Aktuelle Praxisprobleme beim Einsatz von cloudbasierten TSEs

Beim Einsatz von cloudbasierten zertifizierten technischen Sicherheitseinrichtungen (TSE) sind zusätzliche Sicherheitsmaßnahmen in der Anwenderumgebung umzusetzen (sog. Umgebungsschutz). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zu einem späten Zeitpunkt Ende 2020 neue Anforderungen an den Umgebungsschutz bekannt gegeben, deren Einhaltung erfolgen muss, um eine cloudbasierte TSE im Rahmen des jeweils erteilten Zertifikats zu betreiben. Hierdurch sollen Manipulationen durch den Steuerpflichtigen verhindert werden.

Welche Anforderungen sind im Zusammenhang mit der Anwenderumgebung zu erfüllen?

Ein Bestandteil der TSE ist die sog. SMAERS-Komponente (Security Module Application for Electronic Record-keeping Systems). Diese verwaltet die Transaktions-IDs und löst den Signaturprozess aus. Die SMAERS-Komponente muss ferner nach den Vorgaben des BSI in der physischen Einsatzumgebung des elektronischen Aufzeichnungssystems betrieben werden. Das BSI hat auf seiner Internetseite hierzu folgende Informationen veröffentlicht:

> *„Die physische Einsatzumgebung des Aufzeichnungssystems, im Sinne der Sicherheitsvorgaben, erstreckt sich auf den gesamten zusammenhängenden Bereich in der das Aufzeichnungssystem steht und für den der Betreiber des Aufzeichnungssystems unmittelbar verantwortlich ist.*
>
> *Der Betrieb der SMAERS-Komponente z. B. im Büro der Filiale, in dessen Verkaufsraum das Aufzeichnungssystem steht, ist konform.“*

Für den Umgebungsschutz sieht das BSI vor, dass dieser mit Hilfe eines TPM 2.0 (Trusted Platform Modul) sichergestellt wird.

Darüber hinaus dürfen keine Bestandteile der SMAERS von dem Steuerpflichtigen konfiguriert oder administriert werden. Dies kann in unterschiedlicher Form gewährleistet werden.

Welche Probleme bestehen aktuell im Zusammenhang mit der Umsetzung der Anforderungen in der Praxis?

- Die zertifizierte cloudbasierte TSE-Lösung eines Anbieters sieht ausweislich des Umgebungsschutzkonzepts den Einsatz eines TPM 2.0 vor, das lokal betrieben werden muss. Der Einsatz eines TPM 2.0 kann nicht in Kombination mit allen Betriebssystemen verwendet werden. Dies gilt insbesondere in Bezug auf iOS. In diesen Fällen wird eine zusätzliche Hardware benötigt, auf der das TPM 2.0 implementiert wird. Häufig bietet sich die Installation der SMAERS-Komponente auf dem Filial-Server an.

  Der Anbieter hatte vor dem zuvor geschilderten Hintergrund eine softwarebasierte Lösung (White Box Cryptografie) evaluiert und Vorbereitungen zur Zertifizierung begonnen. Die Software-basierte Lösung war in der Praxis als sinnvollere technische Umsetzung eingeordnet worden. Entsprechend haben eine Vielzahl von Steuerpflichtigen auf diese Lösung gesetzt. Im Laufe der Abstimmungen mit dem BSI wurde dem Anbieter Anfang 2022 mitgeteilt, dass für die White Box Cryptografie keine dauerhafte Zertifizierung erteilt werden würde, da eine TPM 2.0-Lösung als sicherer eingestuft wird. Eine nur übergangsweise Zertifizierung ergibt jedoch weder für den Anbieter noch für die Steuerpflichtigen Sinn. Die entsprechenden Aktivitäten in Bezug auf die Zertifizierung einer Software-basierten Lösung wurden daher durch den Anbieter eingestellt.

  In der Praxis sind nun insbesondere die folgenden Konstellationen festzustellen:

  - Die Anforderungen an den Umgebungsschutz wurden in Teilen umgesetzt, da der Steuerpflichtige statt der Implementierung eines TPM 2.0 auf die White-Box-Cryptografie-Lösung gesetzt hatte. Aufgrund des vom Anbieter implementierten zusätzlichen Schutzes durch eine weitere Integrationsschicht erfolgt jedoch zusätzlicher Schutz vor unerkannten Manipulationen.

    Die Implementierung eines TPM 2.0 ist aufgrund der angespannten Situation am Markt in Bezug auf die Lieferketten nicht zeitnah umsetzbar. Gleiches gilt auch für den Fall, dass eine zusätzliche Anschaffung weiterer Hardware erforderlich ist, um eine Implementierung der TPM 2.0 zu ermöglichen.

  - Die Anforderungen an den Umgebungsschutz wurden seitens des Steuerpflichtigen noch nicht umgesetzt. Dies kann z. B. aufgrund fehlender Kenntnisse der Anforderungen an den Umgebungsschutz der Fall sein. Jedoch werden auch in diesem Fall bereits die durch den Anbieter selbst erfüllbaren, systemimmanenten Schutzmaßnahmen umgesetzt. Das betrifft z. B. die unabhängige Administration der SMAERS-Komponente, Anforderungen an die Verschlüsselung der Kommunikation sowie Dokumentationsanforderungen.

- Beim Einsatz der cloudbasierten TSE-Lösung eines Anbieters bestehen zurzeit Rechtsunsicherheiten dahingehend, ob die Anforderungen „Betrieb der SMAERS-Komponente in der operativen Umgebung des elektronischen Aufzeichnungssystems“ erfüllt ist, denn die SMAERS-Komponente wird in der Cloud betrieben. Falls die SMAERS-Komponente nicht in der operativen Einsatzumgebung betrieben wird – z. B. lokale Kassenlogik wird mit einer zentralen SMAERS-Komponente verbunden – verliert die TSE ihre Zertifizierung.

Welche Konsequenzen können sich daraus ergeben, wenn die Anforderungen an den Umgebungsschutz nicht oder nicht vollständig umgesetzt sind?

Aktuell kann noch nicht sicher abgeschätzt werden, ob und in welcher Weise die fehlende (vollständige) Umsetzung der Anforderungen an die Anwenderumgebung aufgegriffen wird. Dies sollte aber nicht dazu verleiten, sich nicht mit dieser Thematik zu befassen, denn die folgenden Konsequenzen wären möglich:

Stellt der Finanzbeamte im Rahmen einer Kassen-Nachschau fest, dass die Anforderungen an den Umgebungsschutz nicht oder nicht vollständig umgesetzt wurden, wird er diesen formellen Mangel bewerten. Je nachdem ob er diesen allein als schwerwiegenden Mangel ansieht oder nicht und ob noch weitere formelle Mängel festgestellt wurden, kann dies die Grundlage dafür bilden, dass die Kassenbuchführung als nicht ordnungsgemäß verworfen wird. Das berechtigt den Finanzbeamten zur Durchführung einer Schätzung.

Ferner kann nicht ausgeschlossen werden, dass ein Ordnungswidrigkeitsverfahren eingeleitet und gemäß § 379 AO ein Bußgeld festgesetzt wird.

Was ist zu tun?

Empfehlenswert ist, zeitnah mit dem Kassenfachhändler bzw. dem IT-Dienstleister Kontakt aufzunehmen und zu klären, ob die Anforderungen an den Umgebungsschutz bereits vollständig umgesetzt worden sind. Ferner sollte der Steuerberater hinzugezogen werden, um ein weiteres Vorgehen zu erörtern. In Betracht kommt insbesondere die individuelle Antragstellung nach § 148 AO (Bewilligung von Erleichterungen) auf Gewährung einer Frist zur vollständigen Umsetzung der Anforderungen an den Umgebungsschutz. Falls ein entsprechender Antrag gestellt wird, ist in diesem begründet darzulegen, dass ein rein technischer Mangel vorliegt (warum, bis wann wird dieser abgestellt), die Aufzeichnungs- und Belegausgabepflichten vollständig, richtig und zeitgerecht erfüllt werden, die TSE-Pflicht bis auf die benannten technischen Mängel umgesetzt wurde und die Besteuerung keinesfalls gefährdet wird.

Wichtig ist, dass im Fall einer Kassen-Nachschau oder einer Betriebsprüfung eine vollständige Dokumentation vorgelegt und der Umsetzungsstand und die ggf. noch notwendigen Schritte erläutert werden können.