TRUMPF Anforderungen Cyber Security

Cybersicherheit hat für TRUMPF einen hohen Stellenwert und TRUMPF unternimmt erhebliche Anstrengungen, um ein angemessenes Schutzniveau für Informationen und Daten zu schaffen und aufrechtzuerhalten. Von Lieferanten fordert TRUMPF folglich ein adäquates Cyber Sicherheitsniveau. Die Anforderungen an Lieferanten sind in diesem Dokument beschrieben und der Auftragnehmer wird auf dessen Einhaltung verpflichtet.

A. Allgemeiner Teil: Allg. Anforderungen an Lieferanten

1. Produktbezogene Anforderungen

1.1. Für Hard- und Softwarekaufverträge gilt Folgendes:

Der Lieferant gewährleistet, dass der Liefergegenstand im Zeitpunkt des Gefahrübergangs dem aktuellen Stand der Technik entspricht. Darunter fallen z.B. Schutz gegen Schadsoftware (z.B. Trojaner, Viren, Spyware usw.), Informationssicherheits- und Datensicherungsmaßnahmen, die Beachtung von geltenden Datenschutzanforderungen an Software sowie sämtliche Vorkehrungen und Maßnahmen nach dem jeweils aktuell anerkannten Stand der ITK-Technik. Der Lieferant gewährleistet, dass der Liefergegenstand durch geeignete technische Schutz- sowie Härtungsmaßnahmen bestmöglich nach aktuellem Stand der Technik gesichert ist und dies nachweislich durch entsprechende technische Prüfungen durch den Lieferanten erfolgt ist [wie beispielsweise durch folgende Erfordernisse für eine technische Überprüfung: statische Codeanalyse (SAST), Schwachstellenanalysen mit Schwachstellenscannern (DAST) und/oder eine korrekte Verarbeitung von Eingabedaten in die Software mit Hilfe von Fuzzing / Robustness Testing]. Zusätzlich hat der Lieferant TRUMPF im Falle von Softwareprodukten eine Stückliste (SBOM - Software bill of materials) zur Verfügung zu stellen, in der alle in der Software enthaltenen Software(unter-)komponenten von Drittanbietern insbesondere Open-Source Software aufgeführt sind. Der Lieferant gewährleistet TRUMPF, dass die Liste der Software von Drittanbietern zum Zeitpunkt der an TRUMPF gelieferten Hardware/Software sich auf dem neuesten Stand befindet.

1.2. Im Übrigen gilt Folgendes:

Der Lieferant wird bei der Leistungserbringung den aktuellen Stand der Technik beachten. Darunter fallen z.B. Schutz gegen Schadsoftware (z.B. Trojaner, Viren, Spyware usw.), Informationssicherheits- und Datensicherungsmaßnahmen, die Beachtung von geltenden Datenschutzanforderungen an Software sowie sämtliche Vorkehrungen und Maßnahmen nach dem jeweils aktuell anerkannten Stand der ITK-Technik. Jedes neue Update, Upgrade, Release oder sonstige neue Version von Software wird vom Lieferanten vor Bereitstellung durch geeignete technische Schutz- sowie Härtungsmaßnahmen bestmöglich nach aktuellem Stand der Technik gesichert und dies erfolgt nachweislich durch entsprechende technische Prüfungen durch den

Lieferanten [wie beispielsweise durch folgende Erfordernisse für eine technische Überprüfung: statische Codeanalyse (SAST), Schwachstellenanalysen mit Schwachstellenscannern (DAST) und/oder eine korrekte Verarbeitung von Eingabedaten in die Software mit Hilfe von Fuzzing / Robustness Testing].

2. Organisationsbezogene Anforderungen

2.1. Der Lieferant ist verpflichtet:

a. sofern die vertragsgegenständlichen Leistungen in der Überlassung oder Zugänglichmachung von Software bestehen: einen sicheren Software Development Lifecycle zu implementieren. Dies umfasst die kontinuierliche Schulung von Softwareentwicklern zu sicherheitsbezogenen Aspekten der Softwareentwicklung;

b. ein Schwachstellenmanagement zu unterhalten und hierbei mindestens (1) seine vertragsgegenständlichen Produkte und Leistungen kontinuierlich auf Informationssicherheits- oder Datenschutzschwachstellen zu überprüfen und TRUMPF unverzüglich über entdeckte Informationssicherheits- oder Datenschutzschwachstellen zu informieren und diese ggf. nach gültigen Standardmetriken (bspw. CVSS) zu bewerten und an cybersecurity.external@trumpf.com und diese innerhalb der vereinbarten Fristen, anderenfalls innerhalb angemessener Frist, zu beheben sowie (2) von TRUMPF oder Dritten mitgeteilte Informationssicherheits- oder Datenschutzschwachstellen zu lokalisieren, analysieren und diese innerhalb der vereinbarten Fristen, anderenfalls innerhalb angemessener Frist, zu beheben;

2.2 TRUMPF ist berechtigt, einen Nachweis über die Einhaltung der vorstehenden Verpflichtungen sowie Nachweise über die Informationssicherheit wie z.B. Zertifikate, Ergebnisse von Penetrations- oder Schwachstellentests mindestens einmal kalenderjährlich zu verlangen.

2.3 Weiter verpflichtet sich der Lieferant wesentliche Änderungen mit Auswirkung auf Informationssicherheit, wie beispielsweise Technologiewechsel oder der Entzug / Ablauf von Zertifikaten an TRUMPF zu melden. Für den Fall, dass dadurch wesentliche negative Auswirkungen auf das Sicherheitsniveau resultieren, ist TRUMPF berechtigt vom Vertrag außerordentlich zurücktreten.

2.4 Der Lieferant übergibt die verarbeiteten Informationen, alle erforderlichen Unterlagen und ggfs. Software, die im Auftrag von TRUMPF erstellt wurde, an TRUMPF in einem vereinbarten Format und zeitlich angemessen, falls die Fortführung der

Leistungserbringung nicht gewährleistet ist. Dies ist insbesondere der Fall, wenn der Lieferant nicht mehr in der Lage ist, Produkte oder Dienstleistungen bereitzustellen.

2.5 Soweit gesetzlich zulässig wird der Lieferant juristisch jeglichen Rechtsweg ausschöpfen, bevor es zu einer Weitergabe von Kundendaten kommt. Darüber hinaus wird der Lieferant, falls es nicht strikt untersagt ist, TRUMPF über die Weitergabe informieren und um Zustimmung bitten.

2.6 Der Lieferant verpflichtet seine Subunternehmer zur Einhaltung aller zuvor genannten Anforderungen in der gesamten Prozesskette entsprechend.

2.7 Die Regelungen in dieser Anlage schränken die sonstigen vereinbarten vertraglichen Verpflichtungen des Lieferanten in keinem Fall ein.

B. Besonderer Teil: Anforderungen an Lieferanten in Ergänzung des Allgemeinen Teils auf bestimmte organisationsbezogenen / unterschiedliche Lieferanten-Kategorien

Die Gültigkeit für die organisationsbezogenen Anforderungen sind unterteilt in drei unterschiedliche Lieferanten-Kategorien, die nachfolgend beschrieben und in den darauffolgenden Ziffern durch die definierten Kürzel gekennzeichnet sind:

1. Full Managed Services (FS): Der Lieferant erbringt den Service über den durch ihn definierten Rahmen (Lokationen, Hardware, Software, Prozesse und technische Konzepte). Der Lieferant kann für die Leistungserbringung gegenüber dem Auftraggeber weitere IT-Dienstleister einbinden (Weiterverlagerung an Subdienstleister). Es gilt für den Leistungsgegenstand das Informationssicherheitsmanagementsystems (ISMS) des Auftragnehmers.

Beispiele: Bereitstellung von Software-as-a-Service Lösungen (z.B. MS Office 365)

2. Remote Managed Services (RS): Der Lieferant erbringt Services in den Lokationen von TRUMPF oder durch von TRUMPF beauftragten Dritten. Der Lieferant greift über ein durch ihn verwaltete IT-Infrastruktur auf die IT-Infrastruktur bei TRUMPF zu (Remote Access). Der Zugriff erfolgt gemäß den durch TRUMPF bereitgestellten Verfahren. Die Services werden nach von TRUMPF vorgegebenen Richtlinien, Betriebsprozessen, technischen Konzepten und innerhalb des Informationssicherheitsmanagementsystems (ISMS) von TRUMPF erbracht.

Beispiele: Administration von Komponenten der IT-Infrastruktur (OnPrem oder Cloud)

3. Support Services (SS): Der Lieferant erbringt einen Service in Rahmen eines Beratungsvertrages oder Wartungsvertrages für Hardware/Software und erhält vertrauliche Daten von TRUMPF zur Leistungserbringung. Die Verarbeitung und Speicherung der

vertraulichen TRUMPF Daten erfolgt in der IT-Infrastruktur des Lieferanten nach seinem Informationssicherheitsmanagementsystem (ISMS).

Beispiele: Managementberatung, Softwarewartung mit Fehler-analysen / Fernwartung, Wirtschaftlichkeitsberechnungen, Marktanalysen, sonstige Verarbeitung von vertraulichen oder geschäftskritischen Informationen von TRUMPF

Der Lieferant ist verpflichtet:

a. ein *Information Security Management System (ISMS)* gemäß ISO 27000 ff. oder gleichwertiger Standards zu unterhalten [FS/RS/SS];

b. die TRUMPF Informationen, die zur vertragsgegenständlichen Leistung notwendigen IT-Systeme sowie die Datenübertragungen über angemessene Schutzmaßnahmen abzusichern, die den aktuellen Stand der Technik beachten sowie den Least-Privilege und Need-to-Know Prinzipien entsprechen [FS/RS/SS];

c. die Netzwerkzugänge aus dem Internet über eine starke Authentifizierung (z.B. Multi-Faktor-Authentifizierung) abzusichern. Die Passwörter für den Zugriffsschutz müssen angemessene Regeln für Länge und Komplexität erzwingen [FS/RS/SS];

d. bei Informationssicherheitsvorfälle, die die Schutzziele für Unternehmenswerte von TRUMPF betreffen (1) TRUMPF unverzüglich über erkannte Sicherheitsvorfälle zu unterrichten (cybersecurity.external@trumpf.com), (2) bei Gefahr in Verzug geeignete und angemessene Maßnahmen zu ergreifen, um die Schutzziele für die Unternehmenswerte von TRUMPF vor der Gefahr zu schützen, (3) die im Rahmen eines Sicherheitsvorfalls ergriffenen Maßnahmen nachvollziehbar zu dokumentieren und die Dokumentation TRUMPF auf Anfrage bereitzustellen, (4) die Veröffentlichung der Information über einen Sicherheitsvorfall mit TRUMPF abzustimmen; (5) bei verdächtigem Verhalten oder unerklärbaren Ausfällen der Systeme des Lieferanten, wo auch TRUMPF Daten gespeichert sind, auf den Systemen unverzüglich einzugreifen und ggf. nachfolgende forensische Untersuchungen auszuführen. Etwaige Protokolle für sicherheitsrelevante Ereignisse auf Systemen des Lieferanten sind zentral zu speichern sowie (6) die Anfragen von Behörden zu Auskünften über oder für die Übermittlung von Unternehmenswerten unverzüglich anzuzeigen und die weitere Vorgehensweise abzustimmen [FS/RS/SS];

e. seine Mitarbeiter zu Bedrohungen, Schutzmaßnahmen und Verhalten zum sicheren Umgang mit Informationen mind. einmal kalenderjährlich zu schulen [FS/RS/SS];

f. die für die Leistungserbringung notwendigen Verantwortlichkeiten, Mitwirkungspflichten und Beistellungspflichten mit TRUMPF abzustimmen und vertraglich zu vereinbaren [FS/RS/SS];

g. die Datensicherungs- und Wiederherstellungsprozesse abzustimmen und vertraglich zu vereinbaren. Dabei sind mindestens der Wiederherstellungszeitpunkt (RPO) und Wiederherstellungsdauer (RTO) zu definieren. Wenn die vertragsgegenständliche Leistung in TRUMPF Geschäftsprozessen zum Einsatz kommen, denen mindestens hohe Verfügbarkeitsanforderungen zugrunde liegen, sind die Wiederherstellungsprozesse und Notfallprozesse mind. einmal kalenderjährlich zu testen und TRUMPF ein geeigneter Nachweis darüber bereitzustellen [FS/RS];

h. die Datenverarbeitung und -speicherungen von TRUMPF Informationen nur in geeigneten Räumlichkeiten mit physischen Schutzmaßnahmen durchzuführen, die einen angemessenen Schutz vor Umwelteinflüssen und dem Zutritt/Zugriff von unbefugten Dritten bieten [FS/SS];

i. sofern TRUMPF Informationen auf Systemen des Lieferanten verarbeitet und gespeichert werden, muss ein zentrales Logmanagement mit einer kontinuierlichen Auswertung von sicherheitsrelevanten Protokollen die Vertraulichkeit und Integrität der Informationen überwachen [FS/SS];

j. sofern die vertragsgegenständliche Leistung in TRUMPF Geschäftsprozessen zum Einsatz kommen, denen mindestens hohe Verfügbarkeitsanforderungen zugrunde liegen, müssen die Serverräume der Schutz- und Verfügbarkeitsklasse 3 der DIN EN 50600 in der jeweils gültigen Fassung genügen [FS];

k. ein Berichtswesen über kundenrelevante Informationssicherheitsrisiken zu unterhalten, dass den folgenden Anforderungen genügt: (1) Bereitstellung über einen regelmäßigen Berichtszyklus, jedoch mind. einmal im Kalenderjahr, mit einer Übersicht über die (2) identifizierten kundenrelevanten Risiken und deren Maßnahmen; (3) durchgeführten Sicherheitsaudits (z.B. Penetrationstests); (4) durchgeführten Security-Awareness-Maßnahmen [FS].