Spezielle Einkaufsbedingungen Cyber-Sicherheit für die Bosch Sicherheitssysteme GmbH

Inhaltsverzeichnis

1. Präambel

Diese Vereinbarung regelt die vertraglichen Bedingungen im Zusammenhang mit der Lieferung von Produkten und der Erbringung von Leistungen ("Vertragsprodukte und -leistungen") durch den LIEFERANTEN oder die Konzerngesellschaften des LIEFERANTEN (mit LIEFERANT verbundene Unternehmen gemäß § 15 AktG) an die Robert Bosch GmbH und an alle Gesellschaften, die von der Robert Bosch GmbH direkt oder indirekt kontrolliert werden (im Folgenden "Bosch" genannt). Der Begriff "kontrolliert" bedeutet, dass an einer Gesellschaft mehr als 50 Prozent der Stimmrechte gehalten werden und deren Geschäftsführung bestimmt werden kann).

Die Vereinbarung legt die grundlegenden Cyber-Sicherheitsanforderungen von Bosch fest, welche für Lieferanten zwingend erforderlich sind, die Dienste wie Software, IT-Dienstleistungen oder System-on-Chips (sowohl mikroprozessorbasiert als auch mikrocontrollerbasiert) anbieten oder andere Hardwarekomponenten mit integrierter Firmware/Software (von Bosch als "sicherheitsrelevante Komponenten" definiert) an Bosch liefern.

Definitionen der in diesem Dokument verwendeten Begriffe finden Sie im Anhang B.

2. Allgemein

Der Lieferant hat die Cyber-Sicherheit sowohl seines Betriebs als auch seiner Lieferungen und Leistungen zu gewährleisten. Zu diesem Zweck hat der Lieferant unter Berücksichtigung des Standes der Technik angemessene, branchenübliche technische und organisatorische Maßnahmen zu treffen und diesen Vertrag einzuhalten. Alle sonstigen zwischen den Parteien vereinbarten Vereinbarungen und Bedingungen (z.B. Einkaufsbedingungen der Robert Bosch GmbH - abrufbar unter www.bosch.com) bleiben unberührt. Im Falle von Widersprüchen zu den vorgenannten Vereinbarungen gehen diese speziellen Bedingungen für Cyber-Sicherheit vor.

3. Cyber-Sicherheit im Betrieb des Lieferanten

3.1. Der Lieferant ist verpflichtet, bei seinen Betriebsabläufen die Cyber-Sicherheit entsprechend branchenüblichen Standards einzuhalten. Der Lieferant hat jedoch mindestens ein angemessenes Managementsystem für Informationssicherheit einzurichten und aufrechtzuerhalten z. B. gemäß ISO/IEC 27001.

3.2. Die Einhaltung spezifischer Anforderungen an die Cyber-Sicherheit im Betrieb des Lieferanten wird in Anhang A vereinbart.

3.3. Der Lieferant trägt dafür Sorge, dass das von ihm zur Einrichtung und Aufrechterhaltung der Cyber-Sicherheit eingesetzte Personal angemessen ausgebildet und qualifiziert ist.

3.4. Der Lieferant sorgt dafür, dass eingesetztes Personal regelmäßig geschult und für Fragen der Einhaltung der Vorschriften und Standards der Cyber-Sicherheit und des Datenschutzes sensibilisiert wird.

4. Cyber-Sicherheit der Lieferungen und Leistungen des Lieferanten

4.1. Der Lieferant ist verpflichtet, branchenübliche Normen, Standards, Prozesse und Methoden einzuhalten, die dem aktuellen Stand der Technik entsprechen, um Cyber-Sicherheitsrisiken, die sich insbesondere aus Schwachstellen oder Schadsoftware in Lieferungen und Leistungen ergeben können, zu verhindern, zu identifizieren, zu bewerten und zu beheben.

4.2. Für bestimmte Lieferungen und Leistungen werden spezifische cyber-sicherheitsbezogene Anforderungen entsprechend Anhang A verbindlich vereinbart.

4.3. Bosch ist berechtigt, auch während einer laufenden Geschäftsbeziehung die Abnahme von Lieferungen und Leistungen vom Nachweis der aktuellen Zertifizierung der vereinbarten spezifischen Cyber-Sicherheitsanforderungen in Anhang A abhängig zu machen.

4.4. Sofern nicht abweichend vereinbart, muss die in den Lieferungen und Leistungen enthaltene Software (einschließlich der Software und Softwarekomponenten von Drittanbietern) zum Zeitpunkt der Lieferung oder des Beginns der Dienstleistung auf dem aktuellen Stand sein, einschließlich aller verfügbaren Sicherheitsupdates. Außerdem sind Anweisungen zur Installation von Sicherheitsupdates beizufügen.

4.5. Alle Schnittstellen der Lieferungen und Leistungen, die von außerhalb der Bosch-Systeme oder der Umgebung, in der diese Systeme betrieben werden sollen, zugänglich sind, müssen in Abstimmung mit Bosch spezifiziert und eindeutig dokumentiert werden. Dies gilt auch für automatische Datenverbindungen, z. B. über Wartungsschnittstellen, Software-Aktualisierungsmechanismen oder Kontrollkanäle, um einen Informationsaustausch mit Systemen des Lieferanten oder Dritter zu ermöglichen.

4.6. Soweit kryptographische Systeme in einer Lieferung oder Leistung enthalten sind, muss der Lieferant den Stand der Technik, den beabsichtigten Anwendungskontext und die erwartete Lebensdauer der Lieferungen und Leistungen berücksichtigen und dementsprechend geeignete kryptografische Mechanismen, ihre Konfigurationen, Schlüssellängen und Aktualisierungs-/Erweiterungsmöglichkeiten auswählen.

4.7. Der Lieferant ist für die Einhaltung aller Gesetze und/oder behördlichen Anforderungen in Bezug auf die verwendete Kryptographie verantwortlich, die für Lieferungen und Leistungen an Bosch gelten.

4.8. Der Lieferant garantiert und gewährleistet, dass die Lieferungen und Leistungen keine Schadsoftware oder manipulierte sowie gefälschte Komponenten Dritter enthalten. Dies und dass keine Anhaltspunkte für eine Nichtkonformität festgestellt wurden, hat der Lieferant nach dem Stand der Technik zu überprüfen und auf Anfrage schriftlich zu bestätigen.

4.9. Der Lieferant muss eine vollständige Stückliste in einem gängigen Dateiformat vorlegen, aus dem alle Hardware- und Softwarekomponenten (einschließlich Open-Source-Komponenten), die in den Lieferungen und Leistungen enthalten sind, in einer klaren Struktur hervorgehen. Dieses Verzeichnis wird auch als "Bill of Material" bezeichnet. Einzelheiten sind Anhang C zu entnehmen.

4.10. Die Stückliste *(„Bill of Material“)* ist auf dem neuesten Stand zu halten und bei Änderungen sowie auf Anfrage erneut bereitzustellen.

4.11. Bosch ist berechtigt, den Inhalt des vom Lieferanten zur Verfügung gestellten Stückliste ganz oder teilweise an Dritte, insbesondere an Abnehmer / Kunden von Bosch-Produkten und -Dienstleistungen, weiterzugeben.

5. Aufrechterhaltung der Cyber-Sicherheit & Meldepflichten

5.1. Der Lieferant gewährleistet die Cyber-Sicherheit von Lieferungen und Leistungen über den Zeitpunkt des Gefahrübergangs hinaus jedoch mindestens für die vereinbarte Lebensdauer bestimmter Lieferungen bzw. während des vereinbarten Zeitraums von Leistungen. Wurde keine bestimmte Lebensdauer vereinbart, so gewährleistet der Lieferant die Cyber-Sicherheit der Lieferungen und Leistungen für einen angemessenen Zeitraum, der nach dem jeweiligen Vertragszweck vernünftigerweise erwartet werden kann.

5.2. Der Lieferant ist verpflichtet, Bosch unverzüglich und unentgeltlich über alle eingetretenen oder vermuteten cyber-sicherheitsrelevanten Ereignisse zu informieren, die sich auf den Betrieb oder die Lieferungen und Leistungen des Lieferanten auswirken, wenn und so weit Bosch, die Kunden von Bosch oder die Lieferungen und Leistungen tatsächlich oder wahrscheinlich davon betroffen sind. Informationen zur Meldung von cyber-sicherheitsrelevanten Ereignissen, einschließlich Schwachstellen finden Sie im Anhang C.

5.3. Der Lieferant benennt einen festen und fachlich qualifizierten, für Cyber-Sicherheit zuständigen Ansprechpartner innerhalb seiner Organisation, der für alle Cyber-Sicherheitsanfragen von Bosch in Bezug auf Lieferungen und Leistungen des Lieferanten zur Verfügung steht. Die Kontaktperson muss per E-Mail und Telefon während der üblichen Geschäftszeiten erreichbar sein, die mindestens Montag bis Freitag zwischen 9 und 17 Uhr CET umfassen. Die Reaktionszeit für die Bestätigung von Bosch-Anfragen beträgt maximal 2 Arbeitstage. Der Lieferant ist verpflichtet, uns über Änderungen des Ansprechpartners unverzüglich schriftlich zu informieren. Im Gegenzug ist, sofern nicht anders angegeben, das Bosch Product Security Incident Response Team (Bosch PSIRT) Ansprechpartner für den Erhalt sicherheitsrelevanter Informationen und kann über die E-Mail-Adresse psirt@bosch.com erreicht werden. (Für Integrator Business ist ie.soc@de.bosch.com zu verwenden)

5.4. Soweit cyber-sicherheitsrelevante Ereignisse in Lieferungen und Leistungen ein Risiko für Produkte oder

Kunden von Bosch darstellen können, wird der Lieferant Bosch unentgeltlich bei der Ergreifung angemessener Maßnahmen zur Sachverhaltsaufklärung, Ursachenermittlung und Schadensbegrenzung unterstützen und insbesondere alle verfügbaren relevanten Informationen unverzüglich zur Verfügung stellen.

5.5. Der Lieferant verpflichtet sich, Bosch während des in Abschnitt 5.1 genannten Zeitraums (Stand der Technik, Normen, Standards...) Fehlerkorrekturen oder Umgehungslösungen (Updates, Fixes oder Patches) zur Verfügung zu stellen, um bei Bedarf Fehler oder Schwachstellen zu beheben, die bei Zulieferer Produkten auftreten und sich auf die vereinbarte und/oder vernünftigerweise erwartete Cyber-Sicherheit und Funktionalität dieser Produkte auswirken, ohne zusätzliche Kosten und ohne unangemessene Verzögerung. Dies gilt auch für Komponenten, die von einem anderen Dritten als dem Lieferanten bereitgestellt werden.

5.6. Bosch ist berechtigt, Meldungen sowie deren Inhalt im Ganzen oder Auszügen, die Informationen über cybersicherheitsrelevante Ereignisse des Lieferanten enthalten, an Dritte, insbesondere an betroffene Kunden von Bosch-Produkten und -Dienstleistungen, weiterzugeben.

6. Cyber-Sicherheits- und Penetrationstests

6.1. Bosch oder von Bosch beauftragte qualifizierte Dritte sind jederzeit berechtigt (aber nicht verpflichtet), Lieferungen und Leistungen auf Schadsoftware oder andere Schwachstellen zu testen, die möglicherweise zu Cyber-Sicherheitsvorfällen führen können. In diesem Fall wird der Lieferant angemessene Unterstützung leisten, um die Tests zu ermöglichen. Insbesondere wird der Lieferant unterstützen, indem er alle für diesen Zweck erforderlichen Zustimmungen von Dritten rechtzeitig einholt und auf Anfrage deren Vorhandensein unverzüglich nachweist.

7. Verpflichtung Dritter

7.1. Der Lieferant stellt sicher, dass alle vorgenannten Verpflichtungen (oder Verpflichtungen, die in ihren Anforderungen mindestens die gleichen Standards festlegen) in die vertraglichen Beziehungen mit seinen Unterlieferanten einbezogen werden, soweit sie für die in den Geltungsbereich dieses Dokuments fallenden Lieferungen relevant sind.

8. Informationsanfragen

8.1. Auf Anfrage stellt der Lieferant Bosch allgemeine Informationen über die für den Betrieb und/oder die Lieferungen und Leistungen des Lieferanten getroffenen Cyber-Sicherheitsmaßnahmen zur Verfügung.

8.2. Auf Anfrage muss der Lieferant die Einhaltung der vereinbarten spezifischen Cyber-Sicherheitsanforderungen gemäß Abschnitt 3.2 oder 4.2 nachweisen (z.B. durch allgemein anerkannte Prüfberichte).

8.3. Auf Anfrage stellt der Lieferant einen detaillierten Cyber-Sicherheitsbericht für einen bestimmten Zeitraum in Bezug auf den Betrieb des Lieferanten und/oder seine Lieferungen und Leistungen zur Verfügung. Dies umfasst insbesondere die Ergebnisse regelmäßiger Cyber-Sicherheitsinspektionen, die Dokumentation der identifizierten Cyber-Sicherheitsrisiken und der ergriffenen Maßnahmen, die Dokumentation von Cyber-Sicherheitsvorfällen einschließlich ihrer Ursachen, Abhilfemaßnahmen und Maßnahmen zur Verhinderung einer Wiederholung.

8.4. Der Lieferant hat Informationen gemäß diesem Abschnitt unverzüglich und auf eigene Kosten zur Verfügung zu stellen.

8.5. Sofern Formulare oder Fragebögen zur Informationsanforderung bereitgestellt werden, sind diese vom Lieferanten zu nutzen.

8.6. Alle Unterlagen des Lieferanten, die für diese Vereinbarung relevant sind, sind vom Lieferanten für einen Zeitraum von mindestens *15 Jahren* aufzubewahren.

9. Audits

9.1. Bosch behält sich das Recht vor, mit einer angemessenen Vorankündigung von mindestens zwei (2) Wochen, die Einhaltung der in diesem Vertrag festgelegten Verpflichtungen durch den Lieferanten auf eigene Kosten zu überprüfen.

9.2. Die Prüfung kann mit Hilfe von qualifizierten Dritten ("Auditoren") erfolgen, die auch Bosch gegenüber zur Verschwiegenheit über Geschäfts- und Betriebsgeheimnisse des Lieferanten verpflichtet sind. Die Auditoren werden insbesondere die Einhaltung der geltenden Richtlinien, Prozesse und Verfahren im Sinne der Ziffern 3.1 und 3.2 sowie die Beschaffungsprozesse des Lieferanten auditieren. Der Lieferant wird das Audit ohne zusätzliche Kosten unterstützen und den Auditoren die für das Audit erforderlichen Informationen zur Verfügung stellen.

9.3. Bei der Durchführung des Audits hat der Lieferant dafür Sorge zu tragen, dass Auditoren keine personenbezogenen Daten Dritter übermittelt oder sonst in irgendeiner Form offengelegt werden. Soweit dies nicht durch verhältnismäßige Maßnahmen in Teilen oder insgesamt sichergestellt werden kann, wird von einem Audit abgesehen.

9.4. Wird bei einer Überprüfung die Nichteinhaltung der in diesen Bedingungen festgelegten Anforderungen an die Cyber-Sicherheit festgestellt, hat der Lieferant diese unverzüglich zu beheben und die Einhaltung gemäß diesen Bedingungen wiederherzustellen.

9.5. Wird bei einer Überprüfung die Nichteinhaltung der in diesen Bedingungen festgelegten Anforderungen an die Cyber-Sicherheit in nicht unerheblichem Ausmaß festgestellt, trägt der Lieferant die Kosten des Audits.

10. Sonstiges

10.1. Die Rechte und Pflichten aus diesem Abkommen können nur mit vorheriger schriftlicher Zustimmung der anderen Vertragspartei delegiert, übertragen oder abgetreten werden. Die Nichtausübung eines in diesem Abkommen vorgesehenen Rechts stellt keinen Verzicht auf frühere oder spätere Rechte dar. Dieses Abkommen - einschließlich der vorliegenden Vereinbarung - kann nur durch eine schriftliche Vereinbarung geändert werden, die von allen Parteien unterzeichnet ist.

10.2. Alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag werden gemäß der zwischen den Parteien im bestehenden Vertragsrahmen vereinbarten Rechtswahl und Streitbeilegung gelöst (z. B. Rahmenvertrag).

10.3. Bei Unklarheiten, insbesondere bzgl. der Bedeutung, des Umfangs oder der Anwendbarkeit dieser Geschäftsbedingungen, wird sich der Lieferant an seinen Ansprechpartner in der entsprechenden Bosch-Fachabteilung wenden.

Anhang A: Spezielle Einkaufsbedingungen Cyber-Sicherheit (Zertifizierungen)

Der Lieferant ist verpflichtet, folgende spezifische cyber-sicherheitsbezogene Anforderungen einzuhalten und durch gültige Zertifizierung nachzuweisen. Wenn Anforderungen spezifiziert werden müssen, die nicht in der Anlage aufgeführt sind, fügen Sie bitte die entsprechenden Felder hinzu.

ISO/IEC 27001 ☐

Besondere Einschränkungen oder Rahmenbedingungen:

IEC 62443 ☐

Besondere Einschränkungen oder Rahmenbedingungen:

Wichtiger Hinweis: Für Lieferanten von Komponenten für Bosch-Kameras muss der Lieferant die Anforderungen der IEC62443-4-1 erfüllen, falls die Komponente speziell für die Kameras entwickelt wurde und Auswirkungen auf die Sicherheit haben kann

Anhang B: Begriffsdefinitionen

„Betrieb des Lieferanten“ bedeutet die Gesamtheit der wirtschaftlichen Einrichtungen des Lieferanten. Umfasst sind insbesondere seine Standorte, einschließlich ihrer Produktions- und Verwaltungseinrichtungen sowie verwendeter Komponenten, (Informations-)Systeme, Daten und Prozesse.

„Cyber-Sicherheit (Cyber-Security)” bedeutet Herstellung und Aufrechterhaltung der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität von Daten und Informationen in der Informations- und Kommunikationstechnik.

„cyber-sicherheitsrelevante Ereignisse“ sind Ereignisse und/oder Vorfälle, die auf eine Verletzung der Cyber-Sicherheit hindeuten (wie z.B. Entdeckung von Schwachstellen, Datenverlust, IT-Störfällen, Cyber-Attacken, Befall mit Schadsoftware, Datenmissbrauch, Datenlecks und/oder unberechtigter Zugriff Dritter auf Systeme oder Daten). Dies gilt auch für Fälle, in denen ein begründeter Verdacht auf eine solche Verletzung besteht, einschließlich, aber nicht beschränkt auf, die Entdeckung von Sicherheitslücken und Schwachstellen.

„Hardware“ bezeichnet alle physikalischen Komponenten von Datenverarbeitungssystemen.

„Informationstechnologie“ bezeichnet sämtliche physischen Komponenten datenverarbeitender Systeme (Hardware) sowie Computerprogramme einschließlich Daten (Software), unabhängig davon, ob diese Software als Bestandteil von Hardware oder als eigenständige Software betrieben werden kann.

„Schadsoftware“ (Malware) bedeutet schadenstiftende Software, wie z.B. Viren, Würmer, Trojaner, Spyware, Ransomware, Hintertüren oder andere Mechanismen, die einen unautorisierten Zugriff, veränderte Programmabläufe und/oder Nachladen weiterer derartiger Software in Lieferungen und Leistungen ermöglichen.

„Cyber-Sicherheitstests” bezeichnet Methoden zur Identifizierung von Schwachstellen mit potenziellen Auswirkungen auf die Cyber-Sicherheit. Sicherheitstests können unter anderem die Überwachung, Modifikation, Durchführung von Verifikation und Validierung in Form von Reviews, Fuzz-Tests, Schwachstellen-Scanning, Scannen der Betriebssystemkonfiguration, Secure-Code-Analyse, Codeüberprüfungen, Analyse der Softwarezusammensetzung, funktionale Sicherheitstests, Flooding, Binäranalyse einschließlich Dekompilierung, Brechen oder Umgehen von Sicherheitsmaßnahmen umfassen.

„Software” bedeutet Computerprogramme sowohl im Quell- als auch/oder im Objektcode einschließlich der enthaltenen Daten.

„Spezifische cyber-sicherheitsbezogene Anforderungen“ bezeichnet die in Anhang A genauer beschriebenen Anforderungen, deren Einhaltung der Lieferant verbindlich zusagt.

„Schwachstellen” meint jede Schwäche oder Unterschreitung vertraglich vereinbarter oder anwendbarer Industriestandards zur Cyber-Sicherheit, die im Falle einer Bedrohungsaktion/eines Angriffs oder/oder zur Durchführung unbefugter Handlungen innerhalb eines Netzwerks oder Computersystems ausgenutzt werden kann.

Anhang C: Anforderungen an den Informationsaustausch

1. Die „Software Bill of Material" (SBOM) wird in einem gemeinsamen Dateiformat geliefert, das derzeit als SPDX- oder CycloneDX-Format definiert ist, einschließlich der Kennzeichnung des gelieferten Produkts und aller Software-Komponenten Dritter und ist nicht auf Open Source-Komponenten beschränkt. Die SBOM umfasst mindestens:
    - Name und Version der Softwarekomponenten
    - Lizenzbedingungen Dritter (falls vorhanden)
    - CPE des ursprünglichen Lieferanten identifiziert die Komponenten eindeutig
    - Lieferant der Komponenten
    - Downloadort der Komponente, falls diese öffentlich verfügbar ist

2. Cyber-sicherheitsrelevante Ereignisse enthalten einen Schwachstellen-Report, der folgende Informationen enthält:
    - Informative Zusammenfassung (Beschreibung)
    - Eine eindeutige Tracking-ID
    - Eine Übersicht oder eine Liste der betroffenen Produkte inklusive Schnittstellen und Protokolle
    - CVSS-Basispunktzahl innerhalb des neuesten CVSS-Bewertungssystems und der betroffenen Produktklasse gemäß dem Standard des Common Vulnerability Scoring System
    - CVSS-Analyse (einschließlich CVSS Vector String und Begründung)
    - Bewertung der Auswirkungen des Vorfalls/der Schwachstelle des Produkts
    - Abhilfevorschläge, aktueller Status ("Abhilfemaßnahmen in Definition"/"geschlossen"),
    - Voraussichtliches Datum der nächsten Kundeninformation an Bosch, Verweise auf Schwachstellen und Quellen
    - Detaillierte Beschreibung des Angriffspfades und der Schwachstelle im Deliverable ("Abschlussbericht") innerhalb eines angemessenen Zeitraums
    - Kategorisierung nach Traffic Light Protocol (TLP)
    - Falls bekannt ist, dass die Sicherheitslücke ausgenutzt wird, sind Einzelheiten zu Auswirkungen und Eindämmungsmaßnahmen anzugeben und die Informationen sind als TLP rot (eingeschränkt) zu klassifizieren.
    - Regelmäßige Aktualisierung des Berichts, sofern sich die Informationen für den Bericht ändern