

DEUTSCHER INDUSTRIE- UND
HANDELSKAMMERTAG E. V.
Breite Str. 29
10178 Berlin

ZENTRALVERBAND DES
DEUTSCHEN HANDWERKS E. V.
Mohrenstr. 20/21
10117 Berlin

HANDELSVERBAND DEUTSCHLAND (HDE) E. V.
Am Weidendamm 1A
10117 Berlin

BUNDESVERBAND DER DEUTSCHEN
INDUSTRIE E. V.
Breite Str. 29
10178 Berlin

BUNDESVEREINIGUNG DER DEUTSCHEN
ARBEITGEBERVERBÄNDE E. V.
Breite Str. 29
10178 Berlin

BUNDESVERBAND GROSSHANDEL,
AUSSENHANDEL, DIENSTLEISTUNGEN E. V.
Am Weidendamm 1A
10117 Berlin

Leiterinnen und Leiter
der Steuerabteilungen der
Landesfinanzministerien

per E-Mail

25. Januar 2021

Fragen der Unternehmen zum aktuellen Stand bei der Zertifizierung von Cloud-TSE- Lösungen

Briefanrede,

mit Schreiben vom 15. Dezember 2020 hatten wir Sie über Probleme bei der Zertifizierung von cloudbasierten TSE-Lösungen informiert, die durch zusätzliche Sicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entstehen. Am 31. Januar 2021 läuft das Zertifikat der einzigen bisher zertifizierten cloudbasierten TSE der gemeinschaftlichen Anbieter Deutsche Fiskal und D-Trust GmbH aus. Nach unserer Kenntnis muss sowohl für die Re-Zertifizierung als auch für die erstmalige Zertifizierung weiterer Anbieter cloudbasierter Lösungen ein Umgebungsschutzkonzept vorgelegt werden, das die zusätzlichen Sicherheitsanforderungen berücksichtigt. Hintergrund dieser neuen, erhöhten Sicherheitsanforderungen ist, dass das BSI den Nutzer der TSE seit Juli 2020 als potenziellen Angreifer der TSE ansieht. Deshalb wird ein zusätzlicher Schutz gefordert, der aus unserer Sicht nur bei den Komponenten erfolgen kann, die beim Steuerpflichtigen selbst (Anwenderumgebung) installiert sind, nicht jedoch beim kryptografischen Kern, der vom TSE-Hersteller gehostet wird.

Unabhängig davon, ob man dieses „Angriffspotenzial“ als virulent bewertet oder nicht, stehen unsere Unternehmen vor folgendem Problem: Nach unseren Kenntnissen liegt bisher noch

keine abschließend durch das BSI erarbeitete allgemeine Spezifikation an die Anwenderumgebung vor. Neue Anforderungen durch die Hersteller im Rahmen der jeweiligen Erstellung und Umsetzung eines Umgebungsschutzkonzeptes für die Cloud-TSE-Lösung können deshalb nicht erfolgen. Es kommt folglich zu **deutlichen Verzögerungen** bei der gesetzlich geforderten Ausrüstung von elektronischen Kassensystemen mit einer cloudbasierten TSE, die die Unternehmen nicht zu verantworten haben. Für den überwiegenden Teil der Unternehmen ist davon auszugehen, dass ein Einsatz dieser Technologie **unmöglich sein wird**.

Das Bundesministerium der Finanzen (BMF) hat unser Schreiben vom 15. Dezember 2020 ebenfalls erhalten und uns mit Schreiben vom 30. Dezember 2020 geantwortet (Anlage 1 Schreiben BMF vom 30. Januar 2020). Das BMF argumentiert zunächst, dass die Anforderungen des BSI an die Einsatzumgebung vom gesetzlichen Auftrag des BSI zur Festlegung der technischen Anforderungen gedeckt seien. Hier haben wir ein anderes Verständnis. Aus unserer Sicht lassen sich weder aus § 146a Abs. 3 AO noch aus § 5 KassenSichV unmittelbar eine Rechtsgrundlage für Vorgaben an die Anwenderumgebung eines elektronischen Aufzeichnungssystems ableiten. Die vom BSI formulierten Anforderungen haben für unsere Unternehmen weitreichende Konsequenzen. Deshalb bitten wir darum, den Umfang des gesetzlichen Auftrags und die darin eingeräumte Regelungsweite an das BSI nochmals zu überprüfen und klarzustellen.

Bei unseren Unternehmen sind angesichts von unklaren Sachständen erhebliche Verunsicherung entstanden. Hilfreich wäre es aus unserer Sicht, wenn bei folgenden Sachverhalten Klärungen erfolgen könnten:

- Beziehen sich die Umgebungsschutzprofile auf die Anwendungsumgebung beim Steuerpflichtigen oder auf die zentrale Hostumgebung der TSE beim TSE-Hersteller?

Unser Sachstand ist: Mit den vom BSI geforderten, erhöhten Anforderungen an die Anwenderumgebung beim Einsatz einer Cloud-TSE sind die Hersteller gezwungen, neue Umgebungsschutzkonzepte zu entwickeln und in den Zertifizierungsprozess einzubringen. Basierend auf den vom BSI und der Bundesdruckerei vorgelegten Dokumenten (Anlage 2: SMAERSOperationalEnvironment_V2 und Anlage 3: Entwurf DTRUST SMAERS Umgebungsschutzkonzept V6.2) handelt es sich aus unserer Sicht um die Einsatzumgebung beim Steuerpflichtigen. (Das BMF weist hingegen in seiner Antwort vom 30. Dezember 2020 die Verantwortung für die Umsetzung der Vorgaben des BSI allein der Bundesdruckerei GmbH – stellvertretend für alle Hersteller cloudbasierter TSE – zu.)

- Verstehen wir folgenden Sachverhalt richtig?

Basierend auf Anlage 2 SMAERS Operational Environment V2, die nach unserer Kenntnis dem Schutzprofil SMAERS 1.0 des BSI vom 28. Juli 2020 als Anlage beigefügt werden soll, empfiehlt das BSI gemäß Kapitel 1 Operational Environment, dass die TSE zusammen mit einer Hardware-Plattform vom Hersteller an den Steuerpflichtigen ausgeliefert werden soll. Ist dies nicht der Fall, muss der Hersteller ergänzende Vorgaben erarbeiten, die vom Steuerpflichtigen befolgt werden müssen, damit die TSE bzw. deren SMAERS-Komponente korrekt in die EDV-Infrastruktur des Steuerpflichtigen integriert wird. Zusätzlich wird ein sicherer Hardware-Anker gefordert. Die Bundesdruckerei sieht deshalb in dem Umgebungsschutzkonzept, das die aktuell fehlenden Vorgaben des BSI der allgemeinen Spezifikationen ersetzen soll, den Einsatz eines Trusted Platform Module 2.0 (TPM 2.0) in jeder Kasse oder im Back-Office Server in allen Niederlassungen bzw. Filialen des Steuerpflichtigen vor. Zudem müssen ein Secure-Boot-Mechanismus eingerichtet und die Festplatte des Host-Systems verschlüsselt werden. Überdies werden strikte Anforderungen an die Administration des Host-Systems gestellt.

- Teilen Sie die Einschätzung unserer Unternehmen, dass beide oben genannte Anforderungen kurzfristig nicht realisierbar sind - weder die Auslieferung der cloudbasierten TSE zusammen mit einer Hardware-Plattform an den Steuerpflichtigen, noch die Implementierung einer TPM 2.0 durch den Steuerpflichtigen in seinen Geschäftsräumen?

Zu Ihrer Information: Auf Anfrage haben große Einzelhandelsunternehmen mit mehreren tausend Filialen geantwortet, dass bisher mangels Bedarf und aus Kostengründen in keiner Kasse und keinem Back-Office Server der Filialen eine TPM 2.0 installiert ist. Die Nachrüstung werde, soweit überhaupt möglich, weit über den 31. März 2021 hinaus dauern. Kein Vertrag der Deutschen Fiskal mit einem Steuerpflichtigen beinhaltet neben der TSE die begleitende Lieferung einer Hardware-Plattform, wie vom BSI empfohlen. Nach unserem Kenntnisstand ist dies bei keinem der Anbieter von cloudbasierten TSE der Fall, denn mit dieser Technologie sollen gerade Eingriffe in die Hardware der Steuerpflichtigen verhindert werden. Dies gilt insbesondere für viele auf stand-alone-Basis verwendete Kassen, die mit einem kasseneigenen Betriebssystem ausgestattet sind. Gerade kleinere Kassen lassen sich nur schwer bzw. überhaupt nicht nachträglich mit einem TPM-Modul ausstatten, da eine TPM 2.0 nur mit den Betriebssystemen Windows und Linux verwendet werden können.

Das BMF hat uns, gestützt auf Informationen des BSI, am 30. Dezember 2020 geantwortet, dass zwar ein Secure Boot in Verbindung mit dem im Prozessor integrierten TPM eingesetzt wird. Diese Anforderungen seien jedoch nicht mit dem Einsatz einer Token-TSE vergleichbar.

Auch diese Einschätzung verstehen wir nicht, weil die steuerpflichtigen Unternehmen und die TSE Hersteller uns mitteilen, dass keineswegs in allen eingesetzten Prozessoren ein TPM integriert ist und dies abhängig vom verwendeten Betriebssystem evtl. auch gar nicht möglich ist.

Es wäre für unsere Unternehmen eine große Hilfe, wenn Sie uns zu den genannten Sachverhalten weitere erklärende Hinweise geben könnten.

Sollten tatsächlich aufgrund erhöhter Sicherheitsanforderungen des BSI an die Anwenderumgebung beim Einsatz einer cloudbasierten TSE weitgehende Eingriffe in die Hardware des Steuerpflichtigen notwendig sein, sehen wir die Umsetzung der vom Gesetzgeber geforderten Aufrüstung von elektronischen Aufzeichnungssystemen gemäß § 146a AO mit cloudbasierten TSE durch die Unternehmen als nachhaltig gefährdet an. Unsere Unternehmen stellen sich darüber hinaus die Frage, ob die vom Gesetzgeber ausdrücklich zugesagte Technologieoffenheit überhaupt noch erreicht werden kann.

Weitere Details bitten wir Sie, dem besonderen Teil dieses Schreibens und den beigefügten Anlagen zu entnehmen. Wir hoffen sehr, dass zusätzliche Erläuterungen zu den angesprochenen Sachverhalten letztlich dazu beitragen können, möglichst bald eine praxistaugliche Lösungen zu finden, die es unseren Unternehmen zeitnah ermöglicht, ihre Kassensysteme mit Cloud-TSE-Lösungen auszurüsten.

Eine Kopie dieses Schreibens haben wir dem BMF und dem BMWi zur Kenntnis zugeleitet. Für Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

DEUTSCHER INDUSTRIE- UND
HANDELSKAMMERTAG E. V.

BUNDESVERBAND
DER DEUTSCHEN INDUSTRIE E. V.

ZENTRALVERBAND DES DEUTSCHEN
HANDWERKS E. V.

BUNDESVEREINIGUNG DER DEUTSCHEN
ARBEITGEBERVERBÄNDE E. V.

HANDELSVERBAND DEUTSCHLAND
(HDE) E.V.

BUNDESVERBAND GROSSHANDEL,
AUSSENHANDEL, DIENSTLEISTUNGEN E. V.