Bundesamt
für Sicherheit in der
Informationstechnik

Gesetzesentwurf zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen

—

Stellungnahme des BSI

Datum: 12. Oktober 2016

1 Einleitung

Nachträgliche Manipulationen an ungesicherten digitalen Aufzeichnungen elektronischer (Kassen-)Systeme sind heutzutage in der Regel nicht oder nur äußerst schwer feststellbar. Um Manipulationen an solchen Aufzeichnungen zu verhindern sind daher geeignete technische Schutzmaßnahmen notwendig.

Im Juli 2016 hat die Bundesregierung daher einen Gesetzesentwurf zum Schutz vor Manipulationen digitalen Grundaufzeichnungen beschlossen.

Der Gesetzesentwurf sieht eine Kombination von technischen und organisatorischen Maßnahmen zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vor:

- *Aufzeichnungspflicht*: Steuerrelevante Aufzeichnungen müssen einzeln, vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.
- *Einführung einer zertifizierten technischen Sicherheitseinrichtung*: Digitale Aufzeichnungen durch elektronische Aufzeichnungssysteme sollen durch eine zertifizierte technischen Sicherheitseinrichtung geschützt und ein Speichermedium gesichert sowie für Kassen-Nachschauen verfügbar gehalten werden.
- *Einführung einer Kassen-Nachschau*: Zur Prüfung der Ordnungsmäßigkeit der Aufzeichnungen können Finanzbehörden unangekündigte Kassen-Nachschauen durchführen.

Der Gesetzesentwurf sieht hierbei nicht den Einsatz einer konkreten technischen Lösung vor, sondern ist bewusst technologieoffen gehalten. Hiernach werden im Rahmen einer Technischen Verordnung sowie untergeordneten Technischen Richtlinien und Schutzprofilen technikneutrale Mindestanforderungen entsprechend des Stands der Technik an die Sicherheit und Interoperabilität der technischen Sicherheitseinrichtung definiert. Technische Vorgaben müssen hierbei nur festgelegt werden, soweit dies zur Sicherung der Interoperabilität – insbesondere zur Ermöglichung von Kassenprüfungen - notwendig ist. Die Einhaltung der Anforderungen wird im Rahmen eines Zertifizierungsverfahrens geprüft und durch ein Zertifikat des BSI bestätigt.

Konkrete technische Konzepte, wie das INSIKA-Verfahren, welches in einzelnen Bereichen in Pilotprojekten erprobt wurde, sowie technische Lösungen, die aufgrund von Gesetzesinitiaven anderer Staaten entwickelt wurden, stehen somit nicht im Widerspruch zu dem Zertifizierungsverfahren. Diese verschiedenen technischen Umsetzungen sind, ggf. mit geringfügigen Anpassungen zur Erhöhung des Sicherheitsniveaus, nach einer erfolgreichen Zertifizierung geeignet, die Anforderungen im Sinne des Gesetzentwurfs zu erfüllen,

1.1 Technische Sicherheitseinrichtung

Der zentrale technische Baustein zur Umsetzung des Gesetzesentwurfs ist die technische Sicherheitseinrichtung. Diese besteht gemäß Gesetzesentwurf aus einem Sicherheitsmodul, einem Speichermedium und einer digitalen Schnittstelle. Die Sicherung erfolgt hiernach zusammenfassend wie folgt:

Für jede Aufzeichnung eines steuerrelevanten Geschäftsvorfalls muss von dem elektronischen Aufzeichnungssystem unmittelbar eine neue Transaktion gestartet werden. Hierzu werden die relevanten Vorgangsdaten über die digitale Schnittstelle an die technische Sicherheitseinrichtung übergeben.

Das Sicherheitsmodul vergibt für jede Transaktion eine eindeutige, fortlaufende Transaktionsnummer. Diese muss so beschaffen sein, dass Lücken in den Aufzeichnungen erkennbar sind. Darüber hinaus legt das Sicherheitsmodul Beginn und Ende der Transaktion fest und erzeugt einen Prüfwert für die Transaktion. Die Festlegung der Daten des Transaktion durch das Sicherheitsmodul muss hierbei manipulationssicher sein. Zudem muss das Sicherheitsmodul über eine geeignete Zeitquelle zur Bestimmung von Beginn und Ende eines Vorgangs verfügen.

Schließlich werden die geschützten Transaktionsdaten auf dem nichtflüchtigen Speichermedium gespeichert. Die gesicherten Transaktionsdaten können über die digitale Schnittstelle auch in ein externes Aufbewahrungssystem übertragen werden.

Im Falle einer Kassen-Nachschau kann die durchführende Finanzbehörde die relevanten geschützten Aufzeichnungen dann einfordern und mittels eines Prüfwerkzeugs auf Vollständigkeit und Authentizität prüfen. Hierbei können nachträgliche Änderungen erkannt werden. Zusätzlich kann etwa im Rahmen von Testkäufen geprüft werden, ob die gekauften Artikel mit dem Kassensystem verbucht werden.

2 Stellungnahme

Um einen wirksamen Schutz gegen Manipulationen an digitalen Grundaufzeichnungen zu erreichen, ist es aus Sicht des BSI unerlässlich, dass die technischen Einrichtungen zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen einem geeigneten einheitlichen Mindestniveau an Vertrauen und Sicherheit genügen müssen.

Die Eignung der jeweiligen Sicherheitsmaßnahmen ist hierbei stark davon abhängig, welchem Angriffpotential die jeweiligen Lösungen ausgesetzt sind. So können Angriffe auf technische Sicherheitseinrichtungen von Registrierkassen Manipulationen an Kassenaufzeichungen ermöglichen, welche zu systematischen Steuerbetrug genutzt werden könnten. Bei einem flächendeckenden, gesetzlich verpflichtenden Einsatz von technischen Sicherheitseinrichtungen in Registrierkassen ist daher davon auszugehen, dass nicht unerhebliche finanzielle und zeitliche Aufwände in Kauf genommen werden, um gezielt nach Schwachstellen in technischen Sicherheitseinrichtungen zu suchen, da es einen ausreichend großen Markt für Verfahren zur Umgehung der Sicherheitsmaßnahmen geben dürfte. Hierdurch ergibt sich ein hohes Angriffspotential.

Hierbei ist zu betonen, dass Angriffe auf technische Systeme in der Regel Schwachstellen ausnutzen, welche nicht in der Architektur des Systems an sich liegen, sondern auf Fehler in der Implementierung oder der mangelhaften Umsetzung von Sicherheitsmaßnahmen zurückzuführen sind.

Daher ist eine unabhängige und systematische Prüfung gemäß des Stands der Technik sowie der Bestätigung des erforderlichen Sicherheitsniveaus durch ein standardisiertes Zertifizierungsverfahren in jedem Fall notwendig.

Das Zulassen von konkreten Verfahren als Sicherheitseinrichtung (zusätzlich oder alternativ) ohne Zertifizierung, würde hingegen ein undefiniertes Schutzniveau nach sich ziehen. Ein erfolgreicher Pilotbetrieb kann kein Zertifizierungsverfahren ersetzen, da sich bei einem flächendeckenden Einsatz von technischen Sicherheitseinrichtungen in Registrierkassen sich eine ungleich höhere Gefährdung ergibt.

Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik ist der Gesetzesentwurf geeignet, die gesteckten Ziele zu erreichen. Durch die Technologieoffenheit sollte es nach Einschätzung des BSI für Hersteller möglich sein, existierende Komponenten (wie INSIKA-Komponenten) einzusetzen, oder diese zügig und gezielt fortzuentwickeln, und zertifizieren zu lassen, so dass die gesetzlichen Anforderungen eingehalten werden können und entsprechende zertifizierte Sicherheitseinrichtungen zeitnah am Markt verfügbar sind.

Ein weiterer Vorteil des Zertifizierungsverfahrens liegt in der Möglichkeit innovative Lösungen zu fördern. Während z.B. INSIKA derzeit eine aufwändige Infrastruktur zur Zuordnung von technischen Sicherheitseinrichtungen zu Steuerpflichtigen erfordert, die zunächst aufgebaut und von staatlicher Seite betrieben werden müsste, ist dieses beim Zertifizierungsverfahren in der Form nicht notwendig. Anstelle dessen entwickelt der Hersteller der technischen Sicherheitseinrichtung ein für das jeweilige Verfahren angepasstes Personalisierungskonzept, das eine eindeutige Zuordnung zum Steuerpflichtigen ermöglicht und im Rahmen des Zertifizierungsverfahren geprüft wird. Dadurch entsteht ein Wettbewerb zwischen den Herstellern, was letztlich zu kostengünstigen Lösungen führen wird.