warnmeldungen einschalten
  - Automatisches Update des Browsers abstellen
  - „bei ungültigen Zertifikaten warnen“, „bei Wechsel zwischen sicherem und nicht sicherem Modus warnen“, „Warnen falls Formulardaten umgelenkt werden“ aktivieren

Computerviren

Computerviren werden über Disketten, selbst gebrannte CD-ROMs, per E-Mail oder durch das Herunterladen infizierter Dateien und Programme übertragen. Die Betroffenen wissen häufig nicht, dass sie infizierte Programme und Dateien weiterreichen. Ein Virus ist eine nicht selbstständige Programmroutine; d.h. derartige Viren werden erst beim Start des Rechners oder bestimmter Programme ausgeführt. Ein Computervirus reproduziert sich selbst und nimmt dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vor.

(Einfache) elektronische Signatur

Die (einfache) elektronische Signatur gem. § 2 Nr. 1 SigG unterliegt keinen besonderen Regulierungen. Sie kann z.B. mit Hilfe des weitverbreiteten „Pretty Good Privacy"-Verfahrens (PGP) erzeugt werden. Es handelt sich hierbei um eine Software, die der Nutzer im Internet herunterladen und mit deren Hilfe er ein Schlüsselpaar generieren kann. Mit dem privaten, geheim zu haltenden Schlüssel signiert der Nutzer ein Dokument. Den öffentlichen Schlüssel gibt der Nutzer z.B. auf seiner Homepage bekannt oder hängt ihn an eine E-Mail an. Mit Hilfe des öffentlichen Schlüssels kann der Empfänger prüfen, ob die übermittelten Daten vollständig und unverfälscht sind. Nicht festgestellt werden kann jedoch, ob die Signatur von dem angegebenen Absender oder von einer fiktiven Person, die unter dem Namen des Absenders auftritt, stammt. Sofern sich zwei Personen kennen, kann dieses Problem ausgeräumt werden, indem sie sich ihre öffentlichen Schlüssel gegenseitig übergeben.

E-Mail-Attachments

Beim Empfang von E-Mails ist das sofortige Öffnen von Attachments (den Anlagen) ein Sicherheitsrisiko. Die Attachments sollten daher vor dem Öffnen auf **Computerviren**, **Trojanische Pferde** etc. untersucht werden. Die Einstellungen des E-Mail-Programms sollten so gewählt werden, dass die Anlagen von E-Mails nicht automatisch geöffnet werden. Wird z.B. das E-Mail-Programm Outlook verwendet, kann durch die Auswahl des hohen Sicherheitsgrades (unter Extras → Optionen → Sicherheit → Anlagensicherheit) das automatische Starten einer Anwendung abgestellt werden.

File-Viren

File-Viren hängen sich an eine Programmdatei an und werden beim Start des betroffenen Programms ausgeführt. Viele Anti-Viren-Produkte können File-Viren entfernen; bei einigen File-Viren gelingt die Beseitigung jedoch nicht. Das Löschen der betroffenen Programmdatei muss durch „Überschreiben" erfolgen, da bei einer Verschiebung in den sog. Papierkorb eine Wiederherstellung möglich ist. Einige Anti-Viren-Produkte verfügen über eine „Löschfunktion", die die befallene Programmdatei durch Überschreiben löscht. Weiter empfiehlt es sich, das gesamte betroffene Programm zu löschen und neu zu installieren.

Fortgeschrittene elektronische Signatur

Genauso wie die (einfache) elektronische Signatur unterliegt auch die fortgeschrittene Signatur gem. § 2 Nr. 2 SigG keinen besonderen Regulierungen und kann mit Hilfe des o.g. „Pretty Good Privacy"-Verfahrens (PGP) erzeugt werden. Hinsichtlich der Identität des Absenders ergeben sich die gleichen Probleme wie bei der **(einfachen) elektronischen Signatur**. Fortgeschrittene Signaturen werden auch von den Zertifizierungsdiensteanbietern, wie den Steuerberaterkammern, angeboten.

Hacker

Hacker können die Zugangssperren zum eigenen DV-System überwinden und dort Veränderungen an den Daten vornehmen.

Hardwareschutz

Computerviren sind Software und können daher durch Hardware geschützte Datenträger nicht beeinflussen. Wird der Schreibschutz durch Betätigen des Schiebers bzw. durch Zukleben der Kerbe an der Diskette gesetzt, kann bei einwandfreiem Diskettenlaufwerk für die schreibgeschützte Diskette eine Infektion ausgeschlossen werden.

Homepage

a) Beispiele für zulässige Inhalte und Gestaltungen einer Homepage:

- Sachlich zutreffende und objektiv nachprüfbare Informationen über die berufliche Tätigkeit
- Verwendung von Logos oder Slogans, sofern diese nicht reklamehaft gestaltet sind
- Angabe der Namen, Berufsbezeichnungen, berufsbezogenen Erfahrungen und Lebensläufe des Inhabers der Steuerberaterpraxis sowie seiner Partner
- Angabe von berufsbezogenen Spezialkenntnissen, sofern die Darstellung nicht reklamehaft ist
- Hinweis auf die Praxisgröße oder Organisation sowie auf nationale oder internationale Niederlassungen oder Kooperationen
- Hinweis auf die Branchen oder Größenordnungen (Klein- oder Großbetriebe) der betreuten Mandanten
- Hinweis auf Zertifikate im Sinne des § 12 BOStB
- Angabe von berufsbezogenen Mitgliedschaften in Kammern und Verbänden
- Informationen in Bildform, z.B. Photo des Inhabers der Steuerberaterpraxis oder der Büroräume, Lageplan der Steuerberaterpraxis. Die Einstellung von Photos der Mitarbeiter ist nur mit deren ausdrücklichem Einverständnis möglich.
- Allgemeine steuerliche Hinweise oder aktuelle berufsbezogene Informationen
- Mandanteninformationen ausschließlich im geschützten Bereich
- Angaben zu berufsbezogenen Veröffentlichungen (z.B. Bücher, Aufsätze) oder Reden
- Veröffentlichung von Stellenanzeigen
- Angabe von Sprechzeiten
- Einrichtung einer Mailbox, z.B. für Nachrichten oder Terminvereinbarungen
- Hinweis auf Kultursponsoring der Steuerberaterpraxis
- Der Inhalt und die Gestaltung der Homepage dürfen nicht auf die Erteilung eines Auftrags im Einzelfall ausgerichtet sein.

- Ausstattung der Homepage mit Metatags[5], sofern diese keinen Verstoß gegen das Berufsrecht (z.B. unzulässige Werbung) oder andere Rechtsvorschriften (z.B. Verstoß gegen das Rechtsberatungsgesetz) darstellen
- Verlinkung auf andere Seiten im Internet, die im direkten Zusammenhang mit der Tätigkeit des Steuerberaters stehen
- Online-Vollmacht, sofern diese durch eine qualifizierte digitale Signatur erteilt wurde

b) Beispiele für unzulässige Inhalte und Gestaltungen einer Homepage:

- Nicht berufsbezogene Informationen
- Darstellungen, die auf die Erteilung eines Auftrags im Einzelfall gerichtet sind
- Hinweis auf die frühere Beamteneigenschaft des Inhabers der Steuerberaterpraxis oder seiner Partner
- Angabe von nicht berufsbezogenen Mitgliedschaften in Kammern und Verbänden
- Gebührenunterbietung
- Irreführende Angaben im Sinne des § 3 UWG
- Der Form und dem Inhalt nach reklamehafte Darstellungen
- Einrichtung eines Gästebuchs
- Veranstaltung von Gewinnspielen
- Werbung für den Verkauf von Gegenständen
- Die Veröffentlichung von ganzen Linklisten kann als unerlaubte Werbung oder als unerlaubtes gewerbliches Auftreten gesehen werden.
- Verlinkung auf gewerbliche Seiten im Internet

Interoperabilität

Mit der Spezifikation ISIS-MTT[6] V.1.0 liegt seit Oktober 2001 die weltweit erste Interoperabilitätsspezifikation für elektronische Signaturen und das E-Mail-Austauschformat vor. D.h. dieser Standard soll über geschaffene Schnittstellen und sonstige Spezifikationen das Überprüfen von Signaturen sowie den Austausch von (verschlüsselten) E-Mails ermöglichen, unabhängig davon welches Trustcenter der Signaturkarteninhaber gewählt hat. Die in Deutschland ansässigen **akkreditierten Zertifizierungsdiensteanbieter**, zu denen auch die Steuerberaterkammern zählen, haben ihre Technologie an der Spezifikation ISIS-MTT ausgerichtet: Hierzu zählen die Trustcenter-, die Smartcard-, die Software- und die Zertifikatsinteroperabilität. Weitere Informationen befinden sich auf der Homepage des T7e.V. (www.t7-isis.de), in dem alle deutschen akkreditierten Zertifizierungsdiensteanbieter zusammengeschlossen sind. Da die notwendige Infrastruktur im europäischen Ausland bislang noch nicht aufgebaut ist, d.h. dort akkreditierte Zertifizierungsdiensteanbieter bis auf wenige Ausnahmen fehlen, sind europäische Anbieter in dem T7e.V. unterrepräsentiert.

[5] Metatags sind Suchbegriffe, bei deren Eingabe durch einen Nutzer eine Suchmaschine diejenigen Homepages anzeigt, die mit dem angegebenen Metatag ausgestattet sind.

[6] ISIS/MTT = Industry Signature Interoperability Specification MailTrusT

Firewall

Die Firewall ist kein Virenschutzprogramm, sondern sie entscheidet darüber, welche Daten oder Dateien von außen nach innen gelangen dürfen. So kann z.B. mittels einer Firewall festgelegt werden, dass E-Mails mit Attachments, die **ausführbare Programme** (*.exe) enthalten, entweder gar nicht oder nur in Verbindung mit einer Warnung in das Netz der Steuerberaterpraxis gelangen. Das Firewallsystem schützt das DV-System vor Angriffen von außen. Durch **aktive Inhalte** können jedoch Angriffe auch von innen gestartet werden, indem z.B. bei der Nutzung des Internet versehentlich ein Programm gestartet wird. Um diese Gefahr zu vermindern, sind bestimmte **Browsereinstellungen** und eine Sensibilisierung der Benutzer notwendig.

Makro-Viren

Makro-Viren befinden sich als Makros innerhalb von Office- oder anderen Dateien, also z.B. in Word-Dateien, und werden beim Start des entsprechenden Programms, z.B. Word, ausgeführt. Makro-Viren können mit Hilfe der meisten Anti-Viren-Produkte entfernt werden.

Makrovirenschutz

Sofern nicht ständig mit makrobehafteten Dateien gearbeitet werden muss, sollte der Makrovirenschutz von Anwendungsprogrammen (z.B. WinWord, Excel, Powerpoint) aktiviert und die Warnmeldungen beachtet werden. Makroviren hängen sich an Office-Dokumente an und kommen beim Start des entsprechenden Programms zur Ausführung.

Proxyserver

Jede Website, die einmal von einem Mitarbeiter aufgerufen wurde, wird im Proxyserver gespeichert. Bei nachfolgenden Aufrufen dieser Seite durch die Mitarbeiter wird diese Seite dann automatisch vom Proxyserver abgerufen und nicht von der ursprüngliche eingegebenen Adresse, z.B. in den USA. Ist der Proxyserver voll, werden die zuerst gespeicherten Seiten gelöscht und durch neue ersetzt. Richten sich die Kosten der Internetnutzung nach dem Datenvolumen, kann dies zu Einsparungen führen. Nachteil dieser Methode ist, dass die im Proxyserver gespeicherte Website bei einem späteren Aufruf durch andere Mitarbeiter bereits veraltet sein kann.

Prüfsummenprogramme

Virenschutzprogramme können durch sog. Prüfsummenprogramme ergänzt werden. Prüfsummenprogramme können die Integrität von Programmen feststellen, indem sie bei jedem Einschalten des Rechners die Größe der Programme erneut berechnen und mit der gespeicherten Größe vergleichen. Werden Abweichungen festgestellt, wird davon ausgegangen, dass diese Differenzen auf Viren zu-

rückzuführen sind, und das betreffende Programm wird nicht ausgeführt. So können mit Hilfe von Prüfsummenprogrammen auch noch nicht bekannte Viren erkannt werden.

Pseudonymisierung

Durch die in § 5 Abs. 3 SigG vorgesehene Möglichkeit der Pseudonymisierung des Signaturschlüsselinhabers sind beliebige organisatorische Details abbildbar: So kann z.B. die natürliche Person, Frau Müller, die in der Steuerberatungsgesellschaft XY als Sekretärin für den Steuerberater Schulz arbeitet, das Pseudonym „Steuerberatungsgesellschaft XY, Sekretariat von StB Schulz“ erhalten. Das Pseudonym ist als solches um den Kennzeichner „:PN“ zu ergänzen. D.h. im Zertifikat wird die Bezeichnung „Steuerberatungsgesellschaft XY, Sekretariat von StB Schulz:PN“ als Name des Signaturschlüsselinhabers verwendet. Mit Hilfe der Pseudonymisierung kann auch eine Poststellen-Signaturkarte erstellt werden. Die Möglichkeit der Vergabe eines Attributzertifikats wird durch den Ersatz des Namens durch ein Pseudonym nicht berührt. Darüber hinaus ermöglichen Pseudonyme beispielsweise, faktisch anonym im Internet einzukaufen und das Erstellen von Benutzerprofilen zu verbzw. zumindest zu behindern. Inwieweit der Gesetzgeber die Gleichwertigkeit der eigenhändigen Unterschrift mit der pseudonymisierten qualifizierten digitalen Signatur anerkennt, ist noch umstritten.

Qualifizierte elektronische Signatur

Die qualifizierte elektronische Signatur gem. § 2 Nr. 3 SigG ersetzt im elektronischen Rechts- und Geschäftsverkehr die eigenhändige Unterschrift und ist als Beweismittel vor Gericht zugelassen. Die Signaturschlüssel werden von einem Zertifizierungsdiensteanbieter (Trustcenter) erzeugt. Der Inhaber der elektronischen Signatur wird anhand seiner Ausweispapiere bei Beantragung der Signaturkarte identifiziert. Der geheime private Signaturschlüssel muss auf einem sicheren Hardware-Token (z.B. Smartcard) liegen. Dadurch wird gewährleistet, dass auch für den Inhaber der Signaturkarte der private Schlüssel unauslesbar ist und dieser daher seine Signatur nur schwerlich abstreiten kann. Mit dem privaten Schlüssel signiert der Nutzer ein Dokument. Den öffentlichen Schlüssel gibt der Nutzer z.B. auf seiner Homepage bekannt oder hängt ihn an eine E-Mail an. Mit Hilfe des öffentlichen Schlüssels kann der Empfänger nun feststellen, ob das Dokument tatsächlich von dem ausgewiesenen Absender stammt (dies wird durch die o.g. Identifizierung anhand der Ausweispapiere sichergestellt) und ob es unverändert ist (wie bei der einfachen und der fortgeschrittenen elektronischen Signatur). Schwachstellen dieses Systems sind, dass der vorgelegte Personalausweis gefälscht sein könnte oder die Smartcard im Lesegerät vergessen und die PIN ausgespäht wurde, so dass ein Unberechtigter die Signatur des Inhabers benutzen kann.

Qualifizierte elektronische Signatur mit Anbieterakkreditierung

Zertifizierungsdiensteanbieter können bei der Regulierungsbehörde für Post und Telekommunikation (RegTP) einen Antrag auf Akkreditierung stellen. Die Akkreditierung ist ein Gütezeichen, das die

RegTP dem Zertifizierungsdiensteanbieter ausstellt, wenn eine umfassende Prüfung der verwendeten technischen Komponenten und des Sicherheitskonzeptes zu einem positiven Ergebnis geführt hat. Die auf einem qualifizierten Zertifikat beruhende qualifizierte elektronische Signatur, ausgestellt durch einen Zertifizierungsdiensteanbieter mit Anbieterakkreditierung, wird auch qualifizierte elektronische Signatur mit Anbieterakkreditierung genannt und entspricht der höchsten Sicherheitsstufe bei den digitalen Signaturen.

Richtlinien zur Nutzung der betrieblichen EDV

- Verpflichtung des Personals zur Einhaltung der Zugriffskontrollen (d.h. z.B. keine Weitergabe von Passworten)
- Verbot von Downloads unbekannter oder unsicherer Programmanbieter
- Verbot der Verbindung privater Hard- und Software mit den Geräten der Praxis
- Bestellungen von z.B. Büromaterial bei Online-Shops nur für zuvor ausgewählte vertrauenswürdige Adressen zulassen. Die ausgewählten Online-Shops sollten insbesondere über einen geschützten Bereich zur Übermittlung von Zahlungs- und Kundendaten verfügen.
- Regelung hinsichtlich zulässiger privater Internetnutzung (Dauer und Art der Dienste), z.B. keine Gewinnspiele oder Besuch von Erotikseiten. Der Besuch bestimmter Web-Sites kann auch durch Filterprogramme verhindert werden (siehe Browsereinstellungen).

  ACHTUNG: Private E-Mails unterliegen dem Fernmeldegeheimnis und dürfen vom Arbeitgeber nicht eingesehen werden!

Sichere Signaturerstellungseinheit

Die qualifizierte elektronische Signatur muss mit einer sicheren Signaturerstellungseinheit erzeugt werden; hierfür trägt der Zertifizierungsdiensteanbieter Sorge.

Sicherheitsregeln

- Grundsätzlich sollte der Steuerberater täglich eine Datensicherung vornehmen, um einer möglichen Datenzerstörung oder einem Verlust vorzubeugen. Ein solches Vorgehen stellt sicher, dass bei einem Virenbefall höchstens die Arbeit eines Tages verloren gehen kann.
- Verpflichtung des Personals zur Einhaltung von Sicherheitsregeln und Festlegung der persönlichen Konsequenzen bei Zuwiderhandlung
- Regelung hinsichtlich der Gesamtverantwortung für den Betrieb und die Sicherheit des Netzes der Steuerberaterpraxis
- Einrichten von Zugriffskontrollen, z.B. über Passworte
- Zuordnung von Rechten hinsichtlich der Internetnutzung (Wer darf E-Mails versenden/empfangen, im Netz recherchieren, Programme aus dem Netz herunterladen etc.)
- E-Mail-Empfang:

- Offensichtlich nicht sinnvolle E-Mails von unbekannten Absendern sollten sofort ungeöffnet gelöscht werden.
- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sollte geprüft werden, ob die Nachricht inhaltlich und sprachlich zum Absender passt (z.B. englischsprachige Nachricht von deutschem Mandanten, fehlender Bezug zur Geschäftsbeziehung) und ob die Anlage (Attachment) auch erwartet wurde.
- Treffen mehrere E-Mails mit gleichlautendem Betreff ein, ist besondere Achtsamkeit geboten.
- E-Mails von unbekannten Absendern, die zwar nicht offenkundig sinnlos, aber auch nicht mit einer (qualifizierten) elektronischen Signatur versehen sind, sollten mit Vorsicht behandelt werden.
- Automatische Empfangsbestätigungen sollten unterlassen werden, sofern sie nicht verlangt oder im Einzelfall mit dem Mandanten vereinbart wurden.
- **E-Mail-Attachments** sollten nur, wenn sie von einem vertrauenswürdigen Absender stammen, und erst nach einer vorherigen Untersuchung auf Viren, **Trojanische Pferde** etc. geöffnet werden.
- Die Einstellung des E-Mail-Programms sollte so gewählt werden, dass das automatische Starten einer Anwendung, z.B. von **ausführbaren Programmen** (*.com, *.exe), Skriptsprachen (*vbs, *.bat), Office-Dateien (*.doc, *.xls, *.ppt) oder Bildschirmschonern (*.scr) abgestellt ist. Achtung: Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten!

- E-Mail-Versand:
  - Es sollten nur solche Daten unverschlüsselt per E-Mail verschickt werden, die von jedem gelesen und für beliebige Zwecke verwendet werden können.
  - Vertrauliche Nachrichten und Anlagen sollten nur verschlüsselt per E-Mail versandt werden.
  - Anlagen zu E-Mails (attachements) sollten in allgemein üblichen, möglichst kompatiblen, sicheren und sparsamen Formaten versandt werden.
  - Der Versand von **ausführbaren Programmen** (*.com, *.exe), Skriptsprachen (*vbs, *.bat), Office-Dateien (*.doc, *.xls, *.ppt) oder Bildschirmschonern (*.scr) sollte vermieden oder vorher mit dem Empfänger telefonisch abgestimmt werden. Durch eine Benachrichtigung des Empfängers kann dieser relativ sicher sein, dass die Datei vom angegebenen Absender geschickt und nicht von einem Virus verbreitet wird.
  - E-Mails sollten - wegen der Gefahr von aktiven Inhalten mit Schadensfunktion - auch nicht im HTML-Format versandt werden.

- Aufforderungen zur Weiterleitung einer E-Mail mit Viruswarnung, Anhängen etc. an Geschäftspartner, Freunde, Bekannte oder Kollegen sollten auf gar keinen Fall befolgt werden.
- Sofern eine elektronische Signatur vom Empfänger (z.B. § 77a FGO oder individuelle Vereinbarungen mit den Mandanten) gefordert oder durch das Berufsrecht (z.B. § 9 Abs. 1 StBGebV, siehe auch § 14 Abs. 4 UStG) vorgeschrieben ist, ist die E-Mail mit dem jeweils verlangten Typ von elektronischer Signatur zu unterzeichnen. Ist eine elektronische Signatur nicht vorgeschrieben, ist das Erfordernis einer elektronischen Signatur sowie die Auswahl des geeigneten Typs von Signatur im Einzelfall zu prüfen.
- Gelegentlich sollte geprüft werden, ob im Postausgangskorb E-Mails liegen, die nicht vom Nutzer verfasst oder dort eingestellt wurden.

- Downloads aus dem Internet: Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für **Computerviren**, **Trojanische Pferde** und **ausführbare Inhalte** mit Schadensfunktion dar. Um nicht versehentlich ein Programm mit Schadensfunktion zu starten, sollten Fenster im Internet nie mit einem möglicherweise dort vorhandenen Buttom „Schließen“ geschlossen werden, da hier ein Programm mit Schadensfunktion hinterliegen könnte. Stattdessen sollte das im oberen rechten Eck vorhandene Kreuzchen des Softwareherstellers für das Schließen eines Fensters verwendet werden.

  Beim Download sollten die folgenden Hinweise beachtet werden:
  - Programme sollten nur von vertrauenswürdigen Seiten, z.B. Originalseite des Herstellers, geladen werden.
  - Nach dem Download sollte die Angabe der Größe der Datei und - soweit angegeben - auch der Prüfsumme mit der vorgegebenen Größe und Prüfsumme verglichen werden. Werden dabei Abweichungen festgestellt, kann davon ausgegangen werden, dass unzulässige Veränderungen, meist durch Viren, vorgenommen worden sind. Die Datei sollte daher sofort gelöscht werden.
  - Die heruntergeladenen Dateien sollten vor der Installation stets mit einem aktuellen Virenschutzprogramm überprüft werden.
  - Gepackte (komprimierte) Dateien sollten erst entpackt und auf Viren überprüft werden. Installierte Entpackungsprogramme sollten so eingestellt werden, dass die zu entpackenden Dateien nicht automatisch gestartet werden.
- Verhaltensregeln / Maßnahmenplan bei Verdacht auf Virenbefall, z.B.:
  - zügige Beendigung der Arbeit, Herunterfahren und Ausschalten des Rechners
  - Der Datenaustausch zwischen einzelnen Rechnern sollte rückverfolgt werden, um festzustellen, welche weiteren Rechner und Disketten möglicherweise infiziert sind. Die betroffenen Anwender (Mitarbeiter in der eigenen Steuerberaterpraxis, Mandanten, andere Geschäftspartner, Freunde oder Bekannte) sind sofort darüber zu unterrichten, dass ih-

nen u.U. infizierte Dateien oder Datenträger zugegangen sind, um die weitere Verbreitung des Virus zu begrenzen.

- Zur Vermeidung eines künftigen Virusbefalls ist es zweckmäßig, den Weg der Erstinfektion zu ermitteln.
- Nach der Virenentfernung ist besondere Vorsicht geboten beim Aufspielen von Datensicherungsdisketten, da diese u.U. auch von dem Virus befallen sind. Hier muss zunächst eine Virenprüfung und ggf. –beseitigung erfolgen.

Trojanische Pferde

Trojanische Pferde sind selbstständige Programme, die neben ihrer eigentlichen Funktion noch weitere Funktionen ausführen, von denen der Anwender jedoch nichts weiß und deren Ausführung er im Regelfall auch nicht bemerkt. Eine solche weitere Funktion kann z.B. die Protokollierung und Versendung des Benutzernamens und Kennwortes an sog. Interessenten sein. Mit Hilfe der Zugangsdaten können diese Interessenten dann den Rechner unberechtigt nutzen, z.B. Ausspionieren vertraulicher Daten oder Nutzung der Telekommunikationsanbindung auf Kosten des Betroffenen. Trojanische Pferde gelangen über aus dem Internet heruntergeladene Programme oder über Dateianhänge an E-Mails (z.B. *.exe-Dateien) in das eigene DV-System. Trojanische Pferde können sich nicht selbstständig verbreiten. D.h. in der Regel muss der Anwender aktiv werden und ein Programm aus dem Internet herunterladen oder eine *.exe-Datei, die als E-Mail-Anhang versandt wurde, starten.

Web-Cookies

Bei der Kommunikation über das Internet (per E-Mail oder durch die Eingabe von Daten auf Internetseiten) hinterlässt der Nutzer viele Spuren, die sich zweckwidrig, z.B. zur Erstellung von Benutzerprofilen, verwenden lassen. Mit Hilfe von sog. Web-Cookies (das sind kleine Datensätze) können Informationen über den Benutzer eines Web-Browsers gesammelt werden. Diese sind dann über den Web-Server wieder abrufbar. Danach können dann die Benutzerprofile angelegt werden. Das Übermitteln von nicht offenkundigen personenbezogenen Daten in Cookie-Dateien kann eine Straftat gem. § 44 BDSG darstellen. In der Regel wird der Nutzer jedoch gar nicht bemerken, dass Informationen über ihn gesammelt werden.

Zeitstempel

Mit Hilfe entsprechender Software drehen sich die Uhren auf Rechnern unter Umständen rückwärts und Verträge, Buchungen oder andere sensible Dokumente können rückdatiert werden. Die **qualifizierte elektronische Signatur** unter einem Dokument kann mit dem (qualifizierten) Zeitstempel des Zertifizierungsdiensteanbieters versehen werden. Die Zeitsignatur eines Trustcenters verknüpft bestimmte Daten mit der gesetzlich gültigen Zeit und bestätigt digital, dass diese Daten, wie z.B. die qualifizierte elektronische Signatur oder ein elektronisches Dokument, zu dem angegebenen Zeit-

punkt dem Trustcenter vorgelegen haben. D.h. anhand des Zeitstempels kann festgestellt werden, ob die qualifizierte elektronische Signatur und z.B. das Attribut „Steuerberater“ zum Zeitpunkt der Vertragsunterzeichnung oder der Unterzeichnung einer E-Mail gültig waren. Über die ausgegebenen Zeitstempel werden von den Zertifizierungsdiensteanbietern Protokolldateien angelegt, so dass eine nachträgliche Fälschung kaum möglich ist.

Zertifikat

Im Unterschied zur **fortgeschrittenen elektronischen Signatur** beruht die **qualifizierte elektronische Signatur** auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat, das von einem Zertifizierungsdiensteanbieter ausgestellt sein muss. Das Zertifikat, auch „qualifiziertes Zertifikat“ genannt, ist eine mit der elektronischen Signatur des Zertifizierungsdiensteanbieters versehene digitale Bescheinigung darüber, dass der öffentliche Signaturschlüssel einer bestimmten Person zugeordnet wurde und die Identität dieser Person bei Ausstellung des Zertifikats eindeutig (z.B. durch Vorlage eines gültigen Personalausweises) festgestellt wurde. Mit der digitalen Signatur übernimmt der Zertifizierungsdiensteanbieter eine Garantenfunktion für die Richtigkeit der Angaben in dem Zertifikat. Darüber hinaus ist der Zertifizierungsdiensteanbieter verpflichtet, das qualifizierte Zertifikat jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und - unter der Voraussetzung der Zustimmung des Signaturschlüssel-Inhabers - abrufbar zu halten. Da qualifizierte Zertifikate rechtlich der eigenhändigen Unterschrift gleichgestellt sind, kann der öffentliche Signaturschlüssel per Zertifikat nur einer natürlichen Person zugeordnet werden. Die Ausstellung eines öffentlichen Schlüssels auf eine juristische Person oder ein Unternehmen ist ausgeschlossen. Die Verbindung zu der juristischen Person, z.B. der Steuerberatungsgesellschaft XY, oder der Berufsbezeichnung, z.B. „Steuerberater“, kann über die **Pseudonymisierung** bzw. das **Attributzertifikat** hergestellt werden.