Von: DieterKoll VELODATA [mailto:Dieter.Koll@velodata.de]
Gesendet: Montag, 11. April 2016 22:00
An: Dr. Wolfgang Schäuble MdB <wolfgang.schaeuble@bundestag.de>
Betreff: Referentenentwurf vom 18. März 2016 des Bundesministeriums

Sehr geehrter Herr Dr. Schäuble,
der Referentenentwurf vom 18. März 2016 des Bundesministeriums der Finanzen zum Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen (Kasse in Handel und Handwerk) löst keine Probleme, sondern er schafft bei einer Umstetzung gravierende Ungerechtigkeiten.

Man bastelt am transatlantischen Freihandelsabkommen TTIP.
Doch eine in Österreich zugelassene Kasse soll nicht in Deutschland zugelassen werden
oder auch umgekehrt. Im Referentenentwurf werden die Kosten der Prüfung allein für Deutschland in Höhe von 75.000 € geschätzt.

Als Softwarehersteller aus dem Raum Aachen sind wir in der Fahrradbranche einer der Marktführer, doch für uns sind die Kosten zu hoch. Müssen wir uns in Zukunft auf das Erstellen des Belegs beschränken und die bisher integrierte Kassenfunktion ausbauen? Das wäre kontraproduktiv zur gewollten Steuergerechtigkeit.

Mangels Kassen- und Belegpflicht wie in einigen anderen europäischen Ländern wird das Ziel, mehr Steuergerechtigkeit, durch weniger „Schwarzumsatz“ voll verfehlt.
Es entstehen nur Kosten für Händler und Handwerker, die bereits eine Kasse einsetzen Die wirklich schwarzen Schafe lachen nur, setzen überhaupt keine Kasse ein oder buchen den Umsatz weiterhin nicht. Wo bleibt hier die Gleichheit vor dem Gesetz?

Viele deutsche Fachhändler haben nach dem BMF-Schreiben vom 26. November 2010 bereits eine Neuanschaffung oder Umrüstung für das Geschäftsjahr 2017 getätigt. Mit Sicherheit werden einige teure Neuanschaffungen, besonders in herkömmliche starre Registrierkassen, zum 1. Januar 2019 durch das BMF zu modernem Sperrmüll.
Wo bleibt hier der Vertrauensschutz?

Laut Referentenentwurf soll es sich um eine technologieoffene und herstellerunabhängige Lösung handeln. Das können wir aus fachlicher Sicht nicht bestätigen, bevorzugt werden große Unternehmen.

Bitte sorgen Sie mit dafür, dass der Referentenentwurf vom 18. März 2016 in der vorgelegten Fassung nicht zum Tragen kommt.

Mit freundlichen Grüßen
VELODATA GmbH
Dieter Koll

In der Anlage
Der bisher bekannte Referentenentwurf vom 18. März 2016
Unsere Stellungnahme zum Referentenentwurf
Die Stellungnahme des INSIKA – ADM e.V. zum Referentenentwurf,

VELODATA GmbH *- **Ihr zuverlässiger Softwarehersteller seit 1979***
Tannenbergstr. 45 52224 Stolberg-Zweifall Tel: 02402-90302-0 Fax: 02402-90302-25
www.velodata.de
HRB11548 Aachen // Geschäftsführer: Heike Hansen / Dieter Koll // UST-ID: DE121743075 // GLID: DE32ZZZ00000733586

VELODATA GmbH Tannenbergstr. 45 52224 Stolberg

Tel. 02402 903020 Mail: Dieter.Koll@velodata.de

Stellungnahme zum Referentenentwurf des Gesetzes zum Schutze von Manipulationen an digitalen Grundaufzeichnungen vom 18.3.2016 des BMF

Einleitung:

Die VELODATA GmbH entstand 1979 aus der Entwicklung einer Lager- und Bestandsverwaltung mit Belegerstellung und Kassenfunktion. Damit konnte die damals übliche Doppelerfassung von Beleg und Zahlbetrag abgeschafft werden. Die VELODATA war damit der erste Anbieter am deutschen Markt.

Wären die Vorschriften des Referentenentwurfs März 2016 bereits 1979 in Kraft getreten, hätte die VELODATA GmbH dieses Produkt nicht entwickeln können und niemals existiert.

Die im Referentenentwurf geschätzten Kosten der Zertifizierung mit r.d. 75.000 € gefährden die Existenz einer großen Zahl von mittelständischen Softwareherstellern in Deutschland. Die tatsächlichen Kosten von Abnahme und Entwicklung sehen wir eher beim doppelten bis dreifachen Betrag.

Der Referentenentwurf vom 18.3.2016 geht völlig an dem Ziel Steuergerechtigkeit vorbei und sieht für uns eher wie die Förderung der Interessen einiger weniger großen internationalen Kassenhersteller oder auch Handelsketten aus.

Dafür sprechen auch zahlreiche Textpassagen. Da begründet der Referentenentwurf das vorgeschlagene Konzept sei kostengünstiger als Insika: *Ein Sicherheitsmodul muss nur einmal zertifiziert werden und kann in einer Vielzahl von Kassen eingesetzt werden. Bei Systemkassen benötigt nicht jede einzelne Kasse ein Sicherheitsmodul, sondern es kann ein Sicherheitsmodul für sämtliche im System verbundene Kassen verwendet werden*

75.000 € für die Zertifizierung sind für EDEKA, DECATHLON oder ALDI erträglich. Für ein betrieblich angepasstes Kassen- und Fakturierungskonzept kleiner Händler ein utopisch hoher Kostenbetrag,

75.000 € durch11.000 Filialem macht 6,82 € pro Filiale.
75.000 € für einen Händler oder selbst 100 Händler sind kaum tragbar.

Beim mittelständischen Facheinzelhandel müssen die Kosten für ein betrieblich angepasstes Kassen- und Fakturierungskonzept oft auf wenige Kassen umgelegt werden.

Da der Referentenentwurf weder eine Kassen noch eine Belegpflicht vorsieht, steht der kleinere Einzelhändler und Handwerker vor folgenden Alternativen:

a) Anschaffung einer preiswerten aber gesetzeskonformen Registrierkasse, es werden keine Einzelpositionen mehr aufgeführt, „gebongt“ wird der reine Zahlbetrag, denn Belege sind nicht gefordert.
Seite 11 Referentenentwurf: Das INSIKA-Konzept ist kostenintensiver für die Wirtschaft als das Zertifizierungsverfahren. Denn die Belegausgabe ist kein zwingender Bestandteil des Konzepts.

b) Verzicht auf jegliche elektronische Kasse. Rechnungen per Fakturierung. Kassenaufzeichnung per Hand.
Einige Steuerberater verweisen Ihre Mandanten auf die unklaren Anforderungen bei der Kassenführung durch das BMF-Schreibens vom 26. November 2010 und die GoBD 2014 und halten eine manuelles Kassenbuch für sicherer. Wir haben im Kundenkreis paradoexerweise die Situation, dass, obwohl unser System alle Funktionen einer Kasse mit Kassenbericht hat, das Kassenbuch vollständig manuell handschriftlich geführt wird.

Der Referentenentwurf vom 18.3.2016 selbst hat keinerlei Aussagekraft für eine Aufwandschätzung oder Programmieranweisung bis auf eine nebulöse Prüfung durch das BSI nebst Kostenschätzung von 75.000,- € für diese Prüfung. Die Entwicklungs- und Dokumentationskosten werden ein Mehrfaches der Prüfungsgebühren betragen.

Handelt es sich bei dem aufgeführten Sicherheitsmodul um eine eigenständige Hardware? Wer soll diese Hardware zu welchem Preis liefern?

Auch die Aussagen zum geforderten Speichermedium deuten auf eine Hardware hin, ohne jeden weiteren technischen Hinweis.

Dann finden sich Aussagen zu einer Transaktionsnummer, die als Einmalpasswort dienen soll. Bitte Klarheit, wir verwenden seit Jahren eine eindeutige Belegnummer, man mag das Transaktionsnummer nennen oder eine zusätzliche Transaktionsnummer fordern. Oder soll an der Kasse ein Passwort eingegeben bzw. generiert werden?

Was ist der Zeitpunkt des Vorgangsbeginns und der Zeitpunkt der Vorgangsbeendigung bzw. Abbruchs? Wir kennen den Ablauf eines Werkstatt- und Fahrzeugverkaufs über Tage gar Wochen, was ist dann der Vorgangsbeginn?

Der Referentenentwurf ist inkonsequent und nicht hilfreich. Das INSIKA-Projekt wird schon wegen des Zwangs zum Belegdruck verworfen. Egal wie man zu INSIKA steht, hier gibt es im Gegensatz zum Referentenentwurf klare abschätzbare Programmiervorgaben zu erträglichen Kosten für kleinere Betriebe bzw. Branchen. Für die Kontrollfunktion bei INSIKA ist auch nicht zwingend ein 2D-Barcode notwendig.

Konsequent für eine Kontrolle im Sinne einer Steuergerechtigkeit wäre eine Verpflichtung bei Barzahlungen (auch im Handwerk) einen Beleg zu erstellen und dem Käufer auszuhändigen, wie dies von einigen EU-Ländern bereits praktiziert wird.

Ohne Verpflichtung zur Belegerstellung macht die Forderung, dass Kassen keine Änderung oder Unterdrückung von einmal vorgenommenen Buchungen durch den Benutzer zulassen dürfen, keinen Sinn.
Wer wirklich Steuern hinterziehen will, der tippt im kleinen Betrieb den Umsatz erst gar nicht in seine Kasse. Nur in ganz wenige Ausnahmefällen werden Umsätze zur Personalkontrolle erfasst und nachträglich manipuliert.

Das im Referentenentwurf vorgeschlagene Konzept fördert große Betriebe bei den Kassenherstellern und im Handel. Benachteiligt werden kleinere mittelständische deutsche Betriebe und Branchen.

Ein denkbarer Ausweg für kleinere Betriebe ist eine Trennung von Kasse und System zur Belegerstellung. Das branchenspezifische System erstellt lediglich den Beleg mit den Einzelpositionen. Dann wird lediglich der Endbetrag (wenn überhaupt gewünscht) an eine getrennte Kasse zwecks „kassieren“ übermittelt. Sicherlich nicht im Sinn der Steuerkontrolle aber logisch.

Wir benötigen eine europäische Regelung zu diesem Thema oder die Anerkennung von Standards anderer EU-Länder.

Nach Stand des Referentenentwurfs benötigen wir zum Beispiel im Fahrradbereich eine Kasse für Österreich und eine andere Kasse für Deutschland.

Dieter Koll
Geschäftsführender Gesellschafter der VELODATA GmbH

Dieter Koll
Geschäftsführender Gesellschafter der VELODATA GmbH
Jahrgang 1948 Kfz-Mechaniker-Meister 1970
Mehrere Jahre Inhaber eines Handwerks- und Handelsbetriebes

Gründung der VELODATA GmbH 1979 Software zur Abschaffung der damals üblichen Doppelerfassung von Rechnung und Zahlbetrag. Die VELODATA war damit vermutlich der erste Anbieter eines Mehrplatzsystems mit Bildschirmkasse am deutschen Markt.

Bei der ersten Softwaregeneration der VELODATA gab es bis etwa 1989 ein Korrekturprogramm für falsch erstellte Belege. Bei der Neuprogrammierung der nachfolgenden Softwaregeneration gibt es keine solche Möglichkeit mehr. Korrekturen werden nummeriert und im Kassenjournal dokumentiert. Manipulationen auf Dateiebene sind nahezu unmöglich und wären wenn bei einer Prüfung immer feststellbar.

Die Anforderungen bei der Kassenführung durch das BMF-Schreiben vom 26. November 2010 und die GoBD 2014 sind wegen widersprüchlicher Aussagen (gesicherte Datenhaltung, Original Daten, und dann einfache Datenformate) für mich wenig hilfreich.

Einige Händler, aber auch Hersteller, haben aufgrund des BMF-Schreibens aus 2010 mit Frist bis zum 31.12.2016 gerade erst in neue angepasste Systeme investiert. Die Übergangsfristen bis 31.12.2018 zu Regelungen, die momentan technisch überhaupt noch nicht klar sind, sind weder haltbar noch zumutbar.

Wenn HDE und DEHOGA von 1,38 Millionen Kassenplätze ausgehen, stelle ich die Zahlen in Frage, da maximal 10% unserer Kunden in einem der Verbände organisiert sind. (Wir sind Fördermitglied im VDZ>HDE sowie im Bundesinnungsverband.)

Der Ansatz zu einer Steuergerechtigkeit per undurchschaubarer Verordnungen bis in Details ist falsch. Der Gesetzgeber wird der Technik immer hinterherlaufen. Hier würden einfache Aussagen mit der Androhung von Gefängnisstrafen, auch für die Geschäftsführer von Kassen- und Softwareherstellern, bei illegalen Manipulationsmöglichkeiten abschrecken. Die Auswahl eines Sicherungssystems sollte freigestellt werden. Dabei ist der Ansatz INSIKA in jedem Fall klarer und und für mittlere und kleine Fachhändler kostengünstiger als die Vorschläge im Referentenentwurf. Auch die Österreich-Lösung sollte man wahlfrei zulassen.

Bei Betrieben, bei denen die Steuergerechtigkeit von der Bargelderfassung abhängt, kann nur eine Verpflichtung zur Belegausgabe und Belegerfassung vor absichtlicher Steuerhinterziehung abschrecken. Dazu gehört dann eine entsprechende Kontrolle per Stichprobe durch die Ämter.

Die verfassungsrechtlichen Bedenken hinsichtlich der Kontrollmöglichkeit des Beleges durch den Endkunden bei INSIKA im jetzigen Referentenentwurf sind völlig absurd.
Diese sind genau so verfehlt wie die Verpflichtung zur Angabe der USt-Id-Nummer auf Belegen aller Art, während ein Abgleich der zur UST-ID gehörenden Unternehmensanschrift zurzeit mit den Daten der Anschrift auf der Rechnung aus angeblichen Datenschutzgründen dem Kunden nicht möglich ist.

Aus meiner persönlichen Sicht werden ehrliche Händler mit überzogenen Vorschriften belastet, während dubiose Händler per Internet ihre Angebote ohne Umsatzsteuerbelastung an den Mann oder die Frau bringen. Wir erhalten als GmbH zahlreiche Rechnungen per Amazon mit unkontrollierbarer USt-Id-Nummer in Verbindung mit Vorkasse an Empfänger im Ausland.

eBay soll in Deutschland 1,43 Milliarden Euro Umsatz erzielen. Wer bestimmte Produktbereiche dort mit der Einschränkung gewerblicher Verkäufer und billigste Anbieter sucht, sieht kaum noch steuerlich ehrliche Angebote aus Europa.

Die andere Seite ist der Handwerks- oder Handelsbetrieb, der bei Nachfrage nach einen Beleg, unverfroren erklärt „dann muss ich allerdings die MwSt noch aufschlagen“.

Hier sehe ich eher verfassungsrechtliche Bedenken, wenn dem klassischen Fachhändler immer mehr Belastungen abverlangt werden und man dann die Konkurrenz auf Kosten des Steuerzahlers billig davon kommen lässt.

INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Analyse des Referentenentwurfs eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 18. März 2016

Stand: 29. März 2016

Das Bundesministerium der Finanzen (BMF) hat am 18. März 2016 einen Referentenentwurf für ein Gesetz zur Manipulationssicherung für Registrierkassen sowie für eine dazugehörige technische Verordnung veröffentlicht. Das in den Entwürfen beschriebene Verfahren verfolgt das gleiche Ziel wie das INSIKA-Verfahren. Dieses wird jedoch in den Begründungen ausdrücklich als ungeeignet eingestuft und ausgeschlossen.

Auch wenn die Beschreibung des Verfahrens in den Entwürfen allgemein gehalten ist, erschließen sich doch die Grundzüge der technischen und praktischen Rahmenbedingungen, so dass sich die daraus resultierenden Lösungen relativ klar beschreiben lassen. Deren Grundstruktur und die Konsequenzen daraus werden hier analysiert.

Insgesamt ist der Gesetzentwurf grundsätzlich ungeeignet, die vom BMF selbst gesteckten Ziele zu erreichen. Viele Daten und Aussagen in den Entwürfen sind im Übrigen falsch oder irreführend.

Ausgangssituation

Am 18. März 2016 hat das BMF einen Referentenentwurf mit dem Titel *Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen* zusammen mit dem Entwurf einer darauf basierenden Verordnung veröffentlicht.[1]

Diese Entwürfe sollen die seit langem geforderte Manipulationssicherheit für Registrierkassen sicherstellen sowie Rechtssicherheit für alle Beteiligten schaffen.

Laut Text des Gesetzentwurfs dient das neu einzuführende Sicherungsverfahren zur „Sicherstellung der Integrität und Authentizität sowie der Vollständigkeit der elektronischen Aufzeichnung".

Eckpunkte des Verfahrens

Im Folgenden ist die im Entwurf skizzierte Lösung beschrieben. Diese wird dort als „Zertifizierungsverfahren" bezeichnet. Da dies irreführend ist,[2] wird in dieser Analyse die Bezeichnung „SE-Verfahren" (SE = Sicherheitseinrichtung) verwendet.

Die hier dargestellten Eigenschaften des Verfahrens ergeben sich entweder direkt aus den Gesetzes- und Verordnungstexten, den Erläuterungen oder aus dem Kontext.

Grundlagen

Betroffene Systeme

Im Entwurf der Verordnung werden ausdrücklich nur Registrierkassen erwähnt – Taxameter, Geldspielgeräte, Wett-Terminals usw. sind nicht genannt. Eine Abgrenzung der Registrierkassen von anderen Systemen erfolgt in den Erläuterungen zur Verordnung – unklar bleibt aber beispielsweise, ob Barverkaufs-Softwaremodule einer Warenwirtschafts- oder Unternehmenssoftware von den Regelungen betroffen sind.

Eine Kassenpflicht wird im Entwurf ausdrücklich ausgeschlossen.

Technik

Der Kern des SE-Verfahrens wird im neuen einzuführenden § 146a AO definiert: „Diese zertifizierte technische Sicherheitseinrichtung muss aus einem Sicherheitsmodul, einem Speichermedium und einer digitalen Schnittstelle bestehen."

Aus dem Kontext (z.B. „nur ein Sicherheitsmodul an der Hauptkasse") geht hervor, dass es sich um eine Hardware handelt. Durch das Sicherheitsmodul soll jede digitale Aufzeichnung protokolliert werden (Form und Inhalt der Protokollierung werden jedoch offen gelassen). Dieses muss eine besonders geschützte Echtzeituhr beinhalten,

[1] Abrufbar auf der Website des BMF unter der Adresse http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2016-03-18-KassenG-und-technische-VO-Kassen.html

[2] Ein „Zertifizierungsverfahren" ist ein Prozess, der die Einhaltung vorher formulierter Anforderungen überprüft und dadurch zu einem zertifizierten System führt.

da es gemäß § 2 des Entwurfs der Verordnung Uhrzeiten von Geschäftsvorfällen „manipulationssicher festlegen“ soll.

Die Aussage „Ein Speichermedium ist ein Objekt in der digitalen Datenverarbeitung zum Speichern von Daten“ schafft im Detail wenig Klarheit, allerdings kann es sich hier ebenfalls nur um Hardware handeln. Das Speichermedium soll alle „elektronischen Grundaufzeichnungen“ aufnehmen.

Die digitale Schnittstelle soll die zu prüfenden Daten liefern. Ob es sich hier um eine reine Definition von Datenformaten oder auch um die Festlegung von Inhalten, Protokollen bzw. physischen Schnittstellen handelt, bleibt unklar.

Alle drei Komponenten zusammen bilden die technische Sicherheitseinrichtung.

Einige Aussagen bleiben völlig unverständlich, wie z. B. „Eine Transaktionsnummer […] ist ein Einmalpasswort. Ein Einmalpasswort ist ein Kennwort zur Authentifizierung.“

Bei aller Unschärfe der Beschreibung läuft die Lösung jedoch am ehesten auf ein „Fiskalbox-System“ ähnlich denjenigen in Belgien oder Schweden hinaus.[3]

Werden Daten außerhalb des Aufzeichnungssystems in einem „externen elektronischen Archiv“ abgelegt, soll dieses Archiv „manipulationssicher“ sein, also auch zertifiziert werden. Daraus lässt sich folgern, dass die Daten selbst nicht abgesichert werden[4] – sonst wäre ein „manipulationssicheres Archiv“ nicht erforderlich. Wie die Daten während der Übertragung in das Archiv gegen Manipulationen gesichert werden sollen, bleibt offen.

Zulassungsverfahren

Die technische Sicherheitseinrichtung soll durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert werden. Dieses soll hierzu die „technischen Richtlinien und Sicherheitsprofile für die technische Sicherheitseinrichtung“ erstellen und es „übernimmt die Zertifizierung und die Fortschreibung der Sicherheitsprofile.“ Im Verordnungsentwurf wird demgegenüber von „Schutzprofilen“ gesprochen. Damit ist unklar, ob eine Zertifizierung nach Common Criteria oder auf Basis einer technischen Richtlinie erfolgen soll.

Die für eine BSI-Zertifizierung erforderliche Evaluierung bzw. Prüfung aller sicherheitsrelevanten Elemente[5] findet keine Erwähnung, obwohl Aufwand und Kosten der Evaluierungen die Zertifizierungskosten um ein Vielfaches übersteigen.

Bauartanforderungen an die Registrierkassen sind nicht vorgesehen. Mithin existiert lediglich die Anforderung, die beschriebene Sicherheitseinrichtung zu verwenden.

Beschaffung der Sicherheitseinrichtungen

Eine zentrale Ausgabe oder Registrierung der Sicherheitseinrichtungen (bzw. Sicherheitsmodule) ist nicht vorgesehen. So können diese von den Herstellern der Sicherheitseinrichtungen bzw. der Registrierkassen ohne weitere Erfassung oder Überprüfung direkt geliefert werden.

Da ausdrücklich festgestellt wird, dass keine zentrale autorisierte Stelle eingerichtet werden soll, muss die Verwaltung der kryptografischen Schlüssel bzw. Zertifikate (sofern solche zum Einsatz kommen sollten) in der Verantwortung der Hersteller liegen.

Praktische Nutzung

Anwendung

Für die Anwender ist das System weitgehend unsichtbar.

Belege

Eine Belegpflicht ist in den Änderungen der Abgabenordnung nicht erwähnt. Im Begründungsteil wird ausdrücklich darauf hingewiesen, dass keine Belegausgabepflicht besteht. Dies wird in dem den Entwürfen beigefügten Schaubild zudem besonders hervorgehoben.

Kassennachschau

Die Kassennachschau nach dem Entwurf für den § 146b AO ist erkennbar nicht als bloße System- bzw. Verfahrensprüfung angelegt; vielmehr wird in Absatz 2 Satz 2 dieser Norm – ebenso wie im Rahmen einer Betriebsprüfung nach § 146 Abs. 5 und § 147 Abs. 6 Satz 2 AO – vollständiger Datenzugriff (Z 3, also Datenträgerüberlassung) gewährt. Ob diese Form des Datengriffs ausreichend

[3] Siehe auch *Sichere Registrierkassen – internationale Fallbeispiele* (http://www.insika.de/images/stories/INSIKA/Sichere_Registrierkassen_international.pdf)

[4] Eine Absicherung der Daten könnte wie beim INSIKA-Verfahren durch Signaturen erfolgen, wodurch sich Veränderungen zweifelsfrei erkennen lassen. Speichermedien und Archivsysteme müssen bei diesem Ansatz nicht „manipulationssicher“ sein.

[5] Die Zertifizierung ist ein eher formaler Akt, der auf einer durch Dienstleister durchgeführte Evaluierung aufbaut.

ist, um den Zweck der Kassennachschau erreichen zu können, wird von der konkreten Ausgestaltung des Verfahrens abhängen.[6]

Der wesentliche Unterschied zur Betriebsprüfung dürfte also das fehlende Erfordernis einer vorherigen Anordnung sein.

Prüfung

Eine Prüfung basiert vor allem auf Daten, die von der Schnittstelle der Sicherheitseinrichtung geliefert werden. Inwieweit es eine Erleichterung der Prüfung durch eine Standardisierung der Daten geben wird, ist unklar.

Sicherheitsaspekte

In den folgenden Abschnitten werden die wesentlichen Sicherheitsaspekte des SE-Verfahrens beleuchtet.[7]

Kryptografie und Hardware

Bei einer Definition der Sicherheitsanforderungen durch das BSI ist davon auszugehen, dass kryptografische Algorithmen sowie die Hardware des Sicherheitsmoduls dem Stand der Technik entsprechen werden.

Für erfolgreiche Angriffe auf dieser Ebene sollte daher nur ein geringes Restrisiko bestehen.

Schlüsselverwaltung

Eine Schlüsselverwaltung, die nicht in der Hand einer vertrauenswürdigen Stelle liegt, macht jedes kryptografische Sicherheitsverfahren grundsätzlich unsicher.[8]

Die Authentizität der zu sichernden Daten kann damit nicht gewährleistet werden.

Belege

Da keine technische Lösung einen Menschen zur Eingabe von Daten in ein System zwingen kann, lässt sich eine Prüfung vollständiger Verbuchung aller Einnahmen bei elektronischen Kassen gemäß § 146 Abs. 1 AO durch die Finanzverwaltung nur bei verpflichtender Ausgabe eines Belegs mit einem Sicherheitsmerkmal leicht und zuverlässig prüfen.

Der Verzicht auf eine Beleg(ausgabe)pflicht hat deshalb zur Folge, dass eine korrekte Nutzung des Systems nur durch einen Datenzugriff überprüft werden kann.

Der Kontrollaufwand steigt damit ganz erheblich an und das Entdeckungsrisiko für eine Nicht-Nutzung bzw. Nicht-Eingabe ist entsprechend geringer.

Verzeichnis der Sicherheitsmodule

Eine zentrale Ausgabe oder Registrierung der im Einsatz befindlichen Sicherheitsmodule sieht der Referentenentwurf des BMF ebenfalls nicht vor. Folglich würde nicht bekannt sein, welche Sicherheitsmodule bei welchem Anwender im Einsatz sind.

Damit wird das Erkennen von „Zweitkassen“ – also Systemen, die zwar eine Sicherheitseinrichtung benutzen, deren Daten bei einer Prüfung jedoch nicht vorgelegt werden – unmöglich gemacht.

Bewertung des SE-Verfahrens

Sicherheit

Das SE-Verfahren hat aufgrund des Verzichts auf
- eine Belegpflicht,
- ein Sicherheitsmerkmal auf den Belegen und
- die zentrale Erfassung der Sicherheitsmodule

massive, konzeptionelle Sicherheitslücken.

Daher ist es nicht vorstellbar, dass ein Sicherheitskonzept erstellt wurde.

Betriebskonzept

Ein Betriebskonzept – also eine Konzeption aller für den Praxisbetrieb relevanten Strukturen und Prozesse – existiert offenbar ebenfalls nicht. Sonst hätte es nicht zu den konzeptionellen Lücken und Fehlern im vorliegenden Entwurf kommen können.

Technologieoffenheit

Die einzige erkennbare Technologieoffenheit des SE-Verfahrens liegt darin, dass einige Rahmenbedingungen noch nicht im vorliegenden Entwurf definiert sind, sondern erst später durch das BSI festgelegt werden sollen.

Einige konkrete Vorgaben für die Sicherheitseinrichtung (z.B. die Integration eines Speichermediums) schränken die Freiheiten bei der Umsetzung

---

[6] So ist eine Prüfung der korrekten Anwendung des Systems ggf. nur mit einem unmittelbaren Zugriff (Z 1) möglich.

[7] Für nicht mit dem Thema vertraute Leser wird *Wie werden Registrierkassen und Taxameter sicher?* empfohlen (http://www.insika.de/images/stories/INSIKA/Sichere_Registrierkassen_und_Taxameter.pdf).

[8] Kryptografie ist in den Entwürfen nur beispielhaft als eine mögliche Funktion des Sicherheitsmoduls erwähnt. Die Erfüllung der formulierten Anforderungen ohne Kryptografie (vor allem in Form von Signaturen) dürfte jedoch jeglichen realistischen Kostenrahmen sprengen.

sogar über das unbedingt notwenige Maß hinaus deutlich ein.

Kosten

Als Maßstab für preiswerte Hochsicherheitskomponenten dürften heute Smartcards gelten. Nicht plausibel ist, dass eine zertifizierte Sicherheitseinrichtung – bestehend aus einem nicht näher benannten Sicherheitsmodul mit einer Echtzeituhr plus Speichermedium plus digitaler Schnittstelle – preiswerter als eine Smartcard sein soll.

Der Gesetzentwurf selbst nennt im Übrigen mehr als € 100 Mio. Erfüllungsaufwand pro Jahr für Wartung und Support.

Kontrollfähigkeit

Kontrollen in Form einer Kassennachschau bedingen einen Datenzugriff und sind damit für Steuerpflichtige und Vollzugsbehörden sehr aufwändig.

Prüfbarkeit

Eine Prüfung kann nicht mit einem „Vertrauensvorschuss" die Vollständigkeit betreffend begonnen werden. Dadurch ist eine Vereinfachung von Prüfungen gegenüber dem Status Quo nicht zu erreichen. Erleichterung bringt allenfalls die vermutlich vorgesehene umfassende oder teilweise Standardisierung der Daten.

Rechtssicherheit

In Ermangelung eines Schlüsselmanagements durch eine vertrauenswürdige Stelle ist sehr fraglich, ob eine Rechtssicherheit bzgl. „Authentizität" und „Unveränderbarkeit" (§ 146 Abs. 4 AO) der Daten überhaupt möglich ist.

Aufgrund mangelnder Belegpflicht und des fehlenden Verzeichnisses aller Sicherheitsmodule ist Rechtssicherheit betreffend „Vollständigkeit" im Sinne des § 146 Abs. 1 AO in jedem Fall ausgeschlossen. Folgerichtig fehlt der Aspekt der Vollständigkeit auch in der Begründung, wo es unter III.3 Abs. 3 lediglich heißt: „Das Zertifizierungsverfahren ist geeignet die Integrität (Unveränderbarkeit) und Authentizität (Herkunft der Daten) zu sichern."

Bewertung der Aussagen zu INSIKA

Der Entwurf erhält eine Gegenüberstellung des SE-Verfahrens mit dem INSIKA-Verfahren sowie eine Reihe von konkreten Aussagen über INSIKA.

Die Aussagen sind ohne Kontaktaufnahme zum ADM e.V. und offenbar auch ohne Berücksichtigung der verschiedenen, öffentlich verfügbaren Dokumente zu INSIKA aufgestellt worden.

Die wesentlichen kritisierten Eigenschaften des INSIKA-Verfahrens leiten sich direkt aus dem Fachkonzept ab, das unter Federführung des BMF erstellt wurde und die Anforderungen für das Entwicklungsprojekt vorgegeben hat.[9]

Belastbarkeit der Vergleiche

Der Begründungsteil des Gesetzentwurfes stellt unter „Alternativen" nicht verschiedene Konzepte gegenüber, sondern behandelt folgende Optionen:

- Null-Option (Beibehaltung Status Quo)
- INSIKA-Verfahren
- SE-Verfahren

Es wird also ein fertig entwickeltes, erprobtes und vollständig dokumentiertes Verfahrens einer grob umrissenen Lösungsidee gegenüber gestellt. Dabei wird unterstellt, dass die am fertigen Verfahren – also INSIKA – kritisierten Nachteile tatsächlicher oder auch nur vermeintlicher Art der neuen Lösungsidee nicht anhafteten.

Die Auswahl der betrachteten Optionen erscheint angesichts der verschiedenen, real verfügbaren und theoretisch möglichen Lösungen[10] sehr eingeschränkt.

Konkrete Aussagen

Neben einigen zutreffenden Aussagen zum INSIKA-Verfahren sind die im Folgenden aufgeführten Aussagen aus der Begründung eindeutig und nachweislich falsch:[11]

Entspricht nicht den europäischen Sicherheitsanforderungen

Es existieren keine europäischen Sicherheitsanforderungen für Verfahren zur Absicherung von digitalen Grundaufzeichnungen. Es existieren lediglich europäische Anforderungen im Bereich qualifizierter elektronsicher Signaturen (QES) – für das im Gesetzentwurf behandelte Einsatzgebiet sind QES jedoch nicht nutzbar. Eine Anpas-

[9] *Fachkonzept zur Einführung eines neuen Verfahrens zum Manipulationsschutz elektronischer bzw. PC-gestützter Registrierkassen und -systeme* aus dem Jahr 2008, erstellt von einer Bund/Länder-Arbeitsgruppe der Finanzbehörden, nicht veröffentlicht

[10] Beispiele in *Sichere Registrierkassen – internationale Fallbeispiele*, siehe Fußnote 3

[11] Zur Ergänzung siehe auch *14 Irrtümer über INSIKA* (http://www.insika.de/images/stories/INSIKA/14_INSIKA-Irrtuemer.pdf)

sung der kryptografischen Algorithmen an den Stand der Technik ist im INSIKA-Verfahren vorgesehen und jederzeit möglich.[12]

Smartcard-Vergabe und -Verwaltung aufwändig

Jedes sinnvoll prüfbare Sicherheitssystem erfordert, dass alle Sicherheitsmodule zentral erfasst werden. Die dafür erforderlichen Prozesse zur Vergabe und Verwaltung von kryptografischen Zertifikaten und Smartcards (Zertifizierungsdienst, in Zukunft Vertrauensdienst) sind Stand der Technik und von mehreren Anbietern verfügbar.

Rechtliche Risiken durch Einbindung einer autorisierten Stelle

In anderen europäischen Ländern bestehen diese Risiken offenbar nicht, da bei fast jeder Sicherheitslösung für Registrierkassen ein zentrales Verzeichnis aller Systeme bzw. Sicherheitsmodule existiert.

Kostenintensiver durch Belegausgabe

Wie bereits dargestellt ist eine Belegausgabe für jedes sichere System zwingende Voraussetzung. Für einen Großteil der Geschäftsvorfälle werden bereits heute Belege ausgegeben.

Neuanschaffung Drucker erforderlich

Signaturen können auch im Klartext gedruckt werden, was den Arbeitsaufwand für Kontrollen allerdings ein wenig erhöht. Bei Bedarf könnte dies durch eine Übergangsfrist für die Weiternutzung älterer Drucker pragmatisch gelöst werden.

Kostenintensiver durch Smartcard

Es ist nicht plausibel, warum eine zertifizierte Sicherheitseinrichtung bestehend aus einem Sicherheitsmodul mit Echtzeituhr, einem Speichermedium und einer digitalen Schnittstelle preiswerter als eine Smartcard sein soll.

Jede Registrierkasse benötigt eine Smartcard

Diese Aussage ist falsch, da eine Smartcard problemlos von mehreren Kassenplätzen genutzt werden kann. Bei Bedarf können statt Smartcards auch andere Arten von Signaturerstellungseinheiten[13] genutzt werden, die einen ausreichenden Durchsatz bieten, um auch größere Anzahlen von Kassenplätzen zu versorgen.

Verfassungsrechtliche Bedenken

Die Möglichkeit, dass jeder Bürger einen Beleg auf Echtheit überprüfen kann, soll verfassungsrechtlich bedenklich sein. Die gleiche Möglichkeit – etwa bei Prüfplaketten an Fahrzeugen oder eichpflichtigen Ladenwaagen bzw. den Sicherheitsmerkmalen von Geldscheinen – ist ganz offenbar verfassungsrechtlich unbedenklich. Durch eine kleine Modifikation des INSIKA-Verfahrens wäre diese Überprüfungsmöglichkeit sogar zu verhindern, auch wenn das nicht unbedingt sinnvoll wäre.

Bewertung der Kostenschätzungen

Der Gesetzentwurf beinhaltet in der Berechnung des Erfüllungsaufwandes eine Reihe von Zahlen, die nicht plausibel sind:

2,1 Mio. betroffene Geräte

HDE und DEHOGA gehen von zusammen 1,38 Mio. Kassenplätzen aus. Da die von den beiden Verbänden vertretenen Branchen einen sehr großen Teil der Registrierkassen betreiben, ist eine Zahl von 2,1 Mio. Geräten sehr hoch angesetzt.

Konkrete Schätzungen für Umrüstung

Ohne Vorliegen der Sicherheitsanforderungen und damit konkreter Entwürfe für die Sicherheitseinrichtung ist keine seriöse Schätzung möglich.

Sicherheitsmodul: € 8 pro Kasse

Aus den Angaben € 17 Mio. für Sicherheitsmodule und 2,1 Mio. betroffenen Geräten ergeben sich ca. € 8 pro Kasse. Selbst bei der Nutzung eines Sicherheitsmoduls durch mehrere Kassen ist dieser Wert angesichts der Anforderungen an das Sicherheitsmodul (z. B. Echtzeituhr) völlig unrealistisch.

Zertifizierung: € 75.000

Bei diesen Kosten kann es sich nur um die Gebühren für die Zertifizierung durch das BSI handeln. Der wesentliche, um ein Vielfaches höhere Aufwand entsteht jedoch bei der Evaluierung, die als Basis für den eher formellen Akt der Zertifizierung erforderlich ist.

[12] Siehe http://www.insika.de/de/letzte-neuigkeiten/46-insika-karte-die-naechste-generation-kommt

[13] Signaturen können auch durch Hardware-Sicherheitsmodule (HSM) erzeugt werden. Für INSIKA müssen diese (analog zur Smartcard) durch einige Zusatzfunktionen erweitert werden.

Kassennachschauen: € 343.000

Bei einer Kassennachschau pro Verkaufsstelle[14] und Jahr liegen die Kosten jeweils bei € 0,32. Da Kassennachschauen mit dem im Gesetzentwurf definierten Verfahren nur mit Datengriff möglich sind, dürfte diese Schätzung um Zehnerpotenzen falsch sein.

Fazit

Der Gesetzentwurf lässt vieles im Unklaren – die Grundzüge des dort skizzierten Verfahrens sind jedoch erkennbar.

Positiv zu werten ist, dass die Hard- und Software der Registrierkassen selbst keinen besonderen Anforderungen unterliegen.

Abgesehen davon weist der Entwurf mehrere grundsätzliche und gravierende konzeptionelle Lücken auf.

Es gibt weder eine Registrierkassenpflicht, eine Belegpflicht noch eine zentrale Registrierung der Sicherheitskomponenten. Jedes dieser Defizite für sich führt bereits zu erheblichen Sicherheitslücken. Eine Gewähr der Vollständigkeit der digitalen Aufzeichnungen ist damit ausgeschlossen.

Kassennachschauen sind prinzipbedingt stets mit einem hohen Aufwand für Verwaltung und Unternehmen verbunden, da sie grundsätzlich einen Datenzugriff erfordern.

Ein Sicherheits- und ein Betriebskonzept wurden ganz offenbar nicht erstellt.

Die Tatsache, dass der Gesetzentwurf nicht nur eine vollständige Neukonzeption, sondern auch Entwicklung, Erprobung und Integration eines Systems verlangt, lässt eine Einführung zum 1.1.2019 gänzlich unrealistisch erscheinen.

Zusammenfassend ist festzustellen, dass durch das im Gesetzentwurf beschriebene Sicherungsverfahren bei deutlich höheren Kosten für alle Beteiligten der Status Quo nur leicht verbessert würde. Eine wirksame Manipulationsbekämpfung und Rechtssicherheit auf Seiten der Anwender würden jedoch nicht erreicht.

Das fertig entwickelte, erprobte und frei verfügbare INSIKA-Verfahren würde alle Zielsetzungen des Gesetzentwurfs erreichen oder übertreffen. Es wäre in praktisch allen Belangen preisgünstiger – allein schon dadurch, dass es keine nennenswerten Wartungs- und Supportkosten gibt.

INSIKA wird als einzige Alternative im Entwurf behandelt und dann ausdrücklich ausgeschlossen. In der Begründung dafür wird eine Reihe von eindeutigen Falschaussagen verwendet.

INSIKA und ADM e.V.

Das INSIKA-Verfahren („INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“) wurde auf der Grundlage eines Konzepts der deutschen Finanzbehörden von der Physikalisch-Technischen Bundesanstalt von 2008 bis 2012 in einem Gemeinschaftsprojekt mit der Industrie entwickelt und erprobt. Nach erfolgreichem Projektabschluss werden das INSIKA-Konzept und insbesondere die daraus entstandenen technischen Verfahren vom ADM e.V. (Anwendervereinigung Dezentrale Mess-Systeme) unterstützt und weiterentwickelt.

Das INISKA-Verfahren kann ohne Patente, Lizenzkosten oder Ähnliches genutzt werden. Es bestehen daher keine wirtschaftlichen Interessen des ADM e.V. Das Hauptanliegen der Mitglieder liegt vielmehr darin, ein möglichst sicheres, preiswertes und einfach zu nutzendes Verfahren zur Absicherung elektronischer Aufzeichnungen von Bargeschäften zu etablieren – und dabei vor allem eine echte Alternative zu konventionellen, sehr aufwändigen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

Weitere Informationen sind auf www.insika.de frei abrufbar. Lediglich der Abruf der technischen Spezifikationen erfordert eine einfache und kostenlose Registrierung.

Kontakt

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D – 31515 Wunstorf

www.insika.de

E-Mail: info@insika.de

[14] Annahme: durchschnittlich zwei Kassenplätzen pro Verkaufsstelle