Whitepaper: Fiskalsysteme – Anforderungen und Lösungen

Jens Reckendorf, Dr. Norbert Zisky

Stand: 20. November 2014

„Einfachheit ist Voraussetzung für Zuverlässigkeit."
– EDSGER W. DIJKSTRA

Allgemeines

Zu diesem Dokument

Den Autoren ist keine systematische Darstellung und Analyse der Lösungsmöglichkeiten für die Anforderungen der Finanzbehörden an Registrierkassen sowie deren Vor- und Nachteile bekannt. Mit diesem Dokument soll diese Lücke geschlossen werden. Es soll als Hintergrundinformation bei der grundsätzlichen Diskussion über Registrierkassen und Fiskalsysteme dienen, ohne Detailkenntnisse in diesen Bereichen sowie über IT-Sicherheitslösungen vorauszusetzen.

Fragen der Motivation zur Einführung von Auflagen für Registrierkassen, also Art und Ausmaß von Steuerhinterziehung mit Hilfe von Manipulationen sowie generelle Probleme des Steuersystems[1] werden hier nicht erörtert. Es werden nur die technischen und die Kostenaspekte betrachtet.

Eine weiter gehende Einführung in die Grundlagen der Kryptografie und das INSIKA-System ist hier aus Platzgründen nicht möglich. Hinweise auf weiterführende Literatur finden sich am Ende des Dokuments.

Begriffe

Vereinfachend werden im Folgenden alle Systeme, mit denen Bargeschäfte erfasst und dokumentiert werden, als „Registrierkasse" bezeichnet – das reicht vom einfachen Low-Cost-System bis zum Software-Modul einer ERP-Software, das die entsprechende Funktion übernimmt.[2]

Als „Fiskalsystem" werden hier vereinfachend alle Registrierkassen bezeichnet, die besonderen behördlichen technischen und organisatorischen Anforderungen – also strengeren als den allgemeinen Anforderungen an elektronische Buchführungssysteme – unterliegen.

Als „vertrauenswürdige Komponente" wird ein Teil des Systems bezeichnet, der sicherheitsrelevante Aufgaben ausführt und so gegen unbefugte Eingriffe abgesichert ist, dass alle Beteiligten rechtlich bindend auf dessen korrekte Funktion vertrauen können. Dazu muss die Sicherheit dieser Komponente von einer unabhängigen, vertrauenswürdigen Stelle überprüft worden sein.

Autoren, mögliche Interessenkonflikte

Jens Reckendorf ist im Vorstand der Vectron Systems AG, einem Hersteller von Kassensystemen, verantwortlich für Technik und Entwicklung. Er war für die Vectron Systems AG in der INSIKA[3]-Projektgruppe tätig.

Dr. Norbert Zisky ist Leiter der Arbeitsgruppe „Datenkommunikation und -sicherheit" bei der Physikalisch-Technischen Bundesanstalt in Berlin und war Projektleiter des INSIKA-Projekts.

Das INSIKA-Verfahren ist publiziert und unterliegt keinem Patentschutz. Für eine Nutzung fallen keine Lizenzzahlungen oder Ähnliches an. Beiden Autoren bzw. den von ihnen vertretenen Organisationen entstehen keine direkten wirtschaftlichen Vor- oder Nachteile durch die Nutzung bestimmter Lösungen. Es liegt jedoch im Interesse jedes Herstellers von Kassensystemen, der in verschiedenen Märkten tätig ist – also auch Vectron – wenn Anforderungen der Finanzbehörden möglichst sicher und dabei mit möglichst geringem Initial- und laufendem Aufwand erfüllt werden können.

1 In Diskussionen zu dem Thema wird immer wieder mehr oder weniger offen argumentiert, dass aufgrund hoher Steuer- und Sozialabgabenlast eine Steuerverkürzung nur eine Art „Notwehr" wäre. Dieser Aspekt muss jedoch völlig getrennt von technischen Lösungen diskutiert werden, die Steuerhinterziehung verhindern und damit helfen, eine gleichmäßige Besteuerung sicherzustellen.

2 Es sind also auch Waagen mit Kassenfunktionen und Verkaufsautomaten eingeschlossen. Bei der Einführung gesetzlicher Anforderungen sind diese Begriffe präzise zu definieren, um „Umgehungslösungen" zu verhindern.

3 INSIKA steht für „INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme", ein Projekt unter Leitung der PTB (Physikalisch-Technische Bundesanstalt) mit Beteiligung mehrerer Hersteller von Registrierkassen, gefördert durch das Bundesministerium für Wirtschaft und Technologie. INSIKA ist eine eingetragene Marke der Anwendervereinigung Dezentrale Mess-Systeme e.V.

Grundlagen

Das Problem

Mit dem Wechsel von der papierbasierten Buchführung auf elektronische Systeme in der zweiten Hälfte des 20. Jahrhunderts wurde es grundsätzlich möglich, Daten relativ leicht und ohne Nachweismöglichkeit zu verändern. Die gesetzlich geforderte Unveränderbarkeit von Buchführungsdaten war im Papierzeitalter noch relativ einfach zu überprüfen – bei digitalen Daten ist das jedoch nur mit einem geeigneten technischen und rechtlichen Rahmen möglich.[4]

In vielen Anwendungsbereichen spielte und spielt dieses Problem praktisch keine große Rolle. Registrierkassen wurden allerdings verstärkt dazu verwendet, erfasste Umsätze nachträglich zu verkürzen. Mit zunehmenden Kontrollen dieser Systeme durch die Finanzbehörden sind die eingesetzten Manipulationsverfahren immer aufwändiger geworden – das reicht bis zur weitgehend automatisierten und schwer nachweisbaren Manipulation mit Hilfe von „Zappern", also Software, die nur für die Manipulation vorübergehend in das System geladen wird und so keine direkten Spuren hinterlässt.[5]

Entsprechende Diskussionen in der Finanzverwaltung und der Politik begannen in verschiedenen Ländern zu sehr unterschiedlichen Zeitpunkten – teilweise bereits in den 1980er-Jahren, teilweise auch erst nach dem Jahr 2010.[6] In Deutschland wurde das Problem öffentlich im Jahr 2003 durch den Bundesrechnungshof thematisiert[7], was schließlich der Auslöser für die INSIKA-Entwicklung war.

Geschichte der Fiskalsysteme

Anfang der 1980er-Jahre wurden in Italien die ersten Fiskalsysteme entwickelt und sind dort seitdem vorgeschrieben. Der Grundansatz wurde in anderen Ländern übernommen, in den meisten Fällen mit mehr oder weniger umfangreichen Veränderungen. So sind im Laufe der Zeit sehr uneinheitliche rechtliche, organisatorische und technische Lösungen entstanden. Die technische Weiterentwicklung im Bereich der Registrierkassen hat auch zu neuen Ansätzen bei den Fiskalsystemen geführt. So wurde die eigentliche Fiskalspeichertechnik teilweise in modulare Drucker, teilweise in spezielle „Fiskalboxen" ausgelagert. Auch bei Fiskalsystemen wurden Journalaufzeichnungen auf Papier weitgehend durch eine elektronische Protokollierung ersetzt. Kryptografische Verfahren (Verschlüsselung, Hash-Werte, Signaturen) kommen verstärkt zum Einsatz.

Fiskalsysteme werden u. a. in folgenden Ländern eingesetzt: Argentinien, Belgien (nur Gastronomie), Brasilien, Bulgarien, Griechenland, Italien, Kanada (nur Québec, nur Gastronomie), Lettland, Litauen, Polen, Portugal, Russland, Schweden, Türkei, Ungarn, Venezuela.[8]

Besondere Herausforderungen

Die organisatorischen, rechtlichen und technischen Rahmenbedingungen für Fiskalsysteme führen zu einigen Besonderheiten, die es bei der Konzeption und Implementierung von IT-Systemen nicht immer gibt. Zum besseren Verständnis der Situation sollten sie bekannt sein.

Nationale Alleingänge

Bisher hat es keine internationalen Standardisierungen bei Fiskalsystemen gegeben. Auch wenn viele der nationalen Lösungen gewisse Parallelen aufweisen, ist letztendlich in jedem Land ein eigener Weg verfolgt worden. Ein Grund dafür ist sicher die Tatsache, dass Fiskalsysteme unter die Steuergesetzgebung fallen, die selbst in der Europäischen Union komplett in nationaler Verantwortung liegt. Viele Lösungen weisen auch protektionistische Elemente auf, schaffen also Markteintrittsbarrieren für Anbieter aus dem Ausland.

Einzelinteressen

Die Interessen der verschiedenen Beteiligten divergieren sehr stark. So ist die Finanzverwaltung vor allem an einer sicheren Aufdeckung von Manipulationen interessiert. Die umgekehrte Nachweisführung – also der Beleg der formalen Korrektheit liegt dagegen vor allem im Interesse der Anwender, also der Steuerpflichtigen. Ein wichtiger Aspekt für die Anwender ist ferner die Minimierung der Kosten. Hersteller verschiedener Systeme (Re-

4 Huber, Reckendorf, Zisky: Die Unveränderbarkeit der (Kassen-) Buchführung nach §146 Abs. 4 AO im EDV-Zeitalter und INSIKA, BBK Nr. 12 bis 14, NWB Verlag, 2013

5 Siehe auch http://de.wikipedia.org/wiki/Zapper_%28Software%29 (abgerufen am 19.06.2014)

6 OECD: Umsatzverkürzung mittels elektronischer Kassensysteme: Eine Bedrohung für die Steuereinnahmen, 02/2013

7 Bundesrechungshof: Bemerkungen 2003 zur Haushalts- und Wirtschaftsführung des Bundes, 54, S. 197-198

8 Quelle: http://de.wikipedia.org/wiki/Fiskalspeicher (abgerufen am 19.06.2014) und eigene Recherchen

gistrierkassen, Fiskaldrucker, externe Fiskalspeichereinheiten) haben jeweils unterschiedliche wirtschaftliche Interessen. Politische Einflüsse[9] spielen ebenfalls eine wichtige Rolle.

Die Interessen aller Beteiligten werden erfahrungsgemäß im Diskussionsprozess über das einzuführende Fiskalsystem nicht unbedingt adäquat vertreten und neutral bewertet. Je nachdem, welche Partei am Entscheidungsprozess wie intensiv beteiligt war, kann das resultierende System sehr unterschiedlich ausfallen. Das auf diesem Weg erzielte Ergebnis stellt meistens nicht die ideale technische Lösung dar.

„Kulturelle Unterschiede"

Fiskalsysteme werden in Zusammenarbeit von Experten für Steuerfragen (Verwaltungsfachleute und Juristen) sowie für verschiedene technische Spezialdisziplinen (Registrierkassen, IT-Sicherheitslösungen) konzipiert. Deren Herangehensweise unterscheidet sich sehr deutlich. In politischen Entscheidungsprozessen wird wiederum anders vorgegangen.

Im Bereich der Finanzverwaltung ist es aufgrund der Rahmenbedingungen üblich, dass sich Vorschriften evolutionär entwickeln, also laufend leicht verändert werden, statt sie einmal neu zu konzipieren. Es wird eher „principle-based" gearbeitet, also ein Grundsatz oder ein Ziel definiert (Beispiel: „Daten müssen unveränderbar gespeichert werden"). Auslegungsspielräume und Einzelfall-Entscheidungen sind dabei oft unvermeidlich.

Technische Lösungen hingegen erfordern vollständig durchkonzipierte Systeme. Für eine Implementierung muss „rule-based" gearbeitet, also konkrete Festlegungen getroffen werden (Beispiel: „Daten müssen durch eine digitale Signatur eines vertrauenswürdigen Subsystems geschützt sein"). Auslegungsprobleme müssen vermieden werden.

In der Politik verhindern Kompromisse und Interessenausgleich oft stringente Lösungen. Besonders problematisch ist das, wenn daraus resultierende Eingriffe ohne detaillierte Kenntnisse des jeweiligen Sachverhalts stattfinden.

Die wichtigsten, daraus resultierenden Missverständnisse und Fehleinschätzungen werden in den Kästen „Sicherheit", „Prozesse" und „Konzipierung und Einführung" plakativ formuliert und diskutiert.

9 Das reicht von der Einflussnahme durch Interessenverbände bis zu Fragen der Übernahme tatsächlicher oder vermeintlicher Kosten durch verschiedene Teile der Verwaltung.

Die Qualität von in diesem Spannungsfeld entstandenen Fiskalsystemen hängt stark davon ab, wie mit den Widersprüchen umgegangen wurde und ob trotz der Konflikte ein sauberes Konzept entstehen und vor allem auch umgesetzt werden konnte.

Haftungsfragen

Für Hersteller und Anwender von Fiskalsystemen gibt es Haftungsrisiken. Sollte ein System nachträglich als nicht ordnungsmäßig eingestuft werden, droht dem Anwender die Schätzung seiner Besteuerungsgrundlagen.[10] Je nach Verschulden des Herstellers drohen diesem straf- und zivilrechtliche Ansprüche. Selbst wenn ein Hersteller nicht vorsätzlich oder fahrlässig gehandelt hat, wird er den Anwendern gegenüber zumindest zur Nachbesserung verpflichtet sein – was nicht nur mit einem hohen Kostenaufwand, sondern auch mit einem Imageschaden verbunden ist.

Marktdruck

In einigen Branchen besteht ein erheblicher Druck der Anwender auf Hersteller von Registrierkassen, Manipulationen zu ermöglichen. Sobald ein Hersteller diesem nachgibt, werden aufgrund der Wettbewerbssituation i. d. R. weitere nachziehen. Das betrifft nicht nur „ungeschützte" Registrierkassen, sondern auch zertifizierte Fiskalsysteme, wie Beispiele aus der jüngeren Vergangenheit zeigen.[11]

Was soll ein gutes Fiskalsystem leisten?

Wie bei jedem technischen System müssen auch für Fiskalsysteme vor der Konzeption und Entwicklung die Ziele und Anforderungen formuliert werden. Entsprechende Dokumente sind allerdings für die wenigsten Systeme verfügbar. Daher soll hier versucht werden, die Anforderungen möglichst allgemeingültig darzustellen.[12] Es werden nur die Anforderungen beschrieben, die bei einem Fiskalsystem über diejenigen an eine nicht gesicherte Registrierkasse hinausgehen.

10 Nach §158 AO ist die Buchführung die Grundlage für die Besteuerung, wenn ihre Richtigkeit nicht beanstandet werden kann. Ist die Buchführung nicht Grundlage der Besteuerung, erfolgt eine Schätzung gemäß §162 AO. Wenn Daten manipuliert worden sind, ist die Richtigkeit eindeutig widerlegt. Sind Manipulationen nur möglich, aber nicht nachgewiesen, ist die rechtliche Situation komplex – momentan entscheidet die Finanzverwaltung aufgrund divergierender Entscheidungen der Finanzgerichte dabei sehr uneinheitlich.

11 Bei zertifizierten Fiskalsystemen in Portugal und Ungarn sind 2014 massive Sicherheitslücken bekannt geworden – siehe auch Fußnoten 4 und 5 im Kasten „Missverständnisse: Sicherheit".

12 Diese Anforderungen basieren nicht auf einer Norm oder einem anderen Standard, da diese nicht existieren. Sie wurden von der INSIKA-Projektgruppe formuliert, u. a. auf Basis eines Fachkonzepts der deutschen Finanzverwaltung und anhand der Analyse bestehender Fiskalsysteme.

Missverständnisse: Prozesse

„Prüfungen werden verlässlicher, wenn viele redundante Informationen abgeglichen werden“

Sowohl bei der Konzeption von Fiskalsystemen als auch in der Praxis der Betriebsprüfung wird oft sehr viel Wert auf Berichte gelegt, also verdichtete Daten. Die Überlegung dahinter scheint zu sein, dass man durch einen Abgleich der Daten (also ein Nachvollziehen der Summenbildungen) Unstimmigkeiten aufdecken kann. Für Manipulationen an einer Papierbuchhaltung mag das auch stimmen, da bei manuellen Eingriffen früher oder später Fehler gemacht werden.

Falls ein System mit digitaler Aufzeichnung von Einzeltransaktionen manipuliert wird (weil es nicht ausreichend abgesichert ist), werden dabei mit Sicherheit auch alle Berichte so berechnet, dass die Daten insgesamt plausibel sind. Man wird also mit einem Abgleich verschiedener Berichte keine Manipulationen aufdecken können, sondern nur den Prüfungsaufwand erhöhen.

Die Prüfung von Einzeltransaktionen erlaubt es heute, sämtliche Summenbildungen während der Prüfung vorzunehmen. Stellt man also die Integrität der Einzeltransaktionen sicher, sind alle daraus ermittelten verdichteten Werte ebenfalls verlässlich.

„Programmänderungen an der Registrierkasse müssen aufgezeichnet werden“

Es wird immer wieder die Anforderungen formuliert, dass Registrierkassen und Fiskalsysteme Änderungen an der Programmierung (also an Parametern, Stammdaten usw.) protokollieren müssen. Diese Anforderung entstammt offenbar der Erkenntnis, dass es manipulierbare Systeme gibt, bei denen die Manipulationen eine Änderung der Programmierung erfordern (z. B. das Einschalten eines „Trainingsmodus“ der die reguläre Umsatzaufzeichnung unterdrückt). Wenn man allerdings dem Hersteller nicht vertraut, weil er Manipulationsfunktionen in das System integriert hat, besteht auch kein Grund, darauf zu vertrauen, dass entsprechende Umprogrammierungen korrekt aufgezeichnet würden bzw. diese Aufzeichnungen unveränderbar wären.

Die einzige sinnvolle Lösung kann daher nur sein, ein System so zu spezifizieren, dass die Sicherheit des Systems nicht durch Programmänderungen beeinflusst wird. Wenn für die Sicherheit des Systems ausschließlich eine vertrauenswürdige Komponente verantwortlich ist und nicht der Hersteller der Registrierkasse, wird diese Forderung automatisch erfüllt.

„Eine technische Lösung kann Kontrollen ersetzen“

Es hat eine Reihe von Fiskalsystem-Einführungen gegeben, bei denen eine regelmäßige Kontrolle der korrekten Benutzung des Systems (siehe unter „Anforderungen“) nicht vorgesehen wurde. Das geschieht offenbar aus Unkenntnis oder aus politischen Erwägungen, vor allem aufgrund der tatsächlichen oder vermeintlichen Kosten dieser Kontrollen. Im Gegenzug wurde versucht, diese Kontrolle durch technische Maßnahmen überflüssig zu machen. Um diesen Ansatz zu bewerten, müssen die grundsätzlichen Manipulationsmöglichkeiten zum Zeitpunkt der Erfassung betrachtet werden (Manipulationen nach der Datenerfassung lassen sich durch rein technische Maßnahmen recht sicher verhindern):

1. Verfälschte Datenaufzeichnung unter Nutzung dafür vorgesehener Funktionen im System (es werden also i. d. R. geringere Umsätze aufgezeichnet als tatsächlich getätigt wurden)
2. Nicht-Erfassung (Umsätze werden gar nicht erst in die Registrierkasse eingegeben)
3. Verwendung mehrerer Registrierkassen (ein Teil der Umsätze wird in einer Registrierkasse erfasst, deren Daten nicht steuerlich angegeben werden)

Von den hier aufgeführten Möglichkeiten lässt sich lediglich Methode 1 durch technische Anforderungen an Registrierkassen erschweren, aber auch nicht verhindern (verbunden mit sehr hohem Aufwand, der vor allem aus den dann nötigen Zertifizierungen samt Marktüberwachung resultiert)[1]. Die beiden anderen Methoden[2] sind grundsätzlich nicht ohne menschliches Eingreifen zu verhindern. Ein gutes Fiskalsystem kann allerdings die erforderlichen Kontrollen möglichst einfach und sicher machen.

„Eine Belegpflicht ist nicht so wichtig“

Erst ein Beleg erlaubt die unbedingt erforderlichen Stichprobenkontrollen mit vertretbarem Aufwand. Diese Kontrollen sind unausweichlich, da nur dadurch ein Entdeckungsrisiko für die Nichtnutzung des Systems bzw. zeitversetzte Erfassung[3] entsteht. Daher beinhaltet jedes den Autoren bekannte Fiskalsystem eine Belegpflicht.

---

1 Mit etwas Aufwand sind auch hier Manipulationen weiterhin möglich. Beispiel: Ein zertifiziertes Fiskalsystem auf einer offenen Systemplattform (z. B. Windows) läuft zusammen mit einer zweiten nicht zertifizierten Registrierkassensoftware. Der Benutzer arbeitet mit der zweiten Software, diese überträgt jedoch nur einen Teil der Vorgänge in die zertifizierte Software (die völlig frei von Manipulationsfunktionen ist). Das erfolgt durch eine Simulation von Tasteneingaben auf Betriebssystemebene, die von dieser Software nicht von echten Eingaben unterschieden werden kann. Dieser Angriff kann ausschließlich durch Kontrollen erkannt werden, niemals durch nachträgliche Prüfungen. Ein Verbot offener System dürfte angesichts deren großer Verbreitung kaum eine praktikable Lösung sein.

2 Aufmerksamen Besuchern in diversen Ländern mit Fiskalkassen-Pflicht wird aufgefallen sein, dass die Nicht-Erfassung und die parallele Verwendung nicht-fiskalisierter Registrierkassen teilweise ein so großes Ausmaß angenommen haben, dass damit der Ansatz ad absurdum geführt wurde. Ermöglicht wird das durch fehlende oder zu seltene Kontrollen (wobei immer eine Rolle spielt, wie leicht diese Kontrollen beim jeweiligen System sind).

3 Falls die Daten in ungesichter Form eine gewisse Zeit gesammelt und erst später im gesichterten System erfasst werden (was manuell aber auch automatisch erfolgen kann), sind für diesen Zeitraum beliebige Manipulationen möglich. Die Kette der Sicherheitsmaßnahmen ist dann direkt am Anfang unterbrochen.

Zur Gliederung werden die Anforderungen im Folgenden in drei gebräuchliche Kategorien unterteilt: funktionale Anforderungen, nichtfunktionale Anforderungen und Rahmenbedingungen.

„Soll" bedeutet im Folgenden, dass diese Anforderung verpflichtend ist, mit „sollte" werden optionale Anforderungen beschrieben.

Funktionale Anforderungen

Die funktionalen Anforderungen legen fest, was ein System leisten soll, also welche Aufgaben es ausführt.

Integrität sicherstellen

Veränderungen oder Löschungen an bereits aufgezeichneten Daten sollen verhindert werden oder sicher erkennbar sein, unabhängig davon, wie diese Veränderungen zustande gekommen sind (z. B. durch bewusste Manipulationen, technische oder Bedienfehler).

Authentizität sicherstellen

An den aufgezeichneten Daten soll der Urheber eindeutig erkennbar sein. Daten dürfen nicht unter einer falschen Identität aufgezeichnet werden können. Daraus resultiert umgekehrt die Nichtabstreitbarkeit der Urheberschaft der Daten.

End-to-end-Absicherung

Der Absicherungsmechanismus soll von der Erfassung der Daten bis zu deren Überprüfung durchgängig wirksam sein. Somit haben alle Zwischenstationen, die Daten speichern oder übertragen, keinen Einfluss auf die Sicherheit des Gesamtsystems. Sie müssen also auch nicht vertrauenswürdig sein. Vergleichbar ist das mit dem Versand einer Nachricht in einem versiegelten Briefumschlag – unabhängig vom Versandweg erlaubt das Siegel immer die Erkennung eines unbefugten Zugriffs auf die Nachricht.

Ausmaß von Veränderungen abschätzbar machen

Wenn aufgezeichnete Daten verändert oder vernichtet wurden – ob durch eine Manipulation, einen technischen Fehler oder einen Datenverlust aufgrund eines Benutzerfehlers – soll es möglich sein, das Ausmaß der Veränderungen zu ermitteln.

Kontrollmechanismus bereitstellen

Jedes Fiskalsystem kann grundsätzlich dadurch umgangen werden, dass Daten erst gar nicht erfasst werden (z. B. auch durch Verwendung einer zusätzlichen, nicht abgesicherten Registrierkasse). Dies ist nur durch stichprobenartige Kontrollen verhinderbar. Daher soll das System einen sicheren Mechanismus für diese Kontrollen bereitstellen.

Datensicherheit gewährleisten

Das System soll einen angemessenen Schutz gegen den immer möglichen Verlust der Daten bieten. Das kann innerhalb des Systems umgesetzt werden (z. B. über eine Datenspeicherung auf zwei getrennten Speichermedien) oder besser dadurch, dass Datensicherungen auf externe Speicher möglich sind, ohne dass die anderen Anforderungen (vor allem die Anforderungen bzgl. der Integrität und Authentizität) verletzt werden.

Nichtfunktionale Anforderungen

Die nichtfunktionalen Anforderungen legen eine Reihe von Eigenschaften fest, die durch die funktionalen Anforderungen nicht bestimmt sind. Im Wesentlichen wird durch sie bestimmt, wie ein System arbeitet. Einen großen Teil der Anforderungen kann man als „Qualitätsmerkmale" ansehen.

Geringe Komplexität

Komplexität erhöht grundsätzlich die Fehleranfälligkeit und die Kosten eines Systems. Bei Sicherheitslösungen sind Fehler zudem häufig potenzielle Sicherheitslücken. Daher soll die Komplexität so weit wie möglich reduziert werden.

Fehlertoleranz

Bei Veränderungen an abgesicherten Daten, technischen Fehlern, Systemstörungen usw. sollen die Auswirkungen möglichst minimiert werden. So darf z.B. ein defekter Datensatz nicht dazu führen, dass folgende Datensätze nicht mehr verifiziert oder sogar überhaupt nicht mehr ausgewertet werden können.

Vertrauenswürdiger Teil des Systems möglichst klein

Jede Sicherheitslösung benötigt eine oder mehrere Komponenten, die vertrauenswürdig sind. Sobald dieses Vertrauen nicht (mehr) gewährleistet ist, muss das gesamte System als unsicher eingestuft werden. Um Aufwand und Sicherheitsrisiken zu minimieren, soll dieser vertrauenswürdige Teil möglichst klein, einfach und preiswert gehalten werden.

Evaluierbarkeit

Die vertrauenswürdigen, also die für die Sicherheit des Systems relevanten Teile (Prozesse, Hard- und Software) sollen durch unabhängige Dritte überprüft werden können. Diese Prüfung soll ein möglichst hohes Sicherheits- und Vertrauensniveau gewährleisten. Die Prüfkriterien und Prozesse soll-

ten so weit wie möglich einem bestehenden Standard folgen (z. B. Common Criteria[13]) und nicht speziell für das vorliegende System definiert werden.

Einfache Kontrollen

Der unter den funktionalen Anforderungen aufgeführte Kontrollmechanismus soll so einfach wie möglich sein. Eine Kontrolle soll so wenig Aufwand wie möglich bedingen und sollte keinen Zugriff auf nur aufwändig zu beschaffende Informationen (wie z. B. Daten aus dem Fiskalsystem, dessen korrekte Benutzung gerade kontrolliert wird) erfordern.

„Minimal-invasiv"

Ein Fiskalsystem basiert auf vorhandenen Registrierkassen, die technisch und fachlich eine sehr große Bandbreite abdecken. Um Integrationsprobleme, Kosten und Risiken zu minimieren, sollen die zusätzlichen Komponenten zur Absicherung der Daten möglichst geringe Eingriffe in die bestehende Technik erfordern.

In möglichst viele Systeme integrierbar

An die Registrierkassen, welche die Basis des Fiskalsystems darstellen, sollen nur so wenige Anforderungen wie möglich gestellt werden (z. B. in Bezug auf das Betriebssystem oder auf Schnittstellen). So lässt sich erreichen, dass möglichst viele Systeme nach- oder umgerüstet werden können. Das führt zur Kostenreduktion und zu einer einfacheren Einführung.

Eindeutig spezifizierte Schnittstellen

Die Schnittstellen des Systems sollen so eindeutig wie möglich spezifiziert sein, um Auslegungsprobleme und Inkompatibilitäten zu vermeiden.

Möglichst geringe Abhängigkeit von bestimmten Technologien

Der rechtliche Rahmen für ein Fiskalsystem besteht i. d. R. wesentlich länger als der Lebenszyklus der meisten Technologien im IT-Bereich dauert. So ist z. B. die Verwendung bestimmter Schnittstellen oder Speichermedien problematisch. Daher sollten die Abhängigkeiten minimiert und dort, wo sie unvermeidbar sind, sorgfältig durchdacht und spezifiziert werden.

Anpassbar an neue Sicherheitsstandards

Bei allen IT-Sicherheitslösungen, also auch bei kryptografischen Verfahren, muss damit gerechnet werden, dass eine Anpassung an neuere Sicherheitsstandards erforderlich ist, wenn die Gefahr droht, dass ein System „geknackt" werden könnte oder gar bereits ein erfolgreicher Angriff stattgefunden hat. Ein Fiskalsystem soll in solchen Fällen mit möglichst wenig Aufwand angepasst werden können.

Auswirkungen von Sicherheitslücken minimieren

Wenn ein einzelnes System kompromittiert wurde (z.B. indem ein dort verwendeter kryptografischer Schlüssel in unbefugte Hände gelangt ist), soll die Sicherheit aller anderen Systeme nicht gefährdet sein.

Rahmenbedingungen

Jedes technische System wird in einem bestimmten Umfeld betrieben. Aus diesem spezifischen Umfeld ergeben sich Einschränkungen, die vom System berücksichtigt werden müssen.

Kosten minimieren

Es soll eine Minimierung der Kosten angestrebt werden. Das gilt sowohl für Einmalkosten (vor allem Entwicklungskosten) als auch für Stückkosten. Zusätzliche laufende Betriebskosten sollten vermieden werden.

Steuerrecht als gesetzlichen Rahmen berücksichtigen

Das spezifizierte System dient zur Erfüllung steuerrechtlicher Vorgaben. Es muss sowohl den Finanzbehörden als auch den Anwendern höchstmögliche Rechtssicherheit bieten. Daher soll es so aufgebaut werden, dass es leicht in den durch das bestehende Steuerrecht vorgegebenen Rahmen integriert werden kann.

Wettbewerbsverzerrung vermeiden

Jeder regulatorische Eingriff in eine Branche kann zu Wettbewerbsverzerrungen führen. Diese sollen so weit wie möglich vermieden werden. Es sollten also alle Hersteller möglichst die gleichen Ausgangsbedingungen für eine Anpassung ihrer Lösungen haben, auch wenn sich z. B. Produkte und Unternehmensgröße erheblich unterscheiden.

Einbettung in ein Kontroll- und Prüfkonzept

Ein Fiskalsystem kann nicht als technische Lösung alleine existieren, sondern muss in ein durch die Verwaltung praktisch umsetzbares Konzept für Kontrollen und Prüfungen eingebunden sein. Dieses Konzept soll Teil der Spezifikation und Entwicklung des Systems sein.

13 Die „Common Criteria for Information Technology Security Evaluation" sind ein internationaler Standard für die Bewertung und Zertifizierung der Sicherheit von Computersystemen im Hinblick auf die Datensicherheit.

Missverständisse: Konzipierung und Einführung

„Kassenhersteller und Steuerexperten entwerfen gute Sicherheitslösungen“

Die Konzeption und Implementierung von sicheren IT-Systemen ist ein Spezialgebiet, für das es relativ wenige Fachleute gibt.

Bei der Konzeption der meisten Fiskalsysteme wurden jedoch keine ausgewiesenen Sicherheitsexperten hinzugezogen. Stattdessen erfolgt sie meistens aus dem Kreis der direkt Betroffenen heraus, also durch Mitarbeiter der Finanzverwaltung und Vertreter der Registrierkassen-Branche, speziell der Anbieter von Fiskalsystemen. Konzeptionelle Fehler lassen sich bei diesem Ansatz nicht vermeiden. Dieses Problem wird dadurch verschärft, dass IT-Sicherheitslösungen auf den ersten Blick relativ einfach erscheinen, so dass oft gar nicht erst der Bedarf gesehen wird, entsprechende Fachleute einzubinden.

„Bestehende Systeme sind bewährt und daher gut“

Fiskallösungen entstehen praktisch nie aus einem Wettbewerb zwischen verschiedenen Lösungsansätzen, sondern werden konzipiert und dann gesetzlich eingeführt. Vorherige Praxistests erfolgen i.d.R. nicht. Da Nachbesserungen einen extrem großen Aufwand nach sich ziehen und – wenn überhaupt – nur mit Übergangsfristen möglich sind, werden einmal bestehende Lösungen nicht oder nur sehr langsam weiter entwickelt.

Aus der Tatsache, dass ein System praktisch genutzt wird, lässt sich daher keine Aussage über die Qualität ableiten. Das erklärt auch, warum in einer Reihe von Ländern Systeme im Einsatz sind, die erwiesenermaßen nicht im Sinne der hier formulierten Anforderungen funktionieren.

„Freiwillige Lösungen funktionieren auch“

Bei einem freiwilligen Einsatz von Fiskalsystemen ist es grundsätzlich ebenfalls möglich, einen Rahmen zu schaffen, der einen Nachweis der Integrität der Daten ab dem Zeitpunkt der Speicherung erlaubt. Dazu ist in jedem Fall aber eine Komponente erforderlich, für deren Sicherheit eine vertrauenswürdige Stelle verantwortlich ist.

Es muss jedoch auch sichergestellt werden, dass alle Verkaufsvorgänge im System erfasst wurden. Das ist ausschließlich durch Stichprobenkontrollen möglich, die aber nur stattfinden können, wenn der Einsatz des Fiskalsystems verpflichtend ist. Für eine sinnvolle Prüfung müssen alle Fiskalsysteme, die ein bestimmter Steuerpflichtiger einsetzt, bekannt sein – diese Information ist bei einer freiwilligen Nutzung nicht verfügbar.

Aus diesen Gründen erfüllt ein freiwilliger Einsatz nur einen kleinen Teil der Anforderungen und ist daher nicht sinnvoll.

„Ein Fiskalsystem führt grundsätzlich zu mehr Bürokratie“

Wird über die Einführung von Fiskalsystemen diskutiert, wird i.d.R. das Argument angeführt, dass damit „noch mehr Bürokratie“ verbunden sei. Ein gut konzipiertes Fiskalsystem bewirkt, dass sich für den Anwender praktisch kaum etwas verändert, die formell korrekte Erfassung der Verkaufsdaten aber erstmalig nachgewiesen kann. Das führt zu einer deutlichen Vereinfachung von Betriebsprüfungen sowie zu einer Verringerung von Dokumentationspflichten.

„Ein Fiskalsystem bedeutet totale Überwachung“

Hier ist zu bedenken, dass im Steuersystem bereits ein sehr weitgehendes Zugriffsrecht der Behörden auf Informationen der Steuerpflichtigen verankert ist – es existiert also bereits eine sehr weitgehende Überwachung. Durch Fiskalsysteme wird ein Teil dieser Daten lediglich vor Veränderungen geschützt, was wiederum den Bedarf nach Überwachung und Prüfung zur Aufdeckung eventueller Manipulationen reduziert.

Lösungen mit einer Online-Datenübertragung erhöhen dagegen tatsächlich die Überwachungsmöglichkeiten der Behörden, so dass diese durchaus kritisch gesehen werden können.

„Strafbarkeit und Haftung für Entwicklung und Verkauf von Manipulationssoftware sind entscheidend für eine Problemlösung“

Als unterstützende Maßnahme ist die Strafbarkeit der Herstellung von Manipulationssoftware (verbunden mit einer Haftung für die Folgen des Einsatzes) sicher hilfreich, auch wenn der Nachweis der Urheberschaft in der Praxis oft ein Problem darstellt. Ein sinnvolles Fiskalsystem muss jedoch in erster Linie durch seine technische Konzeption sicher sein und nicht dadurch, dass Angriffe darauf strafrechtlich verfolgt werden. Sonst werden die Probleme nicht ursächlich bekämpft.

Rechtliche Konsequenzen für die Nichterfassung von Daten (ob durch Nichteingabe oder durch Verwendung von „Zweitkassen“) und die Beihilfe dazu muss es selbstverständlich geben.[1]

1 Im deutschen Recht sind die hier angesprochenen Probleme zzt. völlig unpassend abgebildet: Die (technisch zu verhindernde) Datenmanipulation ist nach §274 StGB strafbar. Eine Nichterfassung ist rechtlich keine Steuerhinterziehung, sondern eine straflose Vorbereitungshandlung, die lediglich eine Ordnungswidrigkeit ist. Hier ist der Gesetzgeber für eine Anpassung des Rechts an die realen Verhältnisse gefragt.

Lösungsansätze

Im Folgenden werden alle bekannten grundsätzlichen Lösungsansätze zur Erfüllung von Anforderungen der Finanzbehörden kurz dargestellt.[14]

System ohne technische Sicherungen

Bei ungesicherten Systemen existieren keine konkreten Vorgaben für Registrierkassen. Es werden lediglich die allgemeinen Vorschriften des Steuerrechts auf diese Systeme angewendet. Technische Sicherungen werden – selbst wenn sie existieren – von den Finanzbehörden nicht verbindlich anerkannt, da eine rechtliche Grundlage fehlt. Diese Systeme gehören nach der hier benutzten Definition nicht zu den Fiskalsystemen.

Der größte Nachteil dieser Systeme ist die fehlende Sicherheit. Daraus resultieren nicht nur eine große Manipulationsanfälligkeit, sondern auch ein großer Prüfungsaufwand sowie die fehlende Rechtssicherheit für die Anwender dieser Systeme.

System ohne technische Sicherungen mit Zertifizierungen

Für Systeme ohne technische Sicherungen sind Compliance-Erklärungen (erfolgen durch den Hersteller) oder Zertifizierungen (erfolgen durch Dritte) möglich, deren Aussagewert ist jedoch gering.[15] Diese Maßnahmen bieten prinzipbedingt keine hinreichende Sicherheit, dass Veränderungen an den Daten ausgeschlossen sind.

Auch diese Lösungen gehören nach der hier benutzten Definition nicht zu den Fiskalsystemen.

Konventionelle Fiskalsysteme

Entsprechend der in den 1980er-Jahren verfügbaren Technik basierten diese Systeme vor allem auf einem mechanischen Schutz des Speichers gegen unerlaubte Zugriffe verbunden mit Bauartanforderungen an das Gesamtsystem. Der eigentliche Fiskalspeicher bestand zu dieser Zeit aus EPROMs[16], die zusammen mit einem Mikroprozessor fest zu einem Modul verbunden wurden, z. B. mit Gießharz. Dadurch konnte der EPROM-Speicher nicht mehr gelöscht werden. Aufgrund der geringen Speicherkapazität werden nur Tagesumsatzsummen gespeichert. Um ein solches System sicher zu machen, muss es komplett gegen Eingriffe geschützt werden, da ansonsten die Umsätze vor dem dauerhaften Abspeichern im Fiskalspeicher manipuliert werden könnten. In der Folge muss die gesamte Registrierkasse verplombt und die Hard- und Software zertifiziert werden.[17] Inzwischen kommt bei solchen Systemen bei gleichem Grundprinzip modernere Technik (z. B. Flashspeicher) zum Einsatz.

Die zunehmende Modularisierung von Registrierkassen, d. h. die Auftrennung in Tastatur, Bildschirm/Display, CPU-Einheit und Drucker widersprach dem ursprünglichen Konzept, alle Komponenten in einem Gehäuse zu integrieren. Dies wurde durch das Konzept des „Fiskaldruckers“ gelöst. Dabei ist das Fiskalspeichermodul im modularen Drucker eingebaut.

Da die ursprünglich verwendeten, auf Papier gedruckten Journale (also die Aufzeichnung aller Buchungsdetails) in der Praxis kaum prüf- und auswertbar sind und die verfügbaren Speicherkapazitäten z. B. durch Flash-Speicher schnell wuchsen, wurden verstärkt Lösungen mit einer elektronischen Aufzeichnung des Journals entwickelt.

Auch wenn die konventionellen Lösungen grundsätzlich die wesentlichen Anforderungen erfüllen, ist vor allem der hohe Aufwand für Entwicklung, Zertifizierung und Betrieb nachteilig. Die komplexen Auflagen und die erforderliche Zertifizierung von Weiterentwicklungen führen zu wenig leistungsfähigen, aber besonders teuren Produkten.

Kryptografische Lösungen

Im weiteren Bemühen, Fiskalsysteme sicherer zu machen, wurden die aufzuzeichnenden Buchungsdaten in einigen Systemen kryptografisch gesichert. Dabei kommen vor allem digitale Signaturen, aber auch Verschlüsselungsverfahren zum Einsatz.

14 Teile des Abschnitts basieren auf http://de.wikipedia.org/wiki/Fiskalspeicher (abgerufen am 10.06.2014)

15 Beispiele sind das „Keurmerk: Het betrouwbare afrekensysteem“ in den Niederlanden oder Software-Bescheinigungen von Wirtschaftsprüfern in Deutschland oder Österreich.

16 EPROMs sind heute nicht mehr gebräuchliche Speicherbausteine, die durch ultraviolettes Licht löschbar sind.

17 Jede Änderung am System (Hardware und Software) erfordert dabei eine erneute Zertifizierung. Die Überwachung der Systeme im laufenden Betrieb ist mit großem Aufwand verbunden und muss durch technische Spezialisten erfolgen.

Es muss unterschieden werden zwischen Systemen, die eine vertrauenswürdige Komponente für die kryptografischen Funktionen verwenden (also z. B. eine zertifizierte „Fiskalbox“ oder eine Smartcard) und solchen, die diese in einem nicht vertrauenswürdigen Teil des Systems (also z. B. als Teil der Anwendungssoftware) implementieren.[18]

Bisher wird dabei vor allem das Prinzip „Security through obscurity“[19] angewandt – kryptografische Lösungen nach aktuellen Standards sind bisher sehr selten. Daher ist auch bei allen den Autoren bekannten Fiskalsystemen (außer INSIKA) nach wie vor eine Zertifizierung des Gesamtsystems erforderlich.

Wenn das Hinzufügen der kryptografischen Elemente nicht die Grundprobleme der konventionellen Lösungen (also vor allem die aufwändige Zertifizierung) vermeidet, steigt lediglich der Aufwand an. Kryptografische Lösungen ohne vertrauenswürde Komponenten können sogar eine Sicherheit suggerieren, die nicht vorhanden ist.

Online-Systeme

In einigen Ländern (z. B. Serbien) werden Systeme eingesetzt, die eine Online-Übertragung von Daten direkt an die Finanzverwaltung erfordern.

Neben den Kosten für die Datenübertragung und -speicherung stellt die Abhängig von der Datenverbindung ein großes Problem dar. In vielen Ländern ist das Konzept auch nicht mit den allgemein akzeptierten Vorstellungen von Kontrollrechten des Staates vereinbar.

Warum das INSIKA-Verfahren die beste verfügbare Lösung ist

Bei der Konzeption des INSIKA-Verfahrens wurden die oben formulierten Anforderungen zugrunde gelegt. Dabei konnten die funktionalen und die nichtfunktionalen Anforderungen vollständig erfüllt sowie die Rahmenbedingungen eingehalten werden.

Konzept

Das INSIKA-System basiert auf einer digitalen Signatur jeder Buchung. Diese Signatur wird von einer Smartcard erzeugt. Zudem sorgt die Smartcard für die fortlaufende Nummerierung der Buchungen. Die Signatur wird auf dem zugehörigen Beleg abgedruckt und mit den Buchungsdaten dauerhaft gespeichert.[20] Im Falle einer Prüfung werden die signierten Buchungsdaten in einem vorgegebenen Format bereitgestellt, z. B. durch einen Datenexport. Damit wird Folgendes erreicht:

- Eine gültige Signatur auf dem Beleg ist der Nachweis dafür, dass die Buchungsdaten von der Smartcard signiert

18 „Fiskalboxen“ werden z. B. in Schweden (zusammen mit einer Verschlüsselung) und Belgien (mit digitalen Signaturen) eingesetzt. Eine auf Signaturen basierende Lösung ohne eine vertrauenswürdige Komponente wird in Portugal verwendet.

19 Dabei wird versucht, die Sicherheit eines Systems oder eines Verfahrens zu gewährleisten, indem seine Funktionsweise geheim gehalten wird. Kryptografische Systeme nach dem Stand der Technik verwenden veröffentlichte Verfahren – nur die Schlüssel müssen geheim bleiben.

20 In den meisten Ländern müssen Registrierkassen ohnehin alle Buchungsdaten speichern, so dass beim Einsatz von INSIKA lediglich einige wenige Daten hinzukämen.

Missverständnisse: Sicherheit

„Ein komplexes System ist sicherer“

Viele – vor allem neuere – Fiskalsysteme sind hochkomplex.[1] Der einzige legitime Grund für diese Komplexität – und die damit unweigerlich verbundenen Kostensteigerungen – kann nur die Erfüllung der im Vorstehenden formulierten Anforderungen sein.

Die Erfahrung mit verschiedensten technischen Systemen zeigt, dass Komplexität die Fehlerwahrscheinlichkeit erhöht – und zwar überproportional, da nicht nur die Anzahl der Komponenten steigt, sondern auch deren Wechselwirkungen. Ein komplexes System enthält also i. d. R. mehr Fehler als ein weniger komplexes. Bei Sicherheitslösungen ist allerdings jeder Fehler eine potenzielle Sicherheitslücke.

Gute Sicherheitslösungen sind also gerade so komplex, wie es zur Erfüllung der Anforderungen nötig ist. Jegliche zu

1 Selbst für Außenstehende ist das am Umfang der entsprechenden Spezifikationen leicht erkennbar. Das belgische System ist auf über 100 Seiten beschrieben – trotzdem bleibt eine große Zahl von Detailfragen offen. Die Komplexität des Systems hat dazu beigetragen, dass der ursprüngliche Einführungstermin Januar 2011 mindestens um vier Jahre überschritten wird. Die Aufwendungen für Hersteller sind immens.

sätzliche Komplexität erhöht Aufwand und Kosten, während das Sicherheitsniveau abnimmt.

„Zusätzliche Sicherheitsmechanismen erhöhen die Sicherheit"

Jedes Sicherheitssystem ist als Kette verschiedener Maßnahmen anzusehen. Versagt ein einzelnes Glied der Kette, so ist das System insgesamt unsicher. Werden also nicht die schwächsten Glieder der Kette, sondern andere verstärkt, sind diese zusätzlichen Maßnahmen überflüssig und erhöhen lediglich Komplexität und Kosten.

Eine Kombination verschiedener Verfahren (z. B. digitale Signaturen und mechanisch gesicherter Speicher) kann nur dann sinnvoll sein, wenn das eine Verfahren die Schwäche eines anderen kompensiert. Hier ist dann allerdings immer die Frage zu stellen, ob der grundsätzliche Ansatz überhaupt sinnvoll ist.

„Es wird eine XYZ-Verschlüsselung benutzt – das Verfahren ist daher sicher"

Auf einem unsicheren kryptografischen Algorithmus lässt sich selbstverständlich kein sicheres System aufbauen. Heute steht allerdings eine Auswahl sicherer Methoden zu Verfügung, bei denen davon auszugehen ist, dass sie in absehbarer Zeit nicht gebrochen werden können.

In der Praxis basieren Sicherheitslücken jedoch i. d. R. auf einer unsauberen Architektur oder fehlerhaften Implementierung von Hard- und/oder Software. So lässt sich alleine aus der Verwendung eines sicheren Algorithmus (z. B. RSA oder ECDSA mit passenden Schlüssellängen zur Erstellung digitaler Signaturen oder AES für symmetrische Verschlüsselung) keine Aussage über die Sicherheit des Gesamtsystems ableiten. Wenn z. B. die privaten Schlüssel nicht ausschließlich in einer sicheren Hardware (wie z. B. einer geeigneten Smartcard) gespeichert und angewendet werden, muss das Gesamtsystem als unsicher angesehen werden. Auch ein Schlüsselmanagement durch nicht vertrauenswürdige Stellen macht ein System grundsätzlich unsicher. „Naive" Implementierungen von Kryptografie entsprechen daher keinen hohen Sicherheitsstandards.

Alle bis heute bekannten, erfolgreichen Angriffe auf moderne kryptografische Verfahren haben nicht den Algorithmus angegriffen, sondern Schwachstellen in der Implementierung oder bewusst geschaffene „Hintertüren" genutzt.[2]

„Eine Zertifizierung garantiert Sicherheit"

Eine Zertifizierung bedeutet zuerst einmal nur, dass ein unabhängiger Dritter überprüft, ob z. B. ein technisches System bestimmte Anforderungen erfüllt. Die Tauglichkeit dieser Anforderungen und damit des zertifizierten Systems für einen bestimmten Zweck wird dabei nicht bewertet.

So kann z. B. eine Smartcard-Software gemäß Common Criteria geprüft und eine Registrierkasse durch einen Wirtschaftsprüfer testiert[3] werden. In beiden Fällen ist das System zertifiziert. Die Vertrauenswürdigkeit unterscheidet sich allerdings ganz erheblich.

Dass Zertifizierungen im Bereich von Registrierkassen keine Garantie für Sicherheit sind, belegen verschiedene Beispiele – in der ersten Jahreshälfte 2014 z. B. in Ungarn[4] und in Portugal[5].

„Besser etwas Sicherheit als gar keine"

In Diskussionen ist vor allem unter dem Aspekt der „politischen Durchsetzbarkeit" oft zu hören, dass die Einführung eines Teils der geplanten Maßnahmen „besser als nichts" sei. Bei Sicherheitslösungen hängt die Sicherheit jedoch davon ab, dass die Kette der verschiedenen Maßnahmen nicht unterbrochen ist – sobald sie das ist, wird das System wertlos. Wenn man z. B. Daten mit einer Signatur sichert, nachdem es bereits eine Möglichkeit zur Manipulation gab, ist diese Signatur ohne jeden Nutzen.

Die Einzelmaßnahmen erzeugen dann nur „Pseudosicherheit". Diese kann bewirken, dass ein Vertrauen in das System gesetzt wird, das nicht gerechtfertigt ist. Hinter dieser Pseudosicherheit lassen sich dann sogar Manipulationsverfahren verstecken.

Ein sauber konzipiertes Sicherheitssystem muss also immer so wie geplant implementiert werden – es eignet sich nicht für „politische" Kompromisse.

„Jedes technische System wird geknackt"

Kein System kann absolut sicher sein. Allerdings sind korrekt geplante und durchgeführte Implementierungen kryptografischer Sicherheitslösungen heute die sichersten Methoden, Daten zu schützen.

Wird die Funktionsweise eines Systems veröffentlicht und verwendet es Standardverfahren (z. B. Smartcard-Hardware, kryptografische Algorithmen) ist eine laufende Überprüfung der Sicherheit durch unabhängige Dritte möglich. Dadurch können eventuelle Schwächen schnell aufgedeckt und beseitigt werden.

2 Alle durch Edward Snowden bekannt gewordenen Informationen über die Angriffe der NSA auf kryptografische Verfahren legen nahe, dass moderne Verfahren grundsätzlich sicher sind, da immer (grundsätzlich vermeidbare) Schwachstellen in der Umsetzung genutzt wurden.

3 In Deutschland gemäß Prüfungsstandard 880 des IDW (Institut der Wirtschaftsprüfer) „Erteilung und Verwendung von Softwarebescheinigungen"

4 In Ungarn wurden die Lizenzen für zwei zertifizierte Fiskalsysteme zurückgezogen, da es in der Software „Hintertüren" gab (Quelle: http://www.pesterlloyd.net/html/1405betrugekassen.html)

5 Ende April 2014 berichtete der portugiesische Fernsehsender SIC über massiven Betrug mit zertifizierten Fiskalsystemen in der Gastronomie. Laut einer Schätzung der Finanzbehörden wären 40 % der Rechnungen manipuliert. Es wurde mehrfach die Aussage gemacht, dass Systeme ohne Manipulationsmöglichkeit unverkäuflich seien.

und nummeriert wurden – sie ist also der Nachweis der ordnungsgemäßen Erfassung. Eine fehlende oder ungültige Signatur ist umgekehrt der Beweis einer nicht ordnungsgemäßen Erfassung.
- Die Signatur macht jede Änderung an den Daten erkennbar
- An der Nummerierung kann erkannt werden, wenn Buchungen in der Aufzeichnung fehlen.
- Die Signatur erlaubt eine eindeutige Rückführung des Datensatzes auf den Besitzer der Smartcard.
- Umgekehrt kann der Nachweis erbracht werden, dass die Daten unverändert und vollständig sind.
- Summenzähler auf der Smartcard und in Tagesabschlüssen erlauben bei Datenverlusten die Ermittlung von Gesamtumsätzen für die Datenlücken.
- Die Sicherheit des Systems basiert ausschließlich auf den beschriebenen Mechanismen – es gibt daher zusätzlichen keine Auflagen und damit auch keine Zertifizierung für das Gesamtsystem.

Für eine weiter gehende Einführung in das INSIKA-System sind verschiedene Darstellungen am Ende dieses Dokuments aufgeführt.

Vorteile

Die erforderlichen Eingriffe in bestehende Registrierkassen sind minimal. Es muss lediglich beim Abschluss einer Transaktion mit der Smartcard kommuniziert werden, das Ergebnis auf dem Beleg gedruckt und zusammen mit den Buchungsdaten elektronisch abgespeichert werden. Der Nachweis darüber wird mit jedem signierten Beleg erbracht. Weiter gehende Auflagen und entsprechende Zertifizierungen sind daher nicht erforderlich. Trotzdem wird ein sehr hohes Sicherheitsniveau erreicht. Die Eingriffe in den Wettbewerb sind minimal, siehe Kasten „Analyse: Markteingriffe durch INSIKA“.

Umsetzung der Anforderungen

Die weiter oben formulierten Anforderungen werden vom INSIKA-System vollständig erfüllt. In der Übersicht auf der letzten Seite wird für jede Anforderung erläutert, wie sie umgesetzt wurde.

Praxiserfahrungen

Ab dem Jahr 2011 wurde INSIKA in der Stadt Hamburg in der Taxibranche eingeführt, begleitet durch eine Fördermaßnahme. Innerhalb von zwei Jahren haben drei Taxameter-Hersteller serienreife Produkte entwickelt, die seit Mitte 2012 in bisher 60 % der Hamburger Taxen (2.000 von 3.300) eingebaut wurden. Die Verkehrsgewerbeaufsicht und die Finanzverwaltung Hamburg sind vollständig einbezogen. Die Beantragung und Ausgabe der Smartcards erfolgt über die D-Trust GmbH, eine Tochtergesellschaft der Bundesdruckerei.

Parallel dazu wurden jeweils mehrmonatige Praxistests mit Registrierkassen durchgeführt. Dabei wurde die komplette Kette von der Installation bis zur Prüfung der gesicherten Daten durch die Finanzverwaltung abgedeckt.

In allen Fällen funktioniert das INSIKA-System wie spezifiziert. Die Praxistauglichkeit wurde damit eindeutig nachgewiesen.

Weiterführende Informationen

- INSIKA-Flyer (deutsch, englisch) – kurze Übersicht über das System: http://www.insika.de/images/stories/INSIKA/INSIKA_Flyer_DE_2013-04.pdf
- PTB-Bericht IT-18 „Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen/ INSIKA – Konzept, Umsetzung und Erprobung“, umfangreiche Einführung in das Thema INSIKA, gedruckte Version: NW-Verlag, ISBN 978-3-95606-001-4, online: http://dx.doi.org/10.7795/210.20130206a
- Huber, Reckendorf, Zisky: Die Unveränderbarkeit der (Kassen-) Buchführung nach §146 Abs. 4 AO im EDV-Zeitalter und INSIKA, BBK Nr. 12 bis 14, NWB Verlag, 2013
- Die INSIKA-Spezifikation kann nach einer Registrierung unter http://www.insika.de/de/spezifikationen abgerufen werden

Kontakt:

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D – 31515 Wunstorf
eMail: info@insika.de

Das INSIKA-Projekt wurde vom Bundesministerium für Wirtschaft und Technologie unter dem Kennzeichen MNPQ 11/07 gefördert.

Anforderung	Umsetzung im INSIKA-Verfahren
Integrität sicherstellen	Jede Veränderung an den Daten ist anhand von Signatur und Sequenznummer eindeutig erkennbar.
Authentizität sicherstellen	Jede Signatur ist eindeutig auf den jeweiligen Steuerpflichtigen zurückzuführen.
End-to-end-Absicherung	Die Daten werden bei der Belegerstellung signiert und sind ab diesem Zeitpunkt bis zur Prüfung abgesichert.
Ausmaß von Veränderungen abschätzbar machen	Durch Summenzähler (in der Smartcard und in den Tagesabschlüssen) können die Gesamtumsätze für Datenlücken ermittelt werden.
Kontrollmechanismus bereitstellen	Die Signatur auf dem Beleg erlaubt eine Kontrolle.
Datensicherheit gewährleisten	Die signierten Daten können ohne Sicherheitsprobleme beliebig kopiert und damit gesichert werden.
Fehlertoleranz	Eine Beschädigung von Daten beeinträchtigt jeweils nicht die Prüfbarkeit und Aussagekraft der anderen Daten. Über Summenzähler können Fehler kompensiert werden.
Geringe Komplexität	Das INSIKA-System besteht lediglich aus dem definierten Prozess, der Smartcard mit ihrer Schnittstelle und dem Export-Datenformat.
Vertrauenswürdiger Teil des Systems möglichst klein	Nur die Smartcard und die ausgebende Stelle bilden die vertrauenswürdigen Komponenten des INSIKA-Systems.
Evaluierbarkeit	Durch die Verwendung hochsicherer Standardverfahren (Smartcard, ECDSA[21], PKI[22]), für die es teilweise bereits Evaluierungen gibt, ist eine Evaluierung nach höchsten Sicherheitsstandards möglich.
Einfache Kontrollen	Eine Kontrolle erfordert nur einen Beleg (und den Zugriff auf die Zertifikatsdaten), jedoch keinen Zugriff auf die Daten des Systems, das diesen Beleg erzeugt hat. Speziell mit einem QR-Code für die Belegdaten ist die Prüfung fast vollautomatisch möglich.
„Minimal-invasiv“	INSIKA erfordert nur eine sehr einfache Kommunikation mit der Smartcard sowie die Aufzeichnung und den Ausdruck einiger zusätzlicher Daten. Alle anderen Aufzeichnungspflichten bestehen ohnehin schon.[23]
In möglichst viele Systeme integrierbar	Durch die sehr einfachen Hard- und Software-Schnittstellen ist die Wahrscheinlichkeit, dass INSIKA in ein bestehendes System integriert werden kann, maximiert worden.
Eindeutig spezifizierte Schnittstellen	Die Smartcard-Schnittstelle sowie das Export-Datenformat sind präzise spezifiziert.
Möglichst geringe Abhängigkeit von bestimmten Technologien	Bis auf die Verwendung einer Smartcard setzt INSIKA auf keine bestimmte Technologie wie z. B. USB-Schnittstellen, SD-Karten, Internetprotokolle usw. auf. Für geeignete Smartcard-Hardware, die Softwareentwicklung sowie geeignete PKI-Dienstleistungen sind verschiedene Anbieter verfügbar.[24]
Anpassbar an neue Sicherheitsstandards	Durch einen Wechsel der Smartcard und ggf. des Signaturverfahrens lässt sich das INSIKA-System bei Bedarf sehr einfach an neue Sicherheitsstandards anpassen.
Auswirkungen von Sicherheitslücken minimieren	INSIKA verwendet ein standardisiertes, offenes Signaturverfahren mit verschiedenen Schlüsseln pro Smartcard. Wenn ein einzelner Schlüssel kompromittiert wurde, ist die Sicherheit aller anderen Smartcards nicht gefährdet.
Kosten minimieren	Durch die Verwendung einer Smartcard, eine einfache Integration, den Wegfall von Zertifizierungen für Registrierkassen und die Upgrade-Möglichkeit für viele Altsysteme sind die Kosten auf ein absolutes Minimum reduziert.
Steuerrecht als gesetzlichen Rahmen berücksichtigen	Da INSIKA vor allem ein Verfahren ist und kein spezifisches Gerät, lässt es sich geradlinig in bestehende Steuergesetzgebung einarbeiten. Es werden im Wesentlichen zusätzliche Anforderungen an Belege und an die darauf basierenden digitalen Aufzeichnungen gestellt.
Wettbewerbsverzerrung vermeiden	Die einfache Integration, die daraus resultierenden geringen Entwicklungsaufwendungen sowie der Verzicht auf Zertifizierungen minimieren den Eingriff in den Wettbewerb. Eine ausführliche Darstellung findet sich im Kasten „Analyse: Markteingriffe durch INSIKA“.
Einbettung in ein Kontroll- und Prüfkonzept	INSIKA gibt einen genauen Rahmen für Prüfungen und Kontrollen vor. Die Verfahren dafür wurden Praxistests unterzogen.

21 ECDSA steht für „Elliptic Curve Digital Signature Algorithm“, ein Signaturverfahren, das eine sehr hohe Sicherheit bei relativ kurzen Signaturen und hoher Verarbeitungsgeschwindigkeit bietet und damit optimal für INSIKA geeignet ist.
22 PKI steht für „Public-Key-Infrastruktur“, im Zusammenhang mit INSIKA ist das ein System, das für die Ausgabe und Verwaltung von Smartcards und das Management der kryptografischen Schlüssel verantwortlich ist.
23 Das gilt z. B. für Deutschland, Österreich, die Niederlande und Frankreich.
24 Für den Praxiseinsatz müssen alle genannten Komponenten einen entsprechenden Evaluierungsprozess durchlaufen haben, damit eine behördliche Anerkennung möglich ist. Ein Anbieterwechsel ist also mit einem gewissen Aufwand verbunden – eine eventuell kritische Abhängigkeit von einzelnen Herstellern oder Dienstleistern besteht dadurch aber nicht mehr.

Analyse: Markteingriffe durch INSIKA

Rechte am INSIKA-Konzept

Das INSIKA-Konzept ist veröffentlicht und kann ohne Berücksichtigung von Lizenzen, Patenten o. Ä. genutzt werden[1]. Durch die Veröffentlichung ist eine nachträgliche Patentanmeldung durch „Trittbrettfahrer" ausgeschlossen. Es entstehen also keine Abhängigkeiten, Rechtsunsicherheiten oder Kosten.

Eine Analogie ist die Verwendung des XBRL-Formats für die E-Bilanz. Dafür nutzt die Finanzverwaltung einen Standard, der in Deutschland von einem Verein betreut wird.

➔ Hier ergeben sich keinerlei Markteingriffe.

Zentrale Stelle zur Ausgabe der Smartcards

Eine zentrale Ausgabe der Smartcards und die zentrale Verwaltung der kryptografischen Zertifikate sind nicht zwingend erforderlich. Eine Zusammenführung der Daten ist aber unumgänglich, damit der Antragsprozess sicher funktioniert und den Behörden alle ausgegebenen Karten bekannt sind. Zur Verringerung des Aufwands und der Kosten ist eine einzige zentrale Stelle jedoch sinnvoll. Die Regulierung dieser hoheitlichen Aufgabe wird so wesentlich einfacher. Die entsprechende Dienstleistung kann bei Bedarf ausgeschrieben werden. Eine dauerhafte Abhängigkeit von einem Monopol-anbieter kann nicht entstehen, da ein Wechsel relativ leicht möglich ist.

Vergleichbare, zentralisierte Aufgaben sind der Druck von Banknoten, die Produktion von Personalausweisen und Reisepässen oder der Fahrerkarten für digitale Tachographen. Eine dezentrale und entsprechend aufwändigere Lösung wurde bei der elektronischen Gesundheitskarte gewählt.

➔ Bei der Verwaltung der INSIKA-Smartcards handelt es sich um einen Prozess, der neu eingeführt wird. In einen bestehenden Markt wird daher nicht eingegriffen. Durch die erforderliche Regulierung ist bei der Vergabe der Aufgabe der zentralen Stelle kein uneingeschränkter Wettbewerb möglich. Monopol-Situationen und Abhängigkeiten sind allerdings leicht vermeidbar.

Prüfsoftware

Zur Prüfung von INSIKA-Daten durch die Finanzbehörden, aber auch durch Anwender, Steuerberater oder Wirtschaftsprüfer ist eine Software zur Verifikation der Daten und Belege erforderlich. Diese Software implementiert Verfahren und Abläufe, die in der veröffentlichten INSIKA-Spezifikation vollständig beschrieben und frei von Rechten Dritter sind. Es bestehen also keine Hindernisse, eine entsprechende Software zu implementieren. Bei der Prüfung durch die Behörden ist es erforderlich, dass diese den Hersteller der von ihnen verwendeten Software als vertrauenswürdig einstufen.

Eine Analogie ist die Software zur Datenanalyse durch die Finanzverwaltung, für die es verschiedene Anbieter gibt.

➔ Auch hier entstehen keinerlei Wettbewerbsbeschränkungen.

Einbindung der Smartcard in Registrierkassen, Taxameter und andere Systeme

Die Hersteller der betroffenen Systeme müssen diese so anpassen, dass die INSIKA-Smartcard angesteuert sowie die gelieferten Daten ausgedruckt und gespeichert werden. Dies ist im Vergleich zu jedem anderen Fiskalsystem ein sehr kleiner Eingriff in die Produkte. Auch in Relation zu den meisten anderen Auflagen im Bereich elektronischer Buchführungssysteme handelt es sich bei INSIKA um eine einfach umzusetzende Anforderung. Im Gegensatz zu den meist sehr allgemein gehaltenen Anforderungen an Buchführungssysteme (etwa durch GoBS und GDPdU) liegt ein wesentlicher Vorteil von INSIKA in der (systembedingten) Genauigkeit der Spezifikation. Es kann keine Interpretationsspielräume und Zweifel über die Auslegung geben; das reduziert den Aufwand erheblich. In anderen Wirtschaftsbereichen sind regulatorische Eingriffe weitaus massiver.

Vergleichbare oder größere regulatorische Eingriffe sind die Pflicht zur Nutzung digitaler Tachographen, das Toll-Collect-Mautsystem sowie die Verwendung geeichter Waagen, geeichter Strom- und Wasserzähler, Smart-Meter usw.

Konventionelle Fiskallösungen sind durch ihre massiven Eingriffe in die Systeme und die erforderliche Zertifizierung jeder Weiterentwicklung sehr innovationsfeindlich. Für INSIKA hingegen gilt das nicht aufgrund der minimalen Eingriffe und der nicht erforderlichen Zertifizierungen. Da keine Ressourcen für den Umgang mit unklaren behördlichen Vorgaben und den daraus resultierenden Problemen aufgewendet werden müssen, wird stattdessen sogar die Entwicklung von Produktinnovationen gefördert.

➔ Die Verpflichtung zur Integration der Smartcards stellt einen Eingriff in den Markt dar. Im Vergleich zu vielen anderen regulatorischen Eingriffen (auch im Bereich der Buchführung) ist dieser als sehr klein einzustufen.

1 Die Markenrechte für „INSIKA" liegen beim ADM e.V. Es handelt sich um einen Projektnamen, der bei der Anwendung des Verfahrens nicht verwendet werden muss. Falls es doch beabsichtigt ist, lassen sich Nutzungsrechte vertraglich vereinbaren.)

Standardisiertes Datenformat

Beim Zugriff auf die signierten INSIKA-Daten ist ein Datenformat vorgegeben. Dies ist erforderlich, da eine kryptografische Verifikation nur mit einer exakten Festlegung der Inhalte und Formate möglich ist. Diese Festlegung betrifft ausschließlich das endgültige Format der Daten, also den Export aus dem System. Es bestehen keinerlei Auflagen für Inhalte, Verfahren und technische Lösungen innerhalb der IT-Systeme. Bis auf die signaturrelevanten Daten müssen bereits heute alle für INSIKA erforderlichen Daten gespeichert und verarbeitet werden.

Ähnliche Festlegungen gibt es bei der E-Bilanz und den ELSTER-Verfahren.

➔ Der Eingriff in den Markt bezieht sich ausschließlich auf das Datenformat für einen kleinen Teil der Daten (Bareinnahmen), die aufgrund bereits bestehender Vorschriften bei einer Betriebsprüfung vorzulegen sind. Eine konkrete Festlegung dieser Exportformate wird von den meisten Marktteilnehmern als Vorteil angesehen, da Auseinandersetzungen über die formale Korrektheit damit nicht mehr entstehen können.

Prozesse

Das INSIKA-Verfahren muss sich in die Prozesse der betroffenen Unternehmen einfügen. Diese bleiben dadurch aber unverändert. Die Pflichten zur Aufzeichnung, Verarbeitung, Archivierung und Bereitstellung der digitalen Aufzeichnungen bestehen bereits heute. Es sind lediglich kleine Erweiterungen (Beantragung, interne Verwaltung und Einsatz der Smartcards) erforderlich, die aber alle keine grundsätzlichen Eingriffe in bestehende Strukturen darstellen.

Vergleichbar ist das beispielsweise mit den regelmäßigen Anpassungen der Pflichtangaben auf Rechnungen. Auch hier bleiben die Abläufe selbst unverändert, lediglich die Inhalte sind an neue Vorschriften anzupassen.

➔ Unternehmensprozesse werden durch INSIKA nur minimal berührt. Eine Wettbewerbsverzerrung kann dadurch nicht erfolgen.

Kostenbelastung für Steuerpflichtige

Die Einführung von INSIKA verursacht Kosten zur Anpassung bestehender Systeme und für die Anschaffung der Smartcards. Eine geringfügige Verteuerung neuer Systeme kann nicht ausgeschlossen werden. Die Kostenbelastung pro Kassenplatz liegt je nach Ausgangssituation in einem Bereich von deutlich unter hundert bis zu mehreren hundert Euro. Laufende Kosten entstehen nicht. Durch vereinfachte Außenprüfungen und weniger Dokumentationsaufwand (Verfahrensbeschreibungen, Kassenberichte usw.) ist „unter dem Strich" sogar mit einer Kostenreduktion zu rechnen.

Vergleichbar ist dies mit jeglicher behördlichen Auflage für Unternehmen, die Kosten verursacht, z. B.: Umweltschutz, Arbeitsschutz, Arbeitnehmerrechte, statistische Meldepflichten, Änderungen im Steuerrecht und diversen Dokumentationspflichten.

➔ Im Vergleich zu den meisten anderen behördlichen Auflagen für Unternehmen sind die durch INSIKA verursachten Kosten minimal. Es sind sogar deutliche Kosteneinsparungen möglich.

EU-Recht

Bei fast jeder nationalen Gesetzgebung sind die Regelungen der europäischen Union zu berücksichtigen. Entsprechende Fragen stellen sich auch bei jedem steuerrechtlichen – also rein nationalen – Eingriff in die Wirtschaft. Beschränkt man sich dabei auf technische Systeme, ist dies vergleichbar mit der Verpflichtung der Anbieter von Buchführungs-, Lohnabrechnungs-, Personalzeiterfassungssoftware und ähnlichen Produkten, das jeweilige nationale Recht abzubilden.

Bei den in den letzten Jahren erfolgten Einführungen der erheblich aufwändigeren Fiskalsysteme in Schweden, Portugal, Belgien, Ungarn und Kroatien stand man dabei vor denselben Fragen. Teilweise wurde hier das sog. 98/34-Verfahren[2] angewendet, teilweise erfolgte die Einführung rein national. Wettbewerbsrechtliche Probleme sind nicht bekannt geworden.

➔ Die Berücksichtigung nationaler, steuerrechtlicher Anforderungen stellt für Anbieter entsprechender Systeme den Regelfall dar, so dass keine unüblichen Markteingriffe erkennbar sind.

Gesamtbetrachtung

Im Vergleich zu vielen anderen regulatorischen Eingriffen des Gesetzgebers bzw. der Verwaltungen stellt das INSIKA-System einen minimalen Eingriff in den Wettbewerb dar. Jeder bekannte Alternativansatz zur sicheren Dokumentation von Bargeschäften ist entweder weitgehend wirkungslos oder hat weitaus größere Eingriffe in den Wettbewerb zur Folge.

2 Mit den Richtlinien 83/189/EWG und 98/34/EG wurde ein Verfahren geschaffen, durch das sich die Mitgliedstaaten gegenseitig und die Kommission vor der Annahme technischer Vorschriften informieren und ihre Entwürfe erforderlichenfalls ändern. Eine entsprechende Notifizierung erfolgte bei den schwedischen und ungarischen Fiskalsystem-Einführungen, bei den anderen genannten erfolgte sie nicht.