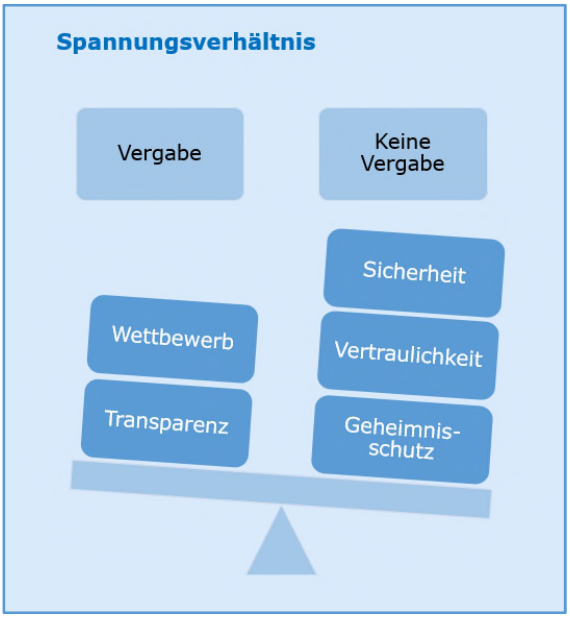
Beschaffung von Cyber-Security

29. Oktober 2020

Cyber-Security wird immer wichtiger. Spätestens seit den Attacken auf den deutschen Bundestag, das Auswärtige Amt und zahlreiche Persönlichkeiten des öffentlichen Lebens ist ein verstärktes Bewusstsein dafür entstanden, dass insbesondere die öffentliche Hand und Unternehmen die Integrität der vorhandenen informationstechnischen Systeme schützen müssen. Der folgende Beitrag verschafft einen Überblick darüber, welche Besonderheiten sich bei der Beschaffung von Waren und Dienstleistungen zur Cyber-Security selbst ergeben. Ein weiterer Beitrag erläutert, wie öffentliche Auftraggeber eine erhöhte Cyber-Integrität im Rahmen von Vergabeverfahren sicherstellen können.

Viele Unternehmen bieten bereits jetzt ein breites Spektrum an effektiven Waren und Dienstleistungen zur Erhöhung der Cyber-Security an. Es beginnt bei einfachen, standardisierten Software-Lösungen wie Firewalls oder Virenschutz, geht über besonders geschützte Server-Räume oder Beratungen zur Schaffung einer kohärenten Cyber-Sicherheitsarchitektur hin zu eigens programmierten Programmen der Sicherheitsbehörden, um zu Ermittlungszwecken in Rechensysteme Dritter einzudringen.

Bei der Beschaffung von Waren und Dienstleistungen zur Cyber-Security besteht eine große Spannung zwischen dem vergaberechtlichen Gebot eines diskriminierungsfreien und transparenten Wettbewerbs und dem Interesse öffentlicher Auftraggeber, maßgeschneiderte Lösungen zu erhalten. Auch Fragen der Sicherheit und Vertraulichkeit spielen selbstredend eine große Rolle. Diese Komplexität wird noch weiter durch das industriepolitische Interesse verstärkt, eine deutsche und europäische Expertise auf den betreffenden Gebieten aufzubauen oder fortzuentwickeln. Wie diese Spannungsverhältnisse im Einzelfall aufgelöst werden können, bestimmt sich maßgeblich nach der zur Verfügung stehenden Verfahrensart:



- Das **Verhandlungsverfahren ohne vorgeschalteten Teilnahmewettbewerb** eignet sich insbesondere bei der Beschaffung eines schon im Zeitpunkt der Vergabeentscheidung feststehenden Produkts eines bestimmten Unternehmens. Dieses Verfahren ist jedoch nur unter engen Voraussetzungen möglich (vgl. § 14 Abs. 4 VgV, § 13 Abs. 2 SektVO; § 12 VSVgV). Das ist im Kontext der Cyber-Security beispielsweise dann der Fall, wenn nur ein auf dem Markt befindliches Produkt den erforderlichen Mindeststandard an IT-Sicherheit gewährleistet. Das Gleiche gilt, wenn die Migration sensibler Daten auf ein neues System oder die Inkompatibilität verschiedener vom Hoheitsträger genutzter Systeme zu schwerwiegenden Sicherheitslücken führen würden. Auch ist denkbar, dass der öffentliche Auftraggeber im Rahmen des Beschaffungsvorhabens zwingend auf bestimmte Ausschließlichkeitsrechte zurückgreifen muss, die bei nur einem Unternehmen liegen. Dies ist etwa dann geboten, wenn der öffentliche Auftraggeber Updates, Softwarepflegeleistungen oder zusätzliche Lizenzen für bestimmte IT-Sicherheitsprodukte benötigt, die von ihm bereits genutzt werden.

- Stehen weder der konkrete Beschaffungsgegenstand noch der Auftragnehmer im Vorfeld der Ausschreibung fest, ist bei komplexeren Vorhaben regelmäßig das **Verhandlungsverfahren mit Teilnahmewettbewerb** vorzugswürdig. Unternehmen können ihre Lösung für die vom öffentlichen Auftraggeber vorgegebenen Anforderungen präsentieren und mit ihm verhandeln. Aus den ihm angebotenen Leistungen kann der Auftraggeber dann die beste Lösung auswählen. Dadurch besteht für den Auftraggeber die Möglichkeit, den Vertragsgegenstand zu modifizieren und konkretisieren, um innovative Lösungen auf dem neuesten Stand der Technik einzukaufen. In der Vergangenheit wurde dieses Verfahren beispielsweise verwendet zur Beschaffung umfangreicher Schwachstellen-analysen der IT-Infrastruktur, bei groß angelegten Projekten zur Mitarbeitersensibilisierung für den Bereich Cyber-Security oder zur Erstellung von Krisenkonzepten für Fälle erfolgreicher Cyber-Attacken.

- Um in Deutschland oder Europa noch nicht auf dem Markt verfügbare Technologien auf- oder auszubauen, bietet sich die – für Beschaffungen mit Verteidigungs- oder Sicherheitsrelevanz allerdings nicht explizit vorgesehene – **Innovationspartnerschaft** an. Obwohl ihr in der Praxis noch keine allzu große Bedeutung zukommt, eröffnet sie die Möglichkeit, gemeinsam mit einem oder mehreren vom öffentlichen Auftraggeber zu bestimmenden Unternehmen neue Produkte oder Dienstleistungen zu entwickeln. Derartige Verfahren könnten dazu beitragen, die Abhängigkeit von außereuropäischen Produkten und Systemen im Bereich der Informationssicherheit zu verringern, und so zu einer Stärkung des deutschen und europäischen Standortes auf dem Gebiet der Cyber-Sicherheit führen. Solche Innovationspartnerschaften bieten sich damit insbesondere bei Großprojekten im Bereich der Informationstechnologie an, wie etwa der Entwicklung komplexer Spähsoftware oder entsprechender Abwehrsysteme.

- Ausschreibungen von standardisierten Waren und Dienstleistungen ohne Sicherheitsrelevanz können im **offenen Verfahren** durchgeführt werden. Dieses Verfahren eignet sich etwa für die Ausschreibung einfacher Mitarbeiterschulungen zur IT-Sicherheit oder regelmäßiger allgemeiner Analysen zur aktuellen Bedrohungslage in diesem Bereich („Threat Assessments"). Auch für die Beschaffung von Standard-Software oder -Hardware (Bildschirme, Desktop-PCs) ist das offene Verfahren geeignet.

- In den eng eingegrenzten Fällen des **Art. 346 AEUV** kann von einer Ausschreibung unter Umständen sogar gänzlich abgesehen werden. Dafür müssten „wesentliche Sicherheitsinteressen" der Bundesrepublik betroffen sein. Seit Inkrafttreten des § 107 Abs. 2 S. 2 GWB im April 2020 ist dies insbesondere auch dann der Fall, wenn der öffentliche Auftrag verteidigungs- oder sicherheitsindustrielle Schlüsseltechnologien betrifft. Zu diesen Schlüsseltechnologien gehören u.a. auch sicherheitsrelevante IT- und Kommunikationsanlagen, wie Cyber-Abwehrsysteme, sowie Lösungen unter Einsatz Künstlicher Intelligenz (KI).

Wie das Spannungsverhältnis zwischen Wettbewerb und Sicherheitsbedenken in der Praxis bestmöglich austariert werden kann und welche Verfahrensarten sich bei der Beschaffung von Waren und Dienstleistungen im Bereich Cyber-Security künftig durchsetzen werden, wird sich in den kommenden Jahren zeigen.

BLOMSTEIN wird diese Entwicklungen beobachten und darüber informieren. Wenn Sie Fragen zu den potenziellen Auswirkungen der Cyber-Security auf Ihr Unternehmen oder Ihre Branche haben, stehen Ihnen Dr. Roland M. Stein und Dr. Christopher Wolters jederzeit gern zur Verfügung.