framatome

Cyber Security – Verpflichtungen des Auftragnehmers

Definitionen:

Auftragnehmer	Der als solcher im Vertrag Bezeichnete und seine Rechtsnachfolger.
Auftraggeber	Der als solcher im Vertrag Bezeichnete und seine Rechtsnachfolger.
Lieferungen und/oder Leistungen	Alle durch den Auftragnehmer und seine Subunternehmer nach dem Vertrag zu erbringenden Lieferungen und Leistungen.
Cybersicherheits-vorfall	Jedes Ereignis resultierend aus einer vorsätzlichen oder unbeabsichtigten Handlung oder Unterlassung, die ein Informationssystem oder die Daten, die das System verarbeitet, speichert oder überträgt, beschädigt oder beschädigen kann.
Feedback	Ein Ereignisbericht, der den Angriffsvektor des Cybersicherheitsvorfalles und die ordnungsgemäße Anwendung technischer und organisatorischer Maßnahmen zur Sicherstellung seiner Behebung identifiziert.

Bestimmungen:

1. Der Auftragnehmer bestätigt, dass er sich der geltenden Gesetze und Regelungen zur Informationssicherheit / IT-Sicherheit bewusst ist und verpflichtet sich dazu, diese einzuhalten, insbesondere Gesetze in Bezug auf das unbefugte Eindringen oder unbefugten Zugriff auf IT-Systeme, vorsätzliche Eingriffe in den Betrieb von Systemen und betrügerische Datenmanipulation.

2. Der Auftragnehmer wird dem Auftraggeber bei Vertragsabschluss die Kontaktdaten seines Beauftragten für Cyber Security / IT-Sicherheit mitteilen und Änderungen hierzu während der Vertragsausführung unverzüglich melden.

3. Für den Fall, dass dem Auftragnehmer ein rechtswidriger oder unbefugter Zugriff und/oder eine Nutzung von Daten und/oder IT-Systemen des Auftraggebers oder des Auftragnehmers bekannt wird oder der Auftragnehmer ein solches Ereignis vermutet, verpflichtet sich der Auftragnehmer, den Auftraggeber einen solchen (vermuteten) Cybersicherheitsvorfall schriftlich zu melden, sobald er davon Kenntnis erlangt und/oder er von einer für ihn direkt oder indirekt zuständigen Behörde hierüber benachrichtigt wird. In einem solchen Fall ergreift der Auftragnehmer alle geeigneten Maßnahmen, die ein sorgfältiger Auftragnehmer zum Schutz seiner Daten und/oder seiner IT-Systeme sowie Daten und/oder IT-Systeme des Auftraggebers ergreifen würde, einschließlich, aber nicht beschränkt auf die Unterbrechung der Verbindung und/oder die Sperrung des Zugangs. In keinem Fall haftet der Auftraggeber für die Folgen einer Verschlechterung der Beschaffenheit der Lieferungen und/oder Leistungen infolge der in diesem Fall getroffenen Maßnahmen.

Bei jedem Zugriff auf IT-Systeme des Auftraggebers muss der Auftragnehmer alle Sicherheitsmaßnahmen und Bedingungen einhalten (und sicherstellen, dass sein Personal diese einhält), die zur Erfüllung des Vertrages erforderlich sind, wie z. B. die geltenden Bedingungen für den Zugang zu den Räumen des Auftraggebers, jene für den Zugriff auf die IT-Systeme des Auftraggebers, über welche der Auftragnehmer schriftlich informiert wurde, sowie alle für die Ausführung des Vertrages spezifischen Sicherheitsbedingungen, auf die in den Vertragsbedingungen Bezug genommen wurde. Der Auftraggeber ermächtigt den Auftragnehmer nur dann zum Zugriff auf die IT-Systeme des Auftraggebers, wenn dies im Vertrag vereinbart ist und ausschließlich im erforderlichen Rahmen der Vertragserfüllung. Der Auftragnehmer darf nur Software verwenden, die er dem Auftraggeber gemeldet hat und die vom Auftraggeber freigegeben wurde. Der Auftragnehmer trifft alle notwendigen Vorkehrungen, um die Einschleusung eines Computervirus in die dem Auftraggeber übergebene Software, Updates und/oder neue Versionen zu vermeiden, und ergreift geeignete Maßnahmen, wenn er das Vorhandensein eines solchen Virus bemerkt.

4. Der Auftragnehmer verpflichtet sich, alle Vorkehrungen und Maßnahmen zu treffen, die von einem sorgfältigen Auftragnehmer zu erwarten sind, um sicherzustellen, dass er keinen Cybersicherheitsvorfall in Bezug auf seine Lieferungen und/oder Leistungen und/oder im Informationssystem des Auftraggebers, auf das der Auftragnehmer Zugriff hat, erzeugen oder verursachen wird, oder dies zu begünstigen.

Darüber hinaus muss der Auftragnehmer im Falle eines unerlaubten oder unbefugten Zugriffs und/oder Nutzung des in den Artikeln 3 und 4 genannten Informationssystems / IT-Systems des Auftraggebers und/oder bei Verdacht auf ein solches Ereignis und/oder im Falle eines sonstigen Cybersicherheitsvorfalls, das Framatome CERT (Computer Emergency Response Team – E-Mail: it.security@framatome.com – Telefon: (+33) 1 34 96 96 95) sowie den zuständigen kaufmännisch Verantwortlichen des Auftraggebers, dessen Kontaktdaten im Vertrag aufgeführt sind, benachrichtigen, sobald er davon Kenntnis erlangt, spätestens jedoch einen (1) Kalendertag nach einem (vermuteten) Cybersicherheitsvorfall.

Zusätzlich zum Framatome CERT muss der Auftragnehmer in den vorgenannten Fällen folgende Stelle alarmieren: dpit-ge-ciso@framatome.com

Jeder Meldung eines Cybersicherheitsvorfalls, muss beinhalten: -

den Beginn des Cybersicherheitsvorfalls,

- die Lieferungen und/oder Leistungen, welche betroffen sind, -

die Daten, welche betroffen sind,

- Indikatoren für die Manipulation (E-Mail, unautorisierte Nutzung des Netzwerks oder anderer Schwachstellen, Angriffsvektor) und
- jegliche weitere Information, welche den Auftraggeber helfen kann, den Cybersicherheitsvorfall zu untersuchen und zu beheben.

Bis der Cybersicherheitsvorfall behoben ist, muss der Auftragnehmer:

- Unverzüglich alle geeigneten und erforderlichen Maßnahmen ergreifen, einschließlich, aber nicht beschränkt auf:
  - ✓ Aktivierung von Eindämmungsmaßnahmen, um die Auswirkungen und den Umfang des Cybersicherheitsvorfalles zu minimieren;
  - ✓ Aktivierung von Maßnahmen zur Beseitigung der Bedrohung von Informationssystemen durch i) Löschen von schädlichen Codes, unerwünschten Konten oder Zugriffen, Behebung von Schwachstellen usw., welche die Quelle der Bedrohung sind, und/oder ii) Aktualisieren von Sicherheitslösungen oder Stärkung von IT-Systemen und Infrastruktur um die Verwendung von Vorgehensweisen, Techniken und Verfahren zu verhindern, die bei Cyberangriffen genutzt werden; und
- das CERT des Auftraggebers regelmäßig schriftlich über den Stand des Cybersicherheitsvorfalls und alle diesbezüglichen relevanten Informationen zu informieren.

Unbeschadet der vorstehenden Maßnahmen, welche vom Lieferanten gemäß dieser Bestimmung zu ergreifen sind, kann der Auftraggeber im Rahmen des Möglichen und auf angemessenes Ersuchen des Auftragnehmers Unterstützung leisten, um bei der Lösung des Cybersicherheitsvorfalls behilflich zu sein. Der Auftragnehmer muss ein Feedback zu jedem Cybersicherheitsvorfall erstellen und dokumentieren, um Informationen zu diesem Vorfall zu verfolgen und zu protokollieren.
Der Auftragnehmer muss das Feedback and das CERT übermitteln, sobald der Cybersicherheitsvorfall behoben ist. Im Falle eines Cybersicherheitsvorfalls, dessen Eintreten oder Übertragung der Auftragnehmer zu vertreten hat, haftet der Auftragnehmer für alle Schäden, Verluste oder sonstigen Folgen, die der Auftraggeber erleidet.