Whitepaper

WHITE PAPER

zur Compliance des Cloud-Dienstes für Cybersicherheit „Trend Vision One“ von Trend Micro mit der Datenschutz-Grundverordnung (DSGVO) und mit Sicherheitsanforderungen an Cloud-Dienste unter Berücksichtigung des C5-Testats von Trend Micro

Der Cloud-Dienst für Cybersicherheit von Trend Micro „Trend Vision One“ und deren integrierte Sicherheitsfunktion „eXtended Detection & Response (XDR)“ ermöglichen es Unternehmen, ihre individuelle Bedrohungslage zu analysieren, identifizierte Risiken und Bedrohungen für die Cybersicherheit des Unternehmens abzuwehren und automatisierte Gegenmaßnahmen zu definieren. Hierbei werden Aktivitätsdaten über mehrere Sicherheitsvektoren hinweg tiefgreifend verknüpft, um die Erkennung und Untersuchung verdächtiger Ereignisse zu optimieren. In diesem Zusammenhang werden durch die Trend Micro-Lösungen personenbezogene Daten erhoben und es können im Einzelfall auffällige Geräte, ungewöhnliche Datenbewegungen oder angegriffene Schwachstellen auf Servern und Endpunkten näher untersucht werden und hierbei ein Personenbezug erfolgen.

Trend Vision One und XDR sind Software as a Service (SaaS)- und somit Cloud-Dienste, was bei der datenschutzrechtlichen Bewertung zu berücksichtigen ist. Trend Micro hat im Januar 2023 das Testat nach den Kriterien des C5:2020-Standards (Cloud Computing Compliance Criteria Catalogue) erhalten, das u.a. Trend Vision One umfasst. Diese Kriterien basieren auf dem Anforderungskatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) und haben sich in Deutschland zum anerkannten Sicherheitsstandard für Cloud-Computing entwickelt.

Dieses White Paper wurde von Trend Micro erstellt, um Kunden bei der Beurteilung hinsichtlich des datenschutzkonformen und sicheren Einsatzes des Cloud-Dienstes für Cybersicherheit von „Trend Vision One“ und von XDR als eine Technik moderner Cyberabwehr unter Berücksichtigung des C5-Testats von Trend Micro zu unterstützen. Es stellt allerdings keinerlei Funktionsbeschreibung, Beschaffenheitsangabe oder Darstellung bestimmter Eigenschaften der Produkte und Cybersicherheitslösungen von Trend Micro dar. Der Kunde muss zudem eine eigene datenschutzrechtliche Bewertung und ein eigenes Risikomanagement durchführen, wenn er Trend Vision One und XDR einsetzen möchte.

I. Executive Summary

- Der **Cloud-Dienst für Cybersicherheit „Trend Vision One“** und deren integrierte Sicherheitsfunktion **„eXtended Detection and Response (XDR)“** ermöglichen es Unternehmen, ihre individuelle Bedrohungslage zu analysieren, identifizierte Risiken und Bedrohungen für die Cybersicherheit des Unternehmens abzuwehren und automatisierte Gegenmaßnahmen zu definieren.
- Die Erhebung, Verarbeitung und Speicherung personenbezogener Daten, die hierbei durch Trend Vision One und XDR erfolgt, sind **datenschutzrechtlich zulässig**, wenn sie zur Wahrung der berechtigten Interessen des Unternehmens, das sich gegen Bedrohungen seiner Cybersicherheit schützt, erforderlich sind, und die Interessen der betroffenen Person nicht überwiegen.
- Trend Micro hat eine **ineinandergreifende Vertragsstruktur von Datenverarbeitungs-verträgen** mit seinen Kunden, innerhalb der Trend Micro-Unternehmensgruppe und mit seinen Unterauftragnehmern bzw. Unterauftragsverarbeitern – insbesondere AWS und Microsoft Azure – geschaffen, durch die sichergestellt wird, dass der **Kunde** seine **Rechte als datenschutzrechtlich „Verantwortlicher“** ausüben kann und dass die im Rahmen der Trend Micro Cloud-Dienste bereitgestellten oder erhobenen personenbezogenen Daten des Kunden nur dann an Unternehmen innerhalb der Trend Micro-Unternehmensgruppe und an Unterauftragsverarbeiter in Drittländern übermittelt werden, wenn ein **angemessenes Datenschutzniveau** gewährleistet ist.
- Das **C5-Testat von Trend Micro** zeigt, dass „Trend Vision One“ die im Kriterienkatalog C5 spezifizierten **Mindestanforderungen an sicheres Cloud Computing** erfüllt. Es stellt für Cloud-Kunden eine wichtige Orientierung für die Auswahl eines Cloud-Anbieters dar und bildet die **Grundlage**, um ein **kundeneigenes Risikomanagement** durchführen zu können.

II. Funktionsweise des Cloud-Dienstes für Cybersicherheit „Trend Vision One“ und der integrierten XDR-Technologie

Der Cloud-Dienst für Cybersicherheit „Trend Vision One“ von Trend Micro priorisiert IT-Sicherheitsrisiken in Unternehmen, um die Erkennung und Untersuchung verdächtiger Ereignisse zu optimieren. Trend Vision One korreliert hierzu führende Bedrohungs- und Schwachstelleninformationen mit umfangreichen Telemetriedaten, die Trend Micro Sensoren und bei Bedarf auch Drittanbieter-Lösungen auf unterschiedlichen Ebenen der Umgebung sammeln, darunter mittels XDR gesammelte Informationen. Diese Informationen werden in verschiedenen Dashboards aufbereitet. Unternehmen können so ihre individuelle Bedrohungslage analysieren, identifizierte Risiken und Bedrohungen für die Cybersicherheit des Unternehmens abwehren und automatisierte Gegenmaßnahmen definieren.

XDR sammelt und korreliert Informationen aus den übermittelten Sensordaten der angeschlossenen Schutzprodukte wie bspw. E-Mail, Endpunkte, Server, Cloud-Workloads und Netzwerke des Unternehmens hinweg. Einzelne, ggf. auch harmlos erscheinende Events können so als Indicators of Compromise (IoC) identifiziert werden. XDR umfasst hierbei u.a. folgende Aktivitäten:

Aufzeichnung von Endpunkt-Events

Es werden alle Aktionen und das Systemverhalten auf dem Endpunkt aufgezeichnet, um die rückblickende Untersuchung verdächtiger Aktivitäten zu ermöglichen. Die Informationen werden auf dem Endpunkt gespeichert und an Trend Vision One werden lediglich Metadaten gesendet, um Indicators of Compromise (IoC) zu identifizieren. Endpunkte mit einem IoC können sodann durch den Kunden optional isoliert und einer Root-Cause-Analyse unterzogen werden, um die Ausbreitung eines Angriffs festzustellen und darauf im erforderlichen Maße zu reagieren. Nur bei tatsächlichen Anhaltspunkten einer Bedrohung erfolgt also eine nähere Analyse, bei der im Einzelfall auch personenbezogene Daten bezüglich der angegriffenen Endpunkte erhoben werden können.

Metadaten-Vergleich und IoC-Suche

Die so ermittelten Metadaten werden mit den Metadaten auf anderen Online- oder Offline-Endpunkten des Unternehmens automatisiert verglichen, um dort entsprechende Indicators of Compromise (IoC) zu finden (Threat Hunting). Hierdurch müssen deutlich weniger Daten zentral gespeichert und verwaltet werden und es werden manuelle Überprüfungen überflüssig gemacht.

Root-Cause-Analyse

Mittels der Root-Cause-Analyse erhalten die Sicherheitsverantwortlichen des Unternehmens eine Übersicht zur Bedrohungsquelle, der Ausbreitung und der erforderlichen Behebungsmaßnahmen. Bei der Root-Cause-Analyse werden zwar einzelne Endpunkte und damit gegebenenfalls auch Anwender (z.B. der Inhaber einer infizierten Mailbox oder an einem Endpunkt angemeldeter Benutzername) identifiziert, jedoch nur, sofern eine Bedrohung vorliegt, und nur gegenüber den hierzu berechtigten Sicherheitsverantwortlichen des Unternehmens. Ziel der Root-Cause-Analyse ist die Verhinderung einer weiteren Ausbreitung und weiterer Schäden.

Managed XDR

Trend Micro bietet zusätzliche Unterstützung in Form eines kostenpflichtigen Managed XDR Service an, bei dem Sicherheitsexperten von Trend Micro den Kunden durch 24x7 Alarm-Monitoring sowie Untersuchung, Wiederherstellung und Reaktion unterstützen, um beim Kunden den Aufwand und die benötigte Zeit für die Identifikation und Analyse von Bedrohungen zu reduzieren.

Visualisierung und Priorisierung der Bedrohungsinformationen

Mittels Trend Vision One werden die über XDR ermittelten Bedrohungsinformationen in verschiedenen Dashboards aufbereitet und visualisiert sowie Alarme priorisiert, um dem Unternehmen das Verständnis von Zusammenhängen zu erleichtern.

Die durch Trend Vision One erhobenen, verarbeiteten und übermittelten personenbezogenen Daten sind in der „Trend Vision One Data Collection Notice" aufgeführt, die auf der Webseite von Trend Micro unter https://success.trendmicro.com/dcx/s/solution/000262137?language=en_US abrufbar ist. Hierunter fallen u.a. Art und Herkunft der Bedrohung, URL, IP-Adresse oder E-Mail-Adresse des Angreifers und der angegriffene Endpunkt, verdächtige Web-Aktivitäten von Nutzern und verdächtige Dateien. In der „Trend Vision One Data Collection Notice" wird auch dargestellt, wie der Kunde einzelne Features von Trend Vision One deaktivieren und dadurch auch die damit einhergehende Erhebung, Verarbeitung und Übermittlung personenbezogener Daten unterbinden kann.

III. DSGVO-Compliance beim Einsatz von Cybersicherheitslösungen

Für die Datenverarbeitung verantwortliche Unternehmen wie auch deren Auftragsverarbeiter sind nach der Datenschutz-Grundverordnung (DSGVO) **gesetzlich verpflichtet**, mittels **geeigneter technischer und organisatorischer Maßnahmen** sicherzustellen, dass die Verarbeitung personenbezogener Daten rechtmäßig und ein dem Risiko **angemessenes Schutzniveau** gewährleistet ist, einschließlich Schutz vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung bzw. unbefugtem Zugang zu personenbezogenen Daten. Solche Maßnahmen umfassen unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten und die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Zudem auch die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Um ihrer Verpflichtung nachzukommen, die Vertraulichkeit und Integrität der Systeme, Dienste und personenbezogenen Daten zu wahren und Datenschutzverstöße wie etwa Datenlecks zu verhindern, werden Unternehmen in aller Regel **Cybersicherheitslösungen** wie bspw. **Trend Vision One** und XDR einsetzen. Allerdings werden im Rahmen der Bedrohungserkennung und Angriffsabwehr wiederum personenbezogene Daten, etwa zu Art und Herkunft der Bedrohung, URL, IP-Adresse oder E-Mail-Adresse des Angreifers, angegriffene Endpunkte sowie verdächtige Web-Aktivitäten von Nutzern oder verdächtige Dateien erhoben und für eine begrenzte Zeit gespeichert.

Eine solche Datenverarbeitung muss ihrerseits dem **datenschutzrechtlichen Grundsatz der Rechtmäßigkeit der Datenverarbeitung** gerecht werden. Ob eine solche Erhebung und Verarbeitung personenbezogener Daten aus Gründen der Cybersicherheit zur Verhinderung von Betrug oder zum Schutz vor Angriffen auf die IT-Infrastruktur von Unternehmen datenschutzrechtlich zulässig ist, ist im Rahmen einer **Interessenabwägung** zu ermitteln.

In den Erwägungsgründen der DSGVO ist diesbezüglich explizit ausgeführt, dass die Verarbeitung von personenbezogenen Daten durch Anbieter von Sicherheitstechnologien und diensten ein berechtigtes Interesse des jeweiligen verantwortlichen Unternehmens darstellt, wie dies für die **Gewährleistung der Netz- und Informationssicherheit** unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste beeinträchtigen. Ein solches **berechtigtes Interesse** besteht beispielsweise darin, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie „Denial of Service"-Angriffe und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

Dies bedeutet, dass die **Erhebung, Verarbeitung und Speicherung personenbezogener Daten durch Cybersicherheitslösungen wie Trend Vision One und XDR datenschutzrechtlich zulässig ist**, wenn sie zur **Wahrung der berechtigten Interessen des Unternehmens**, das sich gegen Angriffe auf seine IT-Infrastruktur schützt, erforderlich ist, und die **Interessen der betroffenen Person** nicht überwiegen. Faktoren, die im Rahmen dieser Interessenabwägung zugunsten des Unternehmens zu berücksichtigen sind, sind etwa Anonymisierung, Pseudonymisierung und Verschlüsselung personenbezogener Daten, Datenminimierung und die Begrenzung der Datenspeicherung auf die erforderliche Zeit.

Diesen Anforderungen werden die Cybersicherheitslösungen Trend Vision One und XDR von Trend Micro insbesondere dadurch gerecht, dass ein mehrschichtiger Ansatz der Bedrohungserkennung verfolgt wird, bei dem der Netzwerkdatenverkehr, E-Mails oder Dateien (z.B. ausführbare potenziell schädliche Dateitypen) des Unternehmens weitestgehend automatisiert und ohne menschliche Einfluss- und Kenntnisnahme auf Schadsoftware und Angriffe überprüft und analysiert werden und eine nähere individuelle Überprüfung lediglich von unbekannten Bedrohungen erfolgt, die durch autorisierte Sicherheitsverantwortliche des Kunden oder von Sicherheitsexperten von Trend Micro im Auftrag des Kunden vorgenommen wird. Zudem werden soweit möglich lediglich Metadaten verarbeitet. Letztlich liegt es aber in der Verantwortung des Kunden als datenschutzrechtlich „Verantwortlicher", die Abwägung der Interessen des Unternehmens einerseits und der betroffenen Personen andererseits beim Einsatz von Cybersicherheitslösungen vorzunehmen.

Sofern im Rahmen der **IT-Compliance und Cybersecurity** personenbezogene Daten im für die zur Bedrohungserkennung und Angriffsabwehr erforderlichen Umfang erhoben und verarbeitet werden, werden also die Interessen der betroffenen Personen meist nicht überwiegen, so dass eine solche **Datenverarbeitung durch das Unternehmen rechtmäßig** ist. Im Rahmen ihrer **Rechenschaftspflicht** müssen Unternehmen sowohl geeignete **technische und organisatorische Maßnahmen** zur Sicherstellung der Vertraulichkeit und Integrität der Systeme, Dienste und personenbezogenen Daten als auch die Rechtmäßigkeit der im Rahmen der Cybersecurity-Maßnahmen vorgenommenen Datenverarbeitung sicherstellen und dokumentieren.

IV. Cloud-Dienste

Trend Vision One und XDR sind Software as a Service (SaaS)- und somit **Cloud-Dienste**. Dies folgt dem generellen Trend in der Wirtschaft, Cloud-Dienste einzusetzen, weil mit diesen zahlreiche Vorteile wie Flexibilität, Skalierbarkeit und bessere Verfügbarkeit gegenüber beim Kunden selbst betriebener Software verbunden werden. Auch die Europäische Kommission verfolgt in ihrer Cloud-Strategie („European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy" vom 16. Mai 2019) einen „Cloud-first"-Ansatz, der bedeutet, dass jede Neuentwicklung vorzugsweise cloud-nativ, also auf Grundlage cloud-basierter IT-Dienste sein sollte, und dass Systeme so konzipiert werden sollten, dass sie von den Vorteilen cloudbasierter Bereitstellungsmodelle profitieren können.

Cloud Computing führt allerdings zu gesteigerten Anforderungen sowohl in Bezug auf **Datenschutz**, da hierbei in der Regel personenbezogene Daten von Kunden an den Cloud-Anbieter übermittelt werden, als auch bezüglich der **Sicherheitsanforderunge**n an die Nutzung externer Cloud-Dienste.

V. DSGVO-Compliance beim Einsatz von Cloud-Diensten

1. Auftragsverarbeitung

Personenbezogene Daten, die Trend Micro von ihren Kunden zum Zwecke der Bereitstellung von Produkten oder Diensten von Trend Micro wie dem Cloud-Dienst „Trend Vision One" zur Verfügung gestellt bekommt oder beim Kunden erhebt, verarbeitet Trend Micro ausschließlich für diese Zwecke und in Übereinstimmung mit den Weisungen der Kunden und einschlägigem Datenschutzrecht, insbesondere der DSGVO. Der Kunde ist hiernach „Verantwortlicher" i.S.d. DSGVO, Trend Micro Auftragsverarbeiter oder ggf. Unterauftragsverarbeiter für den Kunden. Trend Micro und der Kunde schließen hierzu einen **Nachtrag zur Datenverarbeitung (Data Processing Addendum, DPA)** ab.

Das DPA stellt einen Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO dar und ist Bestandteil jedes Vertrages zwischen Trend Micro und den Kunden, der mittels Verweis einbezogen wird. Das DPA kann in der jeweils aktuellen Fassung auf der Webseite von Trend Micro abgerufen werden unter: https://www.trendmicro.com/en_us/about/trust-center/privacy/gdpr/data-processing-addendum.html.

2. Technische und organisatorische Maßnahmen

Trend Micro hat umfassende geeignete technische und organisatorische Maßnahmen gem. Art. 32 DSGVO getroffen, die in Anlage 2 zum DPA beschrieben sind. Sie umfassen u.a.

- Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Maßnahmen zur Gewährleistung fortlaufender Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten
- Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugriff darauf im Falle eines physischen oder technischen Ereignisses rechtzeitig wiederherzustellen
- Verfahren zum regelmäßigen Testen, zur Einschätzung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen, um die Sicherheit bei der Verarbeitung zu gewährleisten
- Maßnahmen zur Nutzeridentifizierung und -autorisierung
- Maßnahmen zum Schutz personenbezogener Daten während der Übertragung
- Maßnahmen zum Schutz personenbezogener Daten während der Speicherung
- Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden
- Maßnahmen zur internen IT und IT Security Governance und Verwaltung
- Maßnahmen zur Gewährleistung von Datenminimierung, Datenqualität, begrenzter Speicherdauer, Rechenschaftspflicht, Datenübertragbarkeit und Löschung

3. Standardvertragsklauseln

Die Standardvertragsklauseln der Europäischen Union (EU) vom 4. Juni 2021 für die Übermittlung personenbezogener Daten an Drittländer, die kein angemessenes Datenschutzniveau gewährleisten, finden ergänzend zwischen dem Kunden und Trend Micro Anwendung, soweit eine Übermittlung personenbezogener Daten des Kunden aus der EU oder dem EWR (Europäischer Wirtschaftsraum) an Trend Micro außerhalb der EU bzw. dem EWR erfolgt. Nach diesen Standardvertragsklauseln gilt ein in der EU ansässiger Kunde als „Datenexporteur" und „Verantwortlicher" und die in der Lizenzurkunde angegebene Trend Micro-Gesellschaft mit Sitz in den USA (oder ggf. einem anderen Drittland) als „Datenimporteur" und „Auftragsverarbeiter", die personenbezogene Daten zum Zweck der Bereitstellung der Trend Micro-Produkte im Namen des Kunden verarbeitet. Durch diese Standardvertragsklauseln wird ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der EU an Trend Micro in den USA oder einem anderen Drittland übermittelt werden.

4. Transfer Impact Assessment

Für den internationalen Datentransfer in Länder ohne angemessenes Datenschutzniveau bestehen auch bei Verwendung von Standardvertragsklauseln weitergehende Prüfanforderungen, ob zusätzliche Garantien und Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen erforderlich sind. Um die tatsächliche Wirksamkeit solcher zusätzlichen vertraglichen, technischen oder organisatorischen Maßnahmen zu beurteilen, sieht Klausel 14 der Standardvertragsklauseln u.a. die Durchführung eines sog. „Transfer Impact Assessment" (TIA) vor, bei dem u.a. die relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungslandes zu berücksichtigen sind.

Trend Micro hat solche Transfer Impact Assessments für verschiedene Länder – insbesondere die USA – durchgeführt und hinsichtlich der USA als zusätzliche technische Maßnahmen insbesondere eine Verschlüsselung der Daten sowohl „at rest" als auch „in transit" vorgenommen. Trend Micro stellt ihren Kunden bei Bedarf die einschlägigen Transfer Impact Assessments zur Verfügung.

5. Weiterübermittlung von personenbezogenen Daten

Trend Micro ist als Datenimporteur nach den Standardvertragsklauseln berechtigt, Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten zu beauftragen, wenn diese Beauftragung im Wege eines schriftlichen Vertrags erfolgt, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die Trend Micro als Datenimporteur gemäß den Standardvertragsklauseln binden, und wenn im Falle einer Weiterübermittlung in ein Drittland ohne Angemessenheitsbeschluss der Empfänger ebenfalls an die Standardvertragsklauseln gebunden ist.

Trend Micro und seine Unterauftragnehmer haben sich an diese Anforderungen gehalten, da jede Übermittlung personenbezogener Daten innerhalb der Trend Micro-Unternehmensgruppe und an Unterauftragnehmer von Trend Micro durch die konzerninterne Datenübermittlungsvereinbarung (IGA) von Trend Micro, Verträge zur Auftragsverarbeitung mit Unterauftragnehmern und durch die Verwendung von Standardvertragsklauseln abgesichert wird. Trend Micro hat eine nachfolgend näher dargestellte **ineinandergreifende Vertragsstruktur von Datenverarbeitungsverträgen** geschaffen, durch die sichergestellt wird, dass der Kunde seine Rechte als Verantwortlicher ausüben kann und dass die im Rahmen der Trend Micro Cloud-Dienste bereitgestellten oder erhobenen personenbezogenen Daten des Kunden nur dann an Trend Micro-Unternehmen und Unterauftragnehmer bzw. Unterauftragsverarbeiter von Trend Micro in Drittländern übermittelt werden, wenn ein angemessenes Datenschutzniveau gewährleistet ist.

a) Weiterübermittlung an Unternehmen innerhalb der Trend Micro-Unternehmensgruppe

Bei der Erbringung der Cloud-Dienste von Trend Micro werden personenbezogene Daten von Kunden in der EU nicht nur von einem Trend Micro-Unternehmen in der EU erhoben und verarbeitet. Sie werden auch von **Trend Micro Incorporated mit Sitz in den USA** und anderen Trend Micro-Unternehmen in verschiedenen Ländern erhoben und verarbeitet, da der Cloud-Dienst „Trend Vision One" von Trend Micro aus Rechenzentren in der EU, USA, Japan, Singapur, Australien und Indien erbracht wird und die Trend Micro Support-Teams, die bspw. Support-Anfragen des Kunden bearbeiten, ebenfalls in mehreren Ländern tätig sind. Um die Übermittlung personenbezogener Daten innerhalb der weltweiten Trend Micro-Unternehmensgruppe zu ermöglichen, haben alle Unternehmen der multinationalen Trend Micro-Unternehmensgruppe eine konzerninterne Datenübermittlungsvereinbarung – das sog. **„Intra Group Enterprise Customer Data Transfer Agreement" (IGA)** – abgeschlossen.

Dies regelt u.a. dass das empfangende Trend Micro-Unternehmen als Unterauftragsverarbeiter fungiert. In Bezug auf die Weiterübermittlung nach Japan ist darauf hinzuweisen, dass Japan gemäß dem Angemessenheitsbeschluss der Europäischen Kommission vom 23. Januar 2019 ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die aus der EU an Unternehmen in Japan übermittelt werden, so dass die Übermittlung personenbezogener Daten an Rechenzentren in Japan zulässig ist. Das IGA beinhaltet auch die Standardvertragsklauseln der EU für die Übermittlung von Daten von einem Auftragsverarbeiter an einen weiteren Auftragsverarbeiter in einem Drittland, das kein **angemessenes Datenschutzniveau** gewährleistet. Durch dieses IGA in Verbindung mit den Standardvertragsklauseln wird ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, die **innerhalb der Trend Micro-Unternehmensgruppe an Trend Micro-Unternehmen außerhalb der EU** übermittelt werden.

b) Weiterübermittlung an Unterauftragsverarbeiter von Trend Micro

Trend Micro verwendet die Rechenzentren und Speicherkapazitäten der Hyperscaler **Amazon Web Services (AWS) und Microsoft Azure**. Trend Micro hat hierzu mit **AWS und Microsoft Azure** entsprechende **Datenverarbeitungsverträge** (Data Processing Addendum bzw. Data Protection Addendum, DPA) abgeschlossen, die die Verarbeitung personenbezogener Daten durch diese Anbieter als Unterauftragnehmer bzw. Unterauftragsverbeiter von Trend Micro gestattet. Diese Datenverarbeitungsverträge stellen unter anderem sicher, dass die Unterauftragsverbeiter Kundendaten nur gemäß den Weisungen von Trend Micro verarbeiten. AWS und Microsoft Azure haben außerdem geeignete technische und organisatorische Maßnahmen getroffen, und sie werden Trend Micro unverzüglich über einen Sicherheitsvorfall informieren, so dass Trend Micro den Kunden entsprechend informieren und der Kunde seinen **Verpflichtungen zur Meldung von Datenschutzverletzungen** gemäß der DSGVO nachkommen kann. Darüber hinaus beziehen auch diese Datenverarbeitungsverträge die **Standardvertragsklauseln** mit ein, so dass ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU an AWS und Microsoft Azure in die USA übermittelt werden, gewährleistet ist.

Trend Micro stellt auf seiner Webseite unter https://www.trendmicro.com/en_us/about/legal/subprocessors.html eine **Liste der Auftragsverarbeiter und Unterauftragsverarbeiter** nach Produkten und Diensten zur Verfügung, die regelmäßig aktualisiert wird und in der alle mit Trend Micro verbundenen Unternehmen und Unterauftragsverarbeiter aufgeführt sind, die zur Verarbeitung von Kundendaten berechtigt sind.

VI. Sicherheitsanforderungen an Cloud-Dienste

Aufgrund der Anforderungen an die Verfügbarkeit von Cloud-Diensten und in Abhängigkeit vom Schutzbedarf der zu verarbeitenden Daten nimmt die IT-Security bzw. Sicherheit in der Informationstechnik von Cloud-Diensten eine zunehmend zentrale Rolle ein.

„Sicherheit in der Informationstechnik" bedeutet nach dem „Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik" (BSIG) „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen."

Nach § 8 Abs. 1 BSIG legt das BSI **Mindeststandards** für die Sicherheit der Informationstechnik des Bundes fest, was bzgl. der Nutzung externer Cloud-Dienste durch den Mindeststandard vom 15. Dezember 2022 (Version 2.1, abrufbar unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) erfolgt ist. Hiernach müssen die unter § 8 Abs. 1 BSIG fallenden Stellen und Einrichtungen des Bundes mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.

VII. C5-Testat

1. Kriterienkatalog C5

Da Cloud Computing in den letzten Jahren stetig zugenommen hat und in vielen Bereichen zum Standard geworden ist, sieht es das BSI als seine Aufgabe an, sowohl Anbietern wie auch Anwendern Hilfen an die Hand zu geben, sodass Cloud Computing sicher angeboten und genutzt werden kann. Eine dieser Anwendungshilfen ist der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue). Er wurde 2016 erstmalig durch das BSI veröffentlicht, 2019 grundlegend überarbeitet und als neue Version „C5:2020" im Januar 2020 fertiggestellt (abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html). Der **Kriterienkatalog C5 spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden**. Er stellt für Cloud-Kunden eine wichtige Orientierung für die Auswahl eines Cloud-Anbieters dar und bildet die **Grundlage**, um ein **kundeneigenes Risikomanagement** durchführen zu können.

Der Kriterienkatalog C5 definiert „Cloud-Dienst" wie folgt: „Im Rahmen von Cloud Computing angebotenen Dienstleistung der Informationstechnik. Dies beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software." Er enthält Kriterien zur Informationssicherheit von Cloud-Diensten aus insgesamt 17 Bereichen wie Organisation der Informationssicherheit, physische Sicherheit, Identitäts- und Berechtigungsmanagement, Kryptographie und Schlüsselmanagement, Umgang mit Sicherheitsvorfällen, Business Continuity Management und Compliance, die ein umfassendes Spektrum an Cloud-Sicherheits- und Ausfallsicherheitsfunktionen abdecken. Die Kriterien gliedern sich ihrerseits in **Basiskriterien** und Zusatzkriterien, wobei die Basiskriterien aus Sicht des BSI das **Niveau an Informationssicherheit widerspiegeln, das ein Cloud-Dienst mindestens bieten muss**, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen normalen Schutzbedarf haben. Die **Basiskriterien bilden den Mindestumfang einer Prüfung nach dem Kriterienkatalog C5** ab. Die Zusatzkriterien stellen im Falle eines höheren Schutzbedarf einen Ausgangs- bzw. Ansatzpunkt für die Bewertung dar.

Der Nachweis der Konformität mit den C5-Kriterien, d.h. die Erteilung des C5-Testats, muss durch einen unabhängigen und sachverständigen Wirtschaftsprüfer unter Anwendung national und international etablierter Prüfungsstandards erfolgen. Der Wirtschaftsprüfer erbringt seine Tätigkeit gegenüber dem Cloud-Anbieter, nicht gegenüber dem Kunden des Anbieters.

2. C5-Testat von Trend Micro

Trend Micro hat im Januar 2023 das Testat nach den Kriterien des C5:2020-Standards (Cloud Computing Compliance Criteria Catalogue) erhalten, das u.a. Trend Vision One umfasst. Die **unabhängige Prüfung nach dem Kriterienkatalog C5 wurde von der Wirtschaftsprüfungsgesellschaft** Deloitte & Touche, Taiwan, durchgeführt und der Prüfungsbericht wird Kunden von Trend Micro auf Anfrage zur Verfügung gestellt.

VIII. Risikomanagement des Kunden

Das C5-Testat bietet Kunden eine wichtige Orientierung für die Auswahl eines Cloud-Anbieters. Allerdings muss der Kunde weiterhin ein **kundeneigenes Risikomanagement** durchführen, wenn er einen Cloud-Dienst anwenden möchte. Auf Grundlage des C5-Prüfungsberichts können sich Kunden ein angemessenes Bild von der Informationssicherheit des Cloud-Dienstes einschließlich der angewandten Grundsätze, Verfahren und Maßnahmen verschaffen. Dies soll dem Kunden ermöglichen, die **Eignung des Cloud-Dienstes für seinen Anwendungsfall zu beurteilen**, und es ihm erleichtern, mehrerer Cloud-Anbieter bzw. Cloud-Dienste, für die ein C5-Bericht ausgestellt wurde, zu vergleichen. Potenzielle Cloud-Kunden sollten ihre Entscheidung nicht nur auf eine vorhandene, aktuelle Berichterstattung nach diesem Kriterienkatalog gründen (unabhängig, ob diese sich auf die Basis- oder Zusatzkriterien bezieht), sondern sollten sich die Berichterstattung des Wirtschaftsprüfers vom Cloud-Anbieter regelmäßig vorlegen lassen und diese für ihren Anwendungsfall bewerten.

Die **Basiskriterien** spiegeln aus Sicht des BSI das Niveau an Informationssicherheit wider, das ein Cloud-Dienst mindestens bieten muss, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen **normalen Schutzbedarf** haben. Die Basiskriterien bilden den Mindestumfang einer Prüfung nach diesem Kriterienkatalog ab. **Nichtsdestotrotz obliegt es den Cloud-Kunden, für ihren individuellen Anwendungsfall zu bewerten, inwiefern die Basiskriterien den Schutzbedarf ihrer Informationen angemessen reflektieren.** Für Cloud-Kunden, deren Informationen einen höheren Schutzbedarf haben, können die Zusatzkriterien einen Ausgangs- bzw. Ansatzpunkt darstellen, um diese Bewertung vorzunehmen.

Die Kunden müssen zudem den **Mitwirkungspflichten** in ihrem Verantwortungsbereich nachkommen. Hierbei sind **korrespondierende Kriterien für Kunden** zu berücksichtigen, denn die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes obliegt nicht alleine dem Cloud-Anbieter. Die korrespondierenden Kriterien für Cloud-Kunden dienen dazu, aufzuzeigen, wo potenziell Mitwirkungspflichten bestehen und an welchen Stellen Cloud-Kunden eigene Maßnahmen entwickeln müssen, um die Sicherheit des Cloud-Dienstes zu gewährleisten. Es handelt sich dabei allerdings um keine abschließende und allgemein gültige Aufstellung.

Welche Lösungen von Trend Micro ein C5-Testat haben, finden Sie auch auf unserer dedizierten C5-Testat Webseite.

IX. Besondere Anforderungen beim Einsatz von Cloud-Diensten durch Banken und Versicherungen

Banken und Versicherungen unterliegen beim Einsatz von Cloud-Diensten zusätzlichen besonderen Anforderungen. Nach § 25b Kreditwesengesetz (KWG) müssen Kreditinstitute und Finanzdienstleistungsinstitute angemessene Vorkehrungen treffen, um übermäßige zusätzliche Risiken zu vermeiden, wenn sie Aktivitäten und Prozesse auf ein anderes Unternehmen auslagern, die für die Durchführung von Bankgeschäften oder Finanzdienstleistungen wesentlich sind. Insbesondere muss ein **angemessenes und wirksames Risikomanagement** durch das Institut gewährleistet bleiben, das die ausgelagerten Aktivitäten und Prozesse einbezieht. Eine solche Auslagerung im Finanz- und Versicherungssektor kann auch an Cloud-Anbieter erfolgen.

In diesem Zusammenhang sind die **„Mindestanforderungen an das Risikomanagement – MaRisk"** der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu beachten, die die aus § 25b KWG resultierenden Anforderungen präzisieren. Die MaRisk umfasst insbesondere die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren und regelt im Modul AT 9 die Auslagerung umfassend. Banken und Finanzdienstleister müssen diese organisatorischen Pflichten beachten – insbesondere bei der Auslagerung von IT-Dienstleistungen, auch wenn diese in die „Cloud" erfolgt.

Zudem hat die BaFin die „Bankaufsichtlichen Anforderungen an die IT" (BAIT) veröffentlicht. Die BAIT geben einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute – insbesondere für das Management der IT-Ressourcen, das Informationsrisikomanagement und das Informationssicherheitsmanagement – vor, und präzisieren die Anforderungen des § 25b KWG. Für Zahlungs- und E-Geld-Institute gelten die an die BAIT angelehnten „Zahlungsdiensteaufsichtlichen

Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)“ und für Versicherungen die ähnlichen „Versicherungsaufsichtlichen Anforderungen an die IT“ (VAIT) der BaFin.

Schließlich ist die **„Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“** (abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_181108_orientierungshilfe_cloud_anbieter.html;jsessionid=43AD361CA056D3E7C3FB01FFE7BC7202.2_cid502?nn=9021442) von Bedeutung, mit der die BaFin und die Deutsche Bundesbank bei den betroffenen Unternehmen, insbesondere Kreditinstitute, Finanzdienstleistungsinstitute und Versicherungsunternehmen, **ein Problembewusstsein im Umgang mit Cloud-Diensten** und den damit verbundenen **aufsichtsrechtlichen Anforderungen** schaffen wollen. Sie weist auf wesentliche Aspekte hin, die solche Unternehmen bei einer Auslagerung an Cloud-Anbieter insbesondere im Rahmen der Risikoanalyse und der Vertragsgestaltung beachten sollten. Im Rahmen ihrer strategischen Überlegungen sollen die Unternehmen nach der Orientierungshilfe „einen Prozess entwickeln und dokumentieren, der alle für die Auslagerung an den Cloud-Anbieter relevanten Schritte von der Strategie über die Migration in die Cloud bis hin zur Exit-Strategie abdeckt“. Im Rahmen der durchzuführenden **Risikoanalyse** sollten u.a. die folgenden Punkte berücksichtigt werden:

- die Ausgestaltung des genutzten Cloud-Dienstes,
- die Kritikalität des auszulagernden Sachverhalts,
- eine **Bewertung** der finanziellen, operationellen (z.B. Systemausfall, Sabotage) und rechtlichen Risiken (z.B. **datenschutzrechtliche Risiken**) sowie Reputationsrisiken; dazu zählen auch Erwägungen zum Standort der Datenspeicherung und der Datenverarbeitung,
- eine **Bewertung der Eignung des Cloud-Anbieters** (Fähigkeiten, Infrastruktur, wirtschaftliche Situation, gesellschaftsrechtlicher und regulatorischer Status, etc.),
- eine Bewertung der Risiken für die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität der Sachverhalte sowie der verarbeiteten oder gespeicherten Daten.

In Bezug auf die Bewertung der Eignung des Cloud-Anbieters führt die BaFin ausdrücklich aus, dass hierfür **Nachweise bzw. Zertifikate auf Basis gängiger Standards** (z.B. ISO/IEC 2700X, **C5-Anforderungskatalog des BSI**), Prüfberichte anerkannter Dritter oder interne Prüfberichte des Cloud-Anbieters herangezogen werden können.

Beim Einsatz von Cloud-Diensten durch Banken und Versicherungen sind also zusätzliche bankaufsichtliche bzw. versicherungsaufsichtliche Anforderungen einzuhalten. Hierbei haben die betroffenen Unternehmen eine **Risikoanalyse** durchzuführen. Hierbei ist u.a. die **Eignung des Cloud-Anbieters** zu bewerten, wobei ein **C5-Testat** herangezogen werden kann.

Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html

Stand: Juni 2023