CB-BEITRAG

Dipl. Wirtschaftsinformatiker Rüdiger Giebichenstein und Dipl.-Kfm. Karsten Thomas

Referentenentwurf für ein Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen veröffentlicht

Dem Bestreben Steuerpflichtiger, durch legale oder illegale Maßnahmen die Steuerlast zu verkürzen, stehen Bemühungen der Finanzbehörden gegenüber, eine Steuerhinterziehung zu verhindern und aufzudecken. Die Verwendung elektronischer Kassensysteme erlaubt aufgrund der maschinellen Auswertbarkeit der gespeicherten Daten bspw. im Rahmen einer Betriebsprüfung grundsätzlich eine hohe Transparenz. Auf der anderen Seite sind bei diesen Systemen bisher Manipulationen möglich, die nur sehr schwer nachzuvollziehen sind. Am 18.3.2016 veröffentlichte das Bundesministerium der Finanzen (BMF) den Referentenentwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen sowie den Entwurf einer Technischen Verordnung zur Durchführung des Gesetzes. Damit soll die Unveränderbarkeit an digitalen Grundaufzeichnungen sichergestellt und die Manipulation erschwert werden.

I. Hintergrund

Bereits 2003 warnte der BGH vor drohenden Steuerausfällen durch die Manipulation an modernen Kassensystemen in Höhe mehrerer Milliarden Euro.[1] Anschließend entwickelten zwei Bund-Länder-Arbeitsgruppen ein Fachkonzept zur Lösung des Problems. Auf der Basis dieses Fachkonzeptes entwickelte die Physikalisch-Technische-Behörde (PTB) gemeinsam mit Partnern aus der Industrie eine technische Lösung im Rahmen des INSIKA-Projektes.[2] INSIKA steht für „INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme". Das INSIKA-Verfahren basiert auf digitalen Signaturen, die über eine Chipkarte erzeugt werden und ermöglicht es, an einer Registrierkasse erfasste und gespeicherte Daten so zu schützen, dass Manipulationen sicher erkannt werden können. Das System ist für Kassen und ähnliche Aufzeichnungsgeräte geeignet und wird seit einigen Jahren erfolgreich in Hamburger Taxen eingesetzt.

Eine Gesetzesinitiative im Jahr 2008 zur Einführung der für das System erforderlichen Rahmenbedingungen scheiterte allerdings u. a. an den Bedenken des damaligen Bundesministeriums für Wirtschaft und Energie (BMWi) – obwohl dieses das Projekt gefördert hatte, denn die PTB ist eine wissenschaftlich-technische Bundesoberbehörde im Geschäftsbereich des BMWi. Die damalige Bundesregierung verzichtete im Anschluss auf weitere Initiativen zur Lösung des Problems.[3]

In einem 2013 veröffentlichten Bericht bewertete auch die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) das Problem als zunehmend relevant und empfahl den Steuerverwaltungen, eine Strategie zur Bekämpfung der Umsatzverkürzung mittels elektronischer Kassensysteme zu entwickeln.[4] Nach einer Initiative des Nordrhein-Westfälischen Finanzministers *Norbert Walter-Borjans* und aufgrund eines Beschlusses der Finanzministerkonferenz im Mai 2014 wurde durch eine Arbeitsgruppe ein Maßnahmenpaket gegen den Betrug mit Kassensystemen erarbeitet, allerdings wurde dieser Ansatz aufgrund von Bedenken aus dem Bundesfinanzministerium (BMF) damals nicht weiter verfolgt. Eine branchenübergreifende verpflichtende Einführung des erprobten INSIKA-Konzeptes scheiterte am Widerstand der Wirtschaft, die nach einer Kosten-Nutzen-Abwägung eine zu hohe finanzielle Belastung für den Handel für die Umrüstung der Kassen sah.[5]

Mit dem nun erschienenen Referentenentwurf des Gesetzes zum Schutz vor Manipulation an digitalen Grundaufzeichnungen hat sich der Gesetzgeber nun offenbar endgültig gegen die INSIKA-Lösung entschieden und fordert stattdessen eine Zertifizierung von Kassensystemen. Damit kommt das BMF mit diesem Referentenentwurf nun auch der Forderung der Wirtschaftsverbände nach.

II. Konkretisierung der GoBD

Die in einem BMF-Schreiben vom 14.11.2014 veröffentlichten „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form

1 Vgl. Bundesrechnungshof – Bemerkungen 2003 zur Haushalts- und Wirtschaftsführung des Bundes, S. 197.
2 http://www.insika.de/.
3 Vgl. BT–Drs. 18/4439.
4 Vgl. OECD-Bericht 2013 – Umsatzverkürzung mittels elektronischer Kassensysteme: eine Bedrohung für die Steuereinnahmen.
5 Vgl. DIHK-Stellungnahme: Bekämpfung von Manipulationen digitaler Grundaufzeichnungen zum BMF vom 19.12.2014.

sowie zum Datenzugriff" (GoBD) bilden das Rahmenwerk des neuen Gesetzes. Durch dieses werden die abstrakt und teilweise offen formulierten Anforderungen an die IT-Systeme, zu denen die Registrierkassen als Vorsysteme zählen, konkretisiert.[6]

Der Steuerpflichtige ist gem. § 146 Abs. 1 S. 1 AO dafür verantwortlich, organisatorisch und technisch sicherzustellen, dass die elektronischen Buchungen und sonst erforderlichen elektronischen Aufzeichnungen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden. Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.[7] Veränderungen und Löschungen von elektronischen Buchungen oder Aufzeichnungen müssen daher so protokolliert werden, dass die beschriebenen Anforderungen weiterhin erfüllt werden können.[8]

Erfüllen die Erfassungen eine Belegfunktion, dann ist eine unprotokollierte Änderung nicht mehr zulässig – wobei die Belegfunktion Grundvoraussetzung für die Beweiskraft der Buchführung ist. Die Ordnungsvorschriften gelten bereits für die erste Erfassung der Geschäftsvorfälle. Die Datensätze müssen dann über alle nachfolgenden Prozesse, wie der Übergabe von Daten aus den Kassen- in die Buchhaltungssysteme, erhalten bzw. progressiv und retrograd nachvollziehbar bleiben.[9]

Somit stellt der nun vorgelegte Gesetzesentwurf eine Konkretisierung der GoBD in Bezug auf die Maßnahmen zum Schutz der Aufzeichnungen bei Kassensystemen dar.

III. Möglichkeiten der Manipulation

Als zentraler Erfassungspunkt aller Umsätze am „Point of sale" (POS) ist die Registrierkasse sicherlich der am besten geeignete Punkt, um Manipulationen der Umsätze vorzunehmen, ohne nachweisbare Spuren zu hinterlassen. Die bisher bekannt gewordenen Fälle zeigen, dass es sich bei der Manipulation nicht nur um eine theoretische Möglichkeit handelt, sondern dass von dieser auch reger Gebrauch gemacht wird.

Exkurs Registrierkasse

Registrierkassen wurden bereits im Jahr 1879 von dem Lokalbesitzer *James Ritty* in Dayton, Ohio, USA, erfunden. Der Kern seiner Erfindung war eine Bargeldschublade, die sich nur dann öffnen ließ, wenn ein Umsatz verbucht ist und das Bargeld eingenommen werden soll. Frühe Registrierkassen machten dabei ein typisches Klingelgeräusch. Hintergrund der Erfindung war die Vermeidung von Diebstahl durch das Verkaufspersonal.

Die elektronische Registrierkasse hat sich daraufhin zu einem auf den Verkauf von Waren oder Dienstleistungen spezialisierten Datenerfassungsgerät entwickelt. Sie kann automatisch elektronische Aufzeichnungen zur Dokumentation von Einzelumsätzen erstellen. Eine solche Registrierkasse kann mit einer oder mehreren Eingabestationen verbunden sein.

Prinzipiell kann zwischen offenen Systemen, bei der die Kasse an ein Computersystem angeschlossen wird, und geschlossenen oder auch proprietären Systemen, bei der Hard- und Software eine Einheit bilden, unterschieden werden.

Grundsätzlich lassen sich die Aufzeichnungen von elektronischen Kassensystemen durch die schlichte Nichterfassung von Umsätzen, nicht dokumentierte Stornierungen sowie eine gezielte Veränderung von erfassten Umsätzen manipulieren.

Der hier vorgestellte Referentenentwurf ist nicht geeignet, um eine Nichterfassung zu verhindern oder zu reduzieren. Dafür bedarf es, wie es z. B. in anderen europäischen Ländern bereits üblich ist, einer Registrierkassenpflicht sowie weiterer Maßnahmen wie z. B. der Pflicht zur Ausgabe des Kassenbons. Allerdings ist das Entdeckungsrisiko auch hierzulande relativ hoch, da durch die Betrachtung von Einkäufen und Lagerbeständen das Missverhältnis bei systematischem Nichterfassen von Umsätzen im Rahmen einer Betriebsprüfung auffällt. Gleiches gilt für undokumentierte Stornierungen von Umsätzen oder die Nutzung eines in den Kassensystemen verfügbaren Trainingsmodus, der so erfasste Umsätze nicht an die Buchhaltungssysteme weiterleitet.

Da elektronische Kassen i. d. R. auch über elektronische und überschreibbare Speicher verfügen, können einmal gebuchte Umsätze relativ einfach und ohne Spuren zu hinterlassen verändert werden, sobald eine Zugriffsmöglichkeit auf die Speicher besteht. Das Finanzministerium NRW demonstrierte auf einer Pressekonferenz eindrucksvoll, wie einfach ein Kassensystem manipuliert werden kann. Bisher bestand für die Anbieter von Kassensystemen kein Grund, den Zugriff auf den internen Speicher zu erschweren oder zu verhindern, da damit in die Entwicklung eines Features investiert werden müsste, dass bei der Vermarktung im Zweifel keinen Mehrwert bietet.

Es gibt Werkzeuge, die es erlauben, einzelne Aufzeichnungsvorgänge zu unterdrücken und sogar gezielt systematische Manipulationen an den aufgezeichneten Datensätzen vorzunehmen. Die Lösungen, die kriminelle Softwarehersteller anbieten, fallen unter die Kategorien „Zapper" und „Phantomware".

Exkurs Zapper und Phantomware

Der Begriff Zapper wurde erstmals von *Richard Thompson Ainsworth* verwendet.[10] Er beschreibt damit spezielle kommerziell verfügbare Programme, die dazu dienen, die einmal erfassten Umsätze weitgehend automatisch durch komplexe Manipulationen des Datenbestandes nach unten zu korrigieren. Dafür überschreiben sie die Datenbanken in den Kassensystemen mit den gewünschten Zahlen. Besonders ausgefeilte Versionen berücksichtigen dabei auch die Lagerbestände und passen diese entsprechend mit an. Je besser und intelligenter die zugrundeliegenden Algorithmen sind, umso schwieriger wird es für die Finanzämter, den Betrug aufzudecken. Teilweise waren in den öffentlich bekannt gewordenen Fällen sogar die Hersteller von Kassensystemen selbst auch gleichzeitig Anbieter solcher Software.

Die Software selbst kann sich dabei auf externen Datenträgern wie einem USB Stick befinden („Zapper") oder ist sehr gut in der Kassenanwendung bzw. deren Quellcode versteckt („Phantomware").

Da durch eine solche Software die Integrität von Datensätzen massiv verletzt wird, unterwandern diese Programme nicht nur die

6 Vgl. BMF, 14.11.2014 – IV A 4 – S 0316/13/10003, StB 2014, S. 430, Tz. 20 und 23.

7 Vgl. § 146 Abs. 4 AO.

8 Vgl. BMF, 14.11.2014 – IV A 4 – S 0316/13/10003, StB 2014, S. 430, (GoBD), Tz. 59.

9 Vgl. BMF, 14.11.2014 – IV A 4 – S 0316/13/10003, StB 2014, S. 430, (GoBD), Tz. 84.

10 Vgl. *Richard Ainsworth* – Zappers: Tax Fraud, Technology and Terrorist Funding, The Boston University School of Law Working Paper Series vom 20.2.2008.

steuerliche Gesetzgebung, sondern auch die allgemeine Sicherheit von IT-Systemen. Ein potentieller Steuerbetrüger begibt sich bei der Anwendung eines solchen Programms in die Abhängigkeit von Kriminellen, denen damit sowohl ein Erpressungspotential als auch ein Einfallstor in die Systeme des Unternehmens zur Verfügung stehen.

Da im Rahmen von steuerlichen Betriebs- und Jahresabschlussprüfungen zunehmend ausgereifte statistische Verfahren (z. B. Benford-Analysen oder Chi-Quadrat-Tests) eingesetzt werden, und da die Komplexität digitaler Kassen laufend zunimmt, wird es immer schwerer, vorgenommene Manipulationen zu verbergen.
Hinsichtlich der Aufdeckung von ausgefeilten Zappern stoßen die Betriebsprüfer allerdings an die Grenzen ihres Repertoires der einsetzbaren Methoden und sind zum Teil auf Whistleblower angewiesen, die konkrete Hinweise auf den Einsatz solcher Programme geben können. Eine flächendeckende Prüfung der Quellcodes der Programme auf den Kassensystemen durch die Finanzbehörden ist zum einen schon aus Kapazitätsgründen nicht zielführend, zum anderen wäre dies immer eine zeitpunktbezogene Betrachtung, von der nicht ohne weiteres auf einen Zeitraum geschlossen werden könnte.
Durch den vorliegenden Referentenentwurf soll nun ein System geschaffen werden, durch das die Integrität der aufgezeichneten Daten gestärkt wird. Somit soll vermieden werden, dass diese so einfach wie bisher manipuliert werden können.

IV. Schutz vor Manipulation

Für die Verhinderung einer Manipulation an digitalen Grundaufzeichnungen und damit die Gleichmäßigkeit der Besteuerung sieht der Referentenentwurf ein dreistufiges Maßnahmenkonzept vor:
1. Technische Sicherheitseinrichtung in einem elektronischen Aufzeichnungssystem
2. Einführung einer Kassen-Nachschau
3. Sanktionierung von Verstößen

1. Technische Sicherheitseinrichtung

Die Aufzeichnungen der Geschäftsvorfälle im Kassensystem unterliegen einer Einzelaufzeichnungspflicht und müssen vollständig, richtig, zeitgerecht, geordnet und unveränderbar aufgezeichnet werden, was inhaltlich bereits durch die GoBD vorgegeben ist.
Der nun geplante Schutz vor Manipulationen basiert im Wesentlichen primär auf einer im neuen § 146a AO definierten zu zertifizierenden technischen Sicherheitseinrichtung. Durch diese soll gewährleistet werden, dass Grundaufzeichnungen bereits unmittelbar bei der Erfassung vor Verlust und nicht nachvollziehbaren Änderungen geschützt werden. Auch bei der nachfolgenden Weiterverarbeitung sind diese Anforderungen an die Integrität und Authentizität der Daten durchgehend einzuhalten.
Da der Entwurf bisher technologieoffen formuliert ist, wird kein bestimmtes Verfahren (wie z. B. INSIKA) vorgeschrieben. Die Sicherheitseinrichtung soll aus einem Sicherheitsmodul, einem Speichermedium und einer digitalen Schnittstelle bestehen. Die konkreten technischen Anforderungen an das Sicherheitsmodul, das Speichermedium, die elektronische Archivierung und die digitale Schnittstelle sollen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Abstimmung mit dem BMF in Form von technischen Richtlinien und Schutzprofilen festgelegt und auf der Internetseite des BSI veröffentlicht werden.[11]

a) Protokollierung

Für jede Aufzeichnung eines Geschäftsvorfalls soll gemäß der technischen Verordnung des Referentenentwurfs nun von einem elektronischen Aufzeichnungssystem unmittelbar eine neue Transaktion gestartet werden (Einzelaufzeichnung). Dieser Vorgang dient auch dazu, alle zu erfassenden Daten in einem einheitlichen Format zusammenzuführen, weshalb die Inhalte der Aufzeichnungen konkret vorgegeben werden:
- der Zeitpunkt des Vorgangsbeginns,
- eine eindeutige und fortlaufende Transaktionsnummer (die so beschaffen sein muss, dass Lücken erkennbar sind),
- die Art des Vorgangs (z. B. Einnahme oder Stornierung),
- die Daten des Vorgangs (z. B. der Betrag, Umsatzsteuerschlüssel etc.),
- die Zahlungsart (z. B. bar, Girocard oder Kreditkarte),
- den Zeitpunkt der Vorgangsbeendigung oder des Vorgangsabbruchs sowie
- einen Prüfwert.

b) Sicherheitsmodul

Die genannten Zeitpunkte sowie der Prüfwert sollen durch das Sicherheitsmodul festgehalten bzw. berechnet werden. Für die Ermittlung des Prüfwerts kann bspw. ein Signaturverfahren eingesetzt werden. Auch wenn die Anforderungen für das Sicherheitsmodul noch nicht formuliert bzw. veröffentlicht sind, kann aus dem Kontext vermutet werden, dass es sich dabei wahrscheinlich um ein Hardwaremodul handeln wird, das auch eine Echtzeituhr enthalten muss.[12]

c) Digitale Schnittstelle

Bei der digitalen Schnittstelle handelt es sich um eine Datensatzbeschreibung, die dem standardisierten Datenabzug sowie der einheitlichen Strukturierung der protokollierten Daten unabhängig vom verwendeten Kassenprogram dienen soll. Außerdem sollen durch die Beschreibung der Schnittstelle Unklarheiten über die zu erfassenden Daten sowie Probleme bei der Verarbeitung der Datensätze von vornherein vermieden werden.

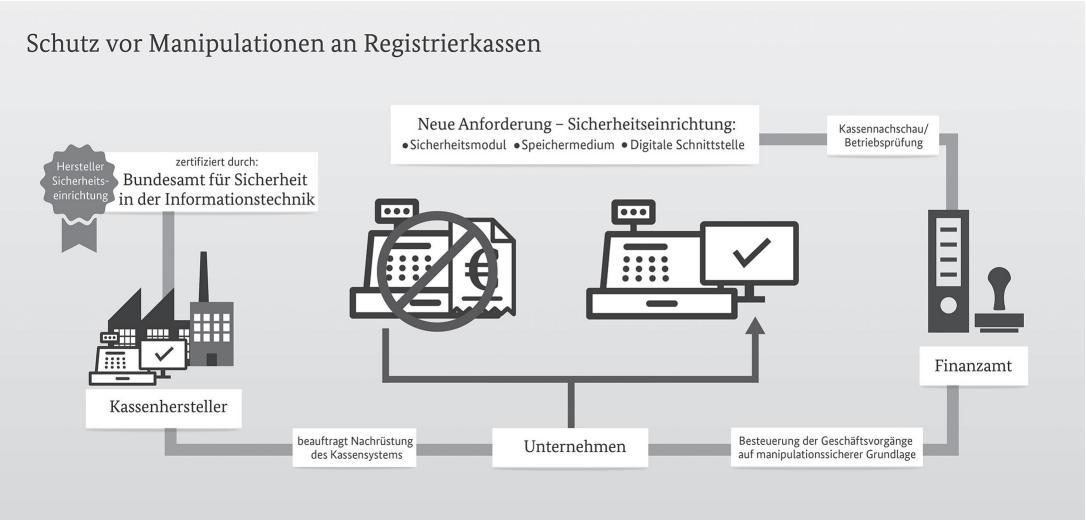
d) Speicherung der Grundaufzeichnungen

Ob für die Speicherung der Speicher des Kassensystems verwendet werden kann, oder es sich um einen Speicher innerhalb eines Hardwaremoduls handeln soll, ist offen gelassen. Dem Gesetz nach kann die digitale Schnittstelle dafür genutzt werden, um die Speicherung auf einem externen Medium oder in einem Archiv vorzunehmen. Es ist aber sicherzustellen, dass die gespeicherten Daten vollständig sind, dauerhaft gespeichert bleiben und bei Bedarf verfügbar und abrufbar sind.

11 Vgl. Referentenentwurf des BMF – Technische Verordnung zur Durchführung des Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 18.3.2016, § 1.

12 Vgl. ADM e. V. vom 31.3.2016 – Analyse des Referentenentwurfs eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 18.3.2016.

Abbildung: Konzept der Zertifizierung (Quelle: BMF)



e) Zertifizierung

Die in ein Kassensystem implementierte technische Sicherheitseinrichtung muss durch das BSI zertifiziert werden. Bei einer solchen Zertifizierung wird überprüft, ob die hier aufgeführten fachlichen Anforderungen und die vom BSI noch zu veröffentlichenden technischen Anforderungen durch die jeweilige Lösung eingehalten werden. So müssen alle Hersteller von Kassensystemen ihre eingesetzte Software vom BSI prüfen und freigeben lassen, bevor diese im Geschäftsbetrieb eingesetzt werden kann. Der für die Umrüstung der Kassensysteme vorgesehene Prozess ist in Abbildung 1 schematisch dargestellt.

Werden durch ein Update Programmänderungen im Bereich der Sicherheitseinrichtung vorgenommen, erlischt die bestehende Zertifizierung und muss neu beantragt werden. Wenn bekannt wird, dass eine bereits zertifizierte Kassensoftware nicht mehr den Anforderungen entspricht, z. B. bei Bekanntwerden ausnutzbarer Sicherheitslücken, erlischt die Zertifizierung.

Obwohl nur zertifizierte Registrierkassensysteme im Geschäftsbetrieb zulässig sein werden (offene Ladenkassen sind davon ausgenommen und können weiterhin verwendet werden), entfaltet ein solches Zertifikat gegenüber den Finanzbehörden analog zu anderen Softwarezertifikaten (wie bspw. nach IDW PS 880) keine Bindungswirkung.[13]

2. Kassennachschau

Eine Verpflichtung zum Einsatz zertifizierter Kassensysteme erscheint nur dann sinnvoll, wenn auch Mechanismen zur Überwachung der Einhaltung eingerichtet werden. Hierzu beabsichtigt der Gesetzesentwurf die Einführung einer sog. Kassen-Nachschau. Diese ist nicht gleichzusetzen mit einer Außenprüfung entsprechend § 193 AO, sondern stellt ein eigenständiges Verfahren dar.

Ein solches Werkzeug erhöht das Risiko der Entdeckung von Manipulationen deutlich. Der Prüfer ist berechtigt, ohne vorherige Ankündigung den ordnungsgemäßen Einsatz eines elektronischen Kassensystems zu überprüfen. Dafür kann u. a. die Übermittlung von Daten über die digitale Schnittstelle verlangt werden.[14] Auch eine Beobachtung der Kassiervorgänge in den Geschäftsräumen sowie die Möglichkeit von Testkäufen sind vorgesehen.

Sollten im Rahmen der entsprechenden Kassen-Nachschau Beanstandungen festgestellt werden, kann auch ohne vorherige Prüfungsanordnung zu einer Außenprüfung übergegangen werden.[15]

Werden die Bondaten im Rahmen der weiteren Verarbeitung an Dritte weitergegeben (Outsourcing), so sieht § 147 Abs. 6 S. 2 AO vor, dass der Finanzbehörde auch in diesem Fall Zugriff auf die Daten zu gewähren ist. Dies hat insbesondere bei Kassensystemen mit zentralen Servern und Prozessen, wie sie regelmäßig bei Filialisten eingesetzt werden, Relevanz.

3. Sanktionierung

Ohne entsprechende Sanktionierungsmöglichkeiten wären die vorgenannten Maßnahmen ein „stumpfes Schwert". Verstöße sollen – unabhängig von einem entstandenen steuerlichen Schaden – mit Geldbußen von bis zu 25 000 Euro geahndet werden.

Dies soll jedoch nicht nur den Steuerpflichtigen betreffen, der

- ungeeignete, nicht den Anforderungen des § 146a Abs. 1 AO entsprechende technische Systeme einsetzt oder
- keine bzw. eine fehlerhafte zertifizierte technische Sicherheitseinrichtung einsetzt,

sondern soll auch Dritte umfassen, die elektronische Aufzeichnungssysteme, technische Sicherheitseinrichtungen oder andere Softwaresysteme bewerben oder inverkehrbringen, die

- entweder nach Gesetz buchungs- oder aufzeichnungspflichtige Geschäftsvorfälle oder Betriebsvorgänge nicht oder in tatsächlicher Hinsicht unrichtig aufzeichnen oder verbuchen,
- oder die Möglichkeit eröffnen, nachträgliche Löschungen oder Veränderungen vorzunehmen.

Sowohl der Erwerb als auch das Bewerben sowie das Inverkehrbringen werden sanktioniert.

V. Erfüllungsaufwand

§ 1 der Technischen Verordnung zählt auf, welche Systeme unter dem Begriff des elektronischen Aufzeichnungssystems zu verstehen sind und damit über eine technische Sicherheitseinrichtung verfügen müssen. Hierzu zählen elektronische oder computergestützte

13 Vgl. BMF, 14.11.2014 – IV A 4 – S 0316/13/10003, StB 2014, S. 430, Tz. 181 (GoBD).
14 Vgl. § 146b Abs. 2 AO (Referentenentwurf vom 18.3.2016).
15 Vgl. § 146b Abs. 3 AO (Referentenentwurf vom 18.3.2016).

Kassensysteme oder Registrierkassen einschließlich Tablet-basierter Kassensysteme.
Da es bisher noch keine zertifizierten Registrierkassen gibt, bedeutet dies, dass jede in Deutschland im Einsatz befindliche Kasse mit einer neuen zertifizierten Software bestückt bzw. entsprechend aufgerüstet werden muss. Im Vergleich zur INSIKA-Lösung sind die Rahmenbedingungen so weit offen gehalten, dass es eventuell möglich sein wird, die Umsetzung der Anforderungen rein auf der Basis von Softwareanpassungen vorzunehmen, ohne zusätzliche Hardwaremodule anzuschaffen.
Sofern eine Aufrüstung nicht möglich ist, werden sich die Unternehmen neue Kassen anschaffen müssen. Davon werden wahrscheinlich hauptsächlich kleine und kleinste Unternehmen betroffen sein. Das BMF schätzt die Kosten dafür auf insgesamt 470 Mio. Euro.
Für Kleinstunternehmen und Einzelkaufleute könnte es der einfachste Weg sein, die bisherige – nicht zertifizierte – Registrierkasse gegen eine offene Ladenkasse auszutauschen, welche den vorgesehenen Gesetzesbestimmungen nicht unterliegt. Dies würde für den Steuerpflichtigen nicht nur die finanziell attraktivere Variante darstellen, sondern auch den Weg von Manipulationen zukünftig offenhalten – entgegen der Intention der Finanzverwaltung.
Kleine und mittlere Unternehmen mit mehreren Kassen, die auf elektronische Abrechnungs- und ggf. Warenwirtschaftsprozesse angewiesen sind, hätten einen hohen finanziellen Erstaufwand für die Anschaffung zertifizierter Registrierkassen oder die Umrüstung der bestehenden Kassen zu tragen, wenngleich diese Umstellung aus technischer Sicht durchaus realisierbar erscheint.
Problematisch sind die Vorgaben aus Sicht größerer Unternehmen zu beurteilen, die zentrale Kassensysteme einsetzen und über integrierte Prozesse von Kassen-, Warenwirtschafts- und Finanzbuchhaltungssystemen verfügen. Die erstmalige Aufrüstung der Kassen mit einem zertifizierten Sicherheitsmodul ist hierbei noch eine geringe Herausforderung. Aufwändiger ist es, die Vorgaben über den gesamten Prozess der Bondaten-Entsorgung von den Kassen in die nachgelagerten Systeme einzuhalten. Regelmäßig erfolgen Anpassungen der Softwaresysteme, die entsprechende Updates der Kassensoftware nach sich ziehen, um bspw. neue Funktionalitäten in der Kasse abzubilden (Handling von Preisaktionen, Gutscheinen, Kommissionsware wie Telefonguthabenkarten oder Bahntickets etc.). Es besteht eine hohe Wahrscheinlichkeit, dass diese Updates den zu zertifizierenden Kern der Kassensoftware betreffen und die Zertifizierung somit ungültig wird und wiederholt werden müsste – auf Dauer ein teures und aus Zeitgründen eher unpraktikables Vorgehen.
Selbstverständlich ist es auch in diesem Fall notwendig, sichere Prozesse hinsichtlich der Stammdatenversorgung an die Kassen sowie der Bondatenentsorgung aus den Kassen zu etablieren – dies fordern auch bisher schon die handels- und steuerrechtlichen Vorgaben, die in den GoBD konkretisiert wurden. Nicht zuletzt haben größere Unternehmen jedoch ohnehin ein internes Kontrollsystem zu etablieren, welches Manipulationen unwahrscheinlich werden lässt, da automatisierte und manuelle Kontrollen (Vier-Augen-Prinzip) präventiv und detektiv miteinander wirken und Eingriffe in die automatisierten Prozesse sehr erschweren.

VI. Kritische Würdigung und Fazit

Grundsätzlich sind eine Absicherung und die Schaffung von Kontrollmöglichkeiten bei Kassensystemen in mehrfacher Hinsicht zu begrüßen. Allerdings wird das vorgelegte Modell der Zertifizierung nicht allen Anforderungen gerecht. Für die Unternehmer bedeutet es einen hohen finanziellen Aufwand.
Zudem sind einige Fragestellungen bislang noch nicht hinreichend geklärt. So mussten bisher Softwarezertifikate (z. B. gemäß IDW PS 880) durch die Finanzverwaltung nicht anerkannt werden – was sich für Warenwirtschafts- und Finanzbuchhaltungssysteme auch nicht ändern wird –, und nun wird die Zertifizierung für Kassensysteme zur Pflicht. Es steht noch nicht fest, ob die Zertifizierung einmalig erfolgt oder regelmäßig zu wiederholen ist und wie in der Praxis eine Übereinstimmung der eingesetzten mit der zertifizierten Version des Sicherheitsmoduls überprüft werden wird.
Auch aus Sicht der Informationssicherheit wirft der Gesetzesentwurf Fragen auf. Kassensysteme sind mittlerweile nahtlos in die Unternehmensprozesse integriert und kommunizieren mit weiteren Peripheriegeräten, die hierfür auch über das Internet mit Dritten (z. B. Zahlungsdienstleistern) verbunden sind. Durch die Pflicht zur Zertifizierung werden die Kosten zum Patchen von Sicherheitslücken, die immer wieder auftreten können, deutlich ansteigen. Das könnte dazu führen, dass diese erst sehr spät oder überhaupt nicht geschlossen werden, um die Zertifizierung nicht erlöschen zu lassen – was die IT-Sicherheit der Kassensysteme und damit des gesamten Unternehmens beeinträchtigt.
Das Gesetz kommt wahrscheinlich einige Jahre zu spät. Seit der erstmaligen Erwähnung 2003 durch den BGH hat sich der Trend zur Digitalisierung deutlich verschärft und ist nicht mehr aufzuhalten. Das bedeutet, dass der manipulierbare Bargeld-Verkehr zugunsten von Kartenzahlungen und anderen neuartigen Zahlverfahren weiter abnimmt, die ohnehin weniger Anfällig für Manipulationen sind und einem deutlich höheren Entdeckungsrisiko unterliegen. Maßnahmen, die in erster Linie den Bargeldverkehr betreffen, verlieren mit fallender Bedeutung desselben an Wert, obwohl sie mit hohen Kosten verbunden sind.
Nach Inkrafttreten des Gesetzes soll es erstmalig für nach dem 31.12.2018 beginnende Wirtschaftsjahre anzuwenden sein: gut, dass bis dahin noch Zeit ist, diese Fragen zu klären.

AUTOREN

Rüdiger Giebichenstein, *Dipl.-Wirtschaftsinformatiker, ist als Partner bei der PwC AG Wirtschaftsprüfungsgesellschaft mit den Beratungsschwerpunkten Cyber Risk & Security, (IT-)Compliance und (IT-) Governance, (IT-)Risikomanagement und Datenschutz für Mandanten verschiedener Branchen tätig.*

Karsten Thomas, *Dipl. Kaufmann, CISA/CRISC, ist als Senior Manager/Prokurist bei der PwC AG Wirtschaftsprüfungsgesellschaft mit den Beratungsschwerpunkten Cyber Risk & Security, (IT-) Risikomanagement, (IT-) Governance, (IT-) Compliance, Datenschutz und Jahresabschlussprüfungen tätig.*