INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Wie werden Registrierkassen und Taxameter sicher?

Stand: 9. September 2015

In der Diskussion über sichere Registrierkassen, Taxameter und ähnliche Systeme (hier der Einfachheit halber alle als „Registrierkassen“ bezeichnet) ist oft unklar, was in diesem Zusammenhang genau unter „**Sicherheit**“ zu verstehen ist und wie man diese herstellen kann. Diese Unklarheiten führen teilweise zu unzulässig vereinfachten oder falschen Argumenten.

Die Sicherheitsanforderungen ergeben sich direkt aus der Abgabenordnung. Unter Sicherheit ist nicht nur der Schutz gegen nachträgliche Manipulationen zu verstehen. Sehr wichtig sind die Maßnahmen zur Sicherstellung einer korrekten Erfassung.

Im Folgenden wird dargestellt, wie Registrierkassen gegen Angriffe geschützt werden müssen und wie die Umsetzung in der Praxis erfolgen kann.

Anforderungen aus der Abgabenordnung

Mit Registrierkassen erzeugte Daten und Belege unterliegen in Deutschland den Regelungen der Abgabenordnung, die an diese Aufzeichnungssysteme weitgehend dieselben Anforderungen stellt wie an elektronische Buchführungssysteme. Im Einzelnen sind das:

§146 Abs. 1 (Erfassung, Aufbewahrung)

*Die Buchungen und die sonst erforderlichen Aufzeichnungen sind **vollständig**, **richtig**, **zeitgerecht** und **geordnet** vorzunehmen.*

Diese Anforderungen wirken sich auf die **Erfassung** der Daten und deren **Aufbewahrung** aus.

Konzentriert man sich nur auf die sichere Aufbewahrung, d.h. die Speicherung der Daten, werden die gesetzlichen Anforderungen nicht erfüllt.

§146 Abs. 4 (Aufbewahrung)

*Eine Buchung oder eine Aufzeichnung **darf nicht** in einer Weise **verändert werden**, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.*

Aufzeichnungen müssen also **unveränderbar** sein.

Dies betrifft vor allem die Phase der **Aufbewahrung** der Daten.

§146 Abs. 5 (Prüfung)

*[...] muss insbesondere sichergestellt sein, dass während der Dauer der Aufbewahrungsfrist die Daten **jederzeit verfügbar** sind und **unverzüglich lesbar** gemacht werden können.*

Hierdurch soll die **Prüfbarkeit** der Daten sichergestellt werden.

Wesentliche Sicherheitsrisiken

Welche Angriffe muss ein sicheres System verhindern bzw. zu verhindern helfen?

Risiken bei der Erfassung

Anforderung „**vollständig**“

Risiko: Nicht-Eingabe, unvollständige Eingabe, Daten einer oder mehrere Registrierkassen werden unterdrückt

Anforderung „**richtig**“

Risiko: Falscheingabe (z.B. unrichtige Beträge, Mengen, Bezeichnungen, Steuersätze)

Anforderung „**zeitgerecht**“

Risiko: Verspätete Erfassung (ggf. in Kombination mit unvollständiger oder falscher Erfassung)

Anforderung „**geordnet**“

Risiko: Eine „ungeordnete“ Erfassung ist mit einem elektronischen System nicht möglich – die Daten könnten allerdings so geordnet oder strukturiert sein, dass sie für Dritte nicht nachvollziehbar, also nicht prüfbar sind.

Risiken bei der Aufbewahrung

Falls die Daten **nicht unveränderbar** sind, können sie beliebig unerkannt manipuliert werden. In diesem Fall können alle bei der Erfassung möglichen Angriffe auch im Nachhinein erfolgen.

Risiken bei der Prüfung

Aufzeichnungen müssen im Rahmen des Datenzugriffsrechts **jederzeit verfügbar** sein und **unverzüglich lesbar** gemacht werden können.

Direkte Sicherheitsrisiken entstehen hier nicht – in der Praxis kommt es aber vor, dass Daten ent-

weder gar nicht vorgelegt werden oder dass es Auseinandersetzungen über die Prüfbarkeit der Daten gibt (sowohl in Bezug auf die Form als auch auf den Inhalt).

Voraussetzungen für Sicherheit

Bei hinreichend hoher krimineller Energie ist jedes Sicherheitssystem überwindbar, durch Hard- oder Softwaremanipulation aber auch durch „social engineering" bis hin zur Korruption. Es kann keine absolute Sicherheit geben. Deshalb gilt es, das Restrisiko auf ein für alle Beteiligten akzeptables Maß zu verringern.

Die technische Seite einer Sicherheitslösung allein kann **niemals** die **Eingabe** eines jeden Geschäftsvorfalls in das System **erzwingen**. Technische Schutzvorkehrungen bedürfen daher stets der Ergänzung durch:

- organisatorische Maßnahmen,
- hinreichend hohe Kontrolldichte sowie
- ausreichenden Sanktionsdruck bei Verstößen.

Folglich erfordert jede taugliche Sicherheitslösung einen ganzheitlichen Ansatz. Bereits kleine, unsachgemäße Veränderungen am Konzept können die Sicherheit des Gesamtsystems zerstören.

Es ist zu unterscheiden zwischen **Kontrollen**, also der laufenden Steueraufsicht (z.B. durch Kassennachschauen) sowie **Prüfungen**, die sich auf die Vergangenheit beziehen (z.B. durch Betriebsprüfungen).

Im Folgenden sind die wesentlichen Voraussetzungen für sichere Systeme beschrieben.

Einsatzpflicht

Effektive Kontrollen und Prüfungen setzen voraus, dass jede eingesetzte Registrierkasse mit einer anerkannten Sicherheitseinrichtung ausgestattet ist. Ein **nicht genutztes** oder ein System **ohne Sicherheitseinrichtung** muss als **Verstoß** gewertet werden. Nur so schaffen Kontrollen Sicherheit, die als Basis für spätere Prüfungen dienen kann.

Zentrales Verzeichnis der Systeme

Sinnvolle Kontrollen und Prüfungen setzen voraus, dass der prüfenden Stelle alle bei einem Steuerpflichtigen eingesetzten Registrierkassen bekannt sind. Nur so kann überprüft werden, ob **alle** Systeme **korrekt genutzt** werden und ob die Daten **aller** Registrierkassen **vorgelegt** wurden.

Ob dazu die Registrierkassen oder nur die eingesetzten Sicherheitseinrichtungen zentral erfasst werden, spielt hier keine Rolle.

Belegpflicht

Die Verpflichtung des Unternehmers, über jeden Geschäftsvorfall einen Beleg auszugeben, ist Voraussetzung für eine jederzeitige effiziente Kontrolle. Dieser Beleg muss dazu einen eindeutigen und sicheren **Nachweis** über die **korrekte Erfassung** beinhalten.

Diese Anforderung kann auch mit elektronischen Belegen erfüllt werden; diese müssen aber kontrollfähig sein (das bedingt allerdings Standardisierungen für Form, Inhalt und Zugriffsverfahren, die bisher bei Registrierkassen nicht und im Taxameter-Bereich nur in Ansätzen vorhanden sind).

Kontrollen der korrekten Erfassung

Kontrollen der korrekten Erfassung der Geschäftsvorfälle müssen in einer ausreichenden Anzahl erfolgen, um ein „Entdeckungsrisiko" zu schaffen. Voraussetzung dafür ist, dass diese Kontrollen **einfach und schnell** erfolgen können sowie ein **verlässliches Resultat** ergeben.

Unveränderbare Speicherung

Wenn Geschäftsvorfälle einmal korrekt erfasst sind, dürfen **keine Veränderungen** mehr **möglich** sein oder müssen zweifelsfrei erkannt werden können.

Vertrauensbasis

Die Sicherheit von IT-Systemen basiert zu einem großen Teil auf Vertrauen. Da fast alle Personen, die mit dem System in Berührung kommen, dessen Sicherheit nicht selbst überprüfen können, müssen sie auf Aussagen Dritter über die Sicherheit des Systems vertrauen.

Es muss also eine **Bewertung der Sicherheit**, der alle Beteiligten in hohem Maße vertrauen können, **möglich und vorhanden** sein.

Rechtssicherheit

Heute kann (fast) nur die Finanzverwaltung den Steuerpflichtigen **Verstöße** nachweisen.

Ein belastbarer **Nachweis der Ordnungsmäßigkeit** der Aufzeichnungen durch Steuerpflichtige ist heute **grundsätzlich nicht möglich**!

Ein sicheres Verfahren kann mithin nur dann als sinnvoll gelten, wenn es **Rechtssicherheit für alle Beteiligten** schafft.

Umsetzung im INSIKA-System

Signaturerstellungseinheit als Sicherheitsanker

Ein zentrales Sicherheitselement bei INSIKA ist die elektronische Signatur jedes Geschäftsvorfalls. Diese Signaturen werden von einer sicheren Signaturerstellungseinheit erzeugt. Sie ist der Sicherheitsanker des Gesamtsystems.

Durch die eindeutige Zuordnung der Signaturerstellungseinheit auf einen Steuerpflichtigen, die verwendeten kryptografischen Algorithmen und Kontroll- sowie Prüfverfahren können Integrität (Daten unverändert und vollständig) und Authentizität (gesicherter Herkunftsnachweis) der Daten sichergestellt werden.

In der Praxis finden heute Smartcards als Signaturerstellungseinheit Verwendung. Registrierkassen können mit relativ geringem Aufwand um einen Smartcardleser oder die Möglichkeit des Zugriffs auf einen solchen ergänzt werden.

Sicherheit bei der Erfassung

Das INSIKA-Verfahren sieht vor, dass zu jedem Geschäftsvorfall ein signierter Beleg auszugeben ist. Die Korrektheit der Signatur ist jederzeit leicht prüfbar. Die Signatur ist der eindeutige Nachweis der korrekten Erfassung.

Sicherheit bei der Aufbewahrung und Prüfung

Jede Veränderung in einem Datensatz ist anhand der Signatur eindeutig erkennbar.

Die Umsätze jedes signierten Geschäftsvorfalls werden zusätzlich in geschützten Summenspeichern der Signaturerstellungseinheit abgelegt. So stehen selbst beim Verlust gespeicherter Daten noch vertrauenswürdige Umsatzwerte zur Verfügung.

Die Umsatzdaten können sowohl in den Registrierkassen als auch bei der nachgelagerten Speicherung in beliebigen Formaten abgelegt werden. Das bietet den Vorteil einer vollständigen Wahlfreiheit der Speicherverfahren. Lediglich für die Prüfung sind die Daten in ein standardisiertes Prüfformat zu übertragen.

Vertrauensbasis und Rechtssicherheit

Das INSIKA-Verfahren verwendet eine Kombination von sicherheitstechnischen Standardmethoden:

Zum einen werden bekannte und etablierte kryptografische Algorithmen eingesetzt.

Zum anderen kommen Smartcards zum Einsatz. Diese bieten als zertifizierte Komponenten das höchste derzeit erreichbare Sicherheitsniveau für Anwendungen, bei denen eine große Zahl von Signaturerstellungseinheiten benötigt wird.

Im Zusammenhang mit den beschrieben organisatorischen Maßnahmen sowie einem geeigneten gesetzlichen Rahmen bietet das INSIKA-Verfahren ein so hohes Vertrauensniveau, das damit erstmalig eine Rechtssicherheit für alle Beteiligten – vor allem auch für die Anwender – geschaffen werden kann.

INSIKA und ADM e.V.

INSIKA („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 konzipiert, entwickelt und erprobt. Seit erfolgreichem Projektabschluss werden das Konzept und 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 den aufwändigen konventionellen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

Kontakt

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

www.insika.de
E-Mail: info@insika.de