I. Neue Anforderungen an die Betriebsumgebung einer cloudbasierten TSE durch das BSI

Das BSI hat am 28. Juli 2020 das Schutzprofil SMAERS 1.0 vorgestellt. Darin wird unter den möglichen Bedrohungen der TSE erstmals der Nutzer der TSE explizit als potenzieller Angreifer der TSE angesehen (Kapitel 3.2, Application Note 1). Deshalb finden sich in den Kapiteln 6.2.1 „Assurance Refinements“ und 6.3.3 „Security Assurance Requirements Rationale“ Forderungen nach einer „guidance documentation“, welche durch die Hersteller zu liefern ist. Dies ist ein vom TSE Hersteller zu erstellendes **Umgebungsschutzkonzept**, **welches vom Anwender d.h. dem steuerpflichtigen Unternehmen erfüllt bzw. umgesetzt werden muss**.

Im ergänzenden Dokument **„SMAERSOperationalEnvironment_V2“** vom November 2020 (vgl. Anlage 2), welches unserer Kenntnis nach dem SMAERS-Schutzprofil als Anhang beigefügt werden soll, wird dies deutlich. Denn sofern der TSE Hersteller keine Hardware-Plattform mitliefert, muss ein Umgebungsschutzkonzept für die Anwendung beim Steuerpflichtigen erstellt werden („In any other case, the manufacturer is obliged to provide additional guidance to ensure that SMAERS is integrated correctly into the cash register or infrastructure operated by the tax payer.”). Damit richten sich die Anforderungen des BSI entweder

- an die Hersteller, falls diese die cloudbasierte TSE mit einer Hardware-Plattform ausliefern oder
- den Steuerpflichtigen, falls die TSE in dessen bestehende Infrastruktur integriert werden soll.

In jedem Fall müssen die Anforderungen des BSI aber in der Anwendungsumgebung des Steuerpflichtigen umgesetzt werden.

Ergänzend wird explizit ein sicherer **Hardware-Anker** beim Anwender verlangt („To prevent physical attacks against the platform, secure hardware SHALL be used as root of trust.“). Überdies soll für jede Plattform in den Unternehmen ein eigenes Sicherungskonzept erstellt werden.

Um die oben genannten Anforderungen zu erfüllen, empfiehlt das BSI aktuell die Implementierung eines Trusted Platform Module 2.0 (TPM 2.0) beim Anwender (Steuerpflichtigen), sieht ein solches jedoch nicht zwingend vor. Neben einem TPM 2.0 kommt die Umsetzung durch Einsatz einer separaten Hardware-Einheit (sog. „Mini-PC) durch den Anwender oder

mittelfristig eine reine Softwarelösung in Betracht. Die Umsetzung durch ein TPM 2.0 kann allerdings nur erfolgen, wenn das Betriebssystem des Steuerpflichtigen ein solches Modul auch unterstützt. Dies ist nur bei den Betriebssystemen von Windows oder Linux der Fall. Sowohl bei proprietären Kassen als auch PC-Kassen, die mit dem Betriebssystem von Apple arbeiten, ist eine Umsetzung via Implementierung eines TPM 2.0 ausgeschlossen. Es ist entweder die Anschaffung gesonderter Hardware durch den Anwender oder eine software-technische Absicherung erforderlich.

Das BSI fordert weiter, dass die SMAERS-Komponente und deren Schutz durch eine der zuvor aufgezeigten Sicherungskonzepte so nah wie möglich am entsprechenden Aufzeichnungssystem, also der jeweiligen Kasse, zumindest aber in der jeweiligen Filiale eingesetzt wird. Danach ist auch eine zentrale Implementierung in einem Rechenzentrum des Unternehmens nicht konform, so dass die **Umsetzung in den einzelnen Filialen der Unternehmen erfolgen muss**.

II. Aktueller Stand einer Umsetzung der neuen Anforderungen durch die Anbieter von TSE-Lösungen

Gemeinsame Erarbeitung eines Umgebungsschutzkonzeptes durch eine Arbeitsgruppe

Die oben genannten Anforderungen wurden erst im Juli (SMAERS 1.0) und November 2020 (SMAERSOperationalEnvironment_V2) veröffentlicht. Sämtliche Investitions-, Entwicklungs- und Integrationsentscheidungen der Hersteller sowie der Anwender fanden auf einer gänzlich anderen technisch-organisatorischen sowie regulatorischen Grundlage statt.

Die Hersteller der cloudbasierten TSE haben deshalb unter dem Dach der TeleTrusT, Bundesverband IT-Sicherheit e.V. einen Arbeitskreis gegründet, der zunächst allgemeine Kriterien für das Umgebungsschutzkonzept für die Anwendung einer cloudbasierten TSE erarbeiten soll. An diesem Arbeitskreis nehmen alle Hersteller, sowohl von soft- als auch hardwarebasierten TSEs, die Zertifizierungs-Prüfstellen MTG AG, TÜViT und SRC, Steuerpflichtige als TSE Nutzer und grundsätzlich auch das BSI teil. Ziel ist, zunächst den allgemeingültigen Aufbau des Umgebungsschutzkonzepts der SMAERS-Komponente bei einer cloudbasierten TSE zu definieren. Darauf aufbauend sollen dann die einzelnen Hersteller von TSE ihre individuellen Umgebungsschutzkonzepte formulieren, die dann noch an die Anwendungsumgebung des jeweiligen Steuerpflichtigen angepasst werden.

Nach Einschätzung der Mitglieder des Arbeitskreises werden die Arbeiten voraussichtlich weder vor dem 31. Januar 2021 noch vor dem 31. März 2021 abgeschlossen sein.

Umsetzung der Anforderungen in einem Umgebungskonzept im Rahmen des Zertifizierungsverfahrens des Herstellers D-Trust GmbH

Der Entwurf eines Umgebungskonzeptes des Herstellers D-Trust-Bundesdruckerei GmbH wird gegenwärtig durch das BSI im Rahmen des laufenden Zertifizierungsprozesses geprüft (vgl. Anlage 3).

Die Anforderungen des BSI an das Umgebungsschutzkonzept beim Anwender / Steuerpflichtigen und das daraus abgeleitete Konzept von D-Trust-Bundesdruckerei zum Schutz von SMAERS durch die Umgebung stellen die Anwender / Steuerpflichtigen vor **große Herausforderungen**. Dies betrifft insbesondere **den geforderten Einsatz einer TPM 2.0** (Kapitel 8.2, TM 2, S. 9 f.).

- Zum einen muss ein Betriebssystem verwendet werden, dass ein TPM 2.0 unterstützt. Dies wird dazu führen, dass bestimmte Kassen aufgrund der neuen Anforderungen nicht mehr mit einer Cloud-TSE ausgestattet werden können.
- Die Nachrüstung der Kassen oder Filialen mit einem TPM ist nicht kurzfristig realisierbar, sondern wird weit über den 31. März 2021 hinaus dauern.
- Die Unabhängigkeit des Integrators vom Steuerpflichtigen und die fehlende Kenntnis der Administratorzugangsberechtigung verwehren dem Steuerpflichtigen den Zugang zu seiner TSE. Notwendige Anpassungen können nur über einen Dritten vorgenommen werden, was tiefgreifende organisatorische Anpassungen im Unternehmen erfordert. Für eine effiziente Integration der TPM dürfte diese in der Regel nicht in jeder Kasse, sondern im Back-Office Server implementiert werden. Die fehlenden Administratorkennwörter erfordern dann, dass jegliche Anpassung an der Software des Backoffice Servers – nicht nur TPM bezogene Anpassungen – durch einen fremden Dritten vorgenommen werden.

III. Folgen für die Praxis im Hinblick auf die Einhaltung der Anforderungen des § 146a AO und der Nichtbeanstandungsregelungen der Länder

Sowohl für die Unternehmen als auch die Finanzverwaltung wird es aufgrund der neuen Anforderungen des BSI an die cloudbasierte TSE zu vielfachen Problemen kommen, die zeitnah gelöst werden sollten. Wir, die unterzeichnenden Spitzenverbände der gewerblichen Wirtschaft, hatten bereits in einem ersten Schreiben vom 15. Dezember 2020 einige

Aspekte aufgezeigt und halten die fristgerechte Umsetzung der neuen Anforderungen des BSI an den Umgebungsschutz nicht für möglich. In seinem Schreiben ,“Bekanntmachung eines Hinweises auf die Veröffentlichung geänderter Schutzprofile des Bundesamtes für Sicherheit in der Informationstechnik; „Schutzprofil „Sicherheitsmodulanwendung für elektronische Aufzeichnungssysteme“ BSI-CC-PP-0105-V2-2020, Version 1.0“‘ vom 7. August 2020 hält das BMF die Fortführung der Zertifizierung allerdings grundsätzlich auch auf Basis der ersten Fassung des Schutzprofils in Version 0.75 für möglich; gleiches gilt für die Re-Zertifizierung von bereits nach der ersten Fassung zertifizierten Produkten, sofern nur geringfügige Anpassungen am Produkt vorgenommen wurden.

Petitum: Die Re-Zertifizierung der TSE der Anbieter Deutsche Fiskal / Bundesdruckerei / D-Trustsollte auf Basis der ersten Fassung des Schutzprofils in Version 0.75 erfolgen. Die erstmalige Zertifizierung weiterer Anbieter sollte ebenfalls auf Grundlage dieses Schutzprofils erfolgen. So kann der in unser aller Interesse stehende flächendeckende Einsatz manipulationssicherer Kassensysteme fristgerecht umgesetzt werden.

Gestufte Einführung der neuen Anforderungen als Entlastung sowohl für die Unternehmen als auch die Finanzverwaltung

Sollte am Schutzprofil 1.0 festgehalten werden, kann aktuell weder sicher davon ausgegangen werden, dass eine zertifizierte Cloud-TSE-Lösung nach dem 31. Januar 2021 vorhanden sein wird, noch ist die Umsetzung neuer Anforderungen in den Unternehmen bis zum Auslaufen der Frist am 31. März 2021 sicher möglich. Somit würde es zu Belastungen der Unternehmen und der Finanzämter durch die erforderliche Antragstellung kommen Es dürfte für die zuständigen Finanzämter kaum möglich sein, die Validität der jeweils variierenden technischen Begründungen bei Anträgen auf Erleichterung nach § 148 AO zu prüfen.

Hinzu tritt der Umstand, dass die Finanzverwaltung in Betriebsprüfungen oder Kassen-Nachschauen zwar das Vorliegen eines Zertifikates für die jeweilige Cloud-Lösung überprüfen, die Einhaltung der Umsetzung der weiteren Anforderungen in der lokalen SMAERS-Komponente jedoch nicht. Damit sind „vereinfachte Prüfungen“ anhand eines Ausdrucks des Kassenbelegs in Fällen von Cloud-Lösungen erst recht ungeeignet für die Beurteilung, ob die Anforderungen des § 146a AO erfüllt sind.

Petitum: Wir möchten Sie daher nochmals eindringlich bitten, sich sowohl beim BMF als auch beim BSI dafür einzusetzen, dass die neuen, erhöhten Anforderungen an die Anwendungsumgebung einer cloudbasierten TSE-Lösung, sofern sie für notwendig gehalten werden, erst nach einer sachgerechten sowie praxistauglichen Umsetzungsfrist für die Unternehmen in einem abgestuften zeitlichen Verfahren verbindlich werden.

Die Einschränkung der Technologieoffenheit für alle Unternehmen wird damit allerdings nicht zufriedenstellend gelöst. Deshalb sollte geprüft werden, ob das vom BSI geforderte Umgebungsschutzkonzept **vom gesetzgeberischen Willen gedeckt, zwingend erforderlich und zudem verhältnismäßig is**t. Denn falls ein Technologiewechsel erforderlich ist, werden die bereits getätigten Investitionen der Unternehmen vollständig entwertet.