Cyber-Security im Vergabeverfahren

12. April 2019

Cyber-Security wird immer wichtiger. Spätestens seit den Attacken auf den deutschen Bundestag, das Auswärtige Amt und auf zahlreiche Persönlichkeiten des öffentlichen Lebens ist klar, dass die Integrität der eigenen informationstechnischen Systeme geschützt werden muss. Der folgende Beitrag verschafft einen Überblick darüber, wie öffentliche Auftraggeber eine erhöhte Cyber-Integrität von Waren und Dienstleistungen im Rahmen von Vergabeverfahren sicherstellen können. Ein weiterer Beitrag erläutert, welche Besonderheiten sich bei der Beschaffung von Waren und Dienstleistungen zur Cyber-Security selbst ergeben.

Bereits durch die Gestaltung des Vergabeverfahrens können öffentliche Auftraggeber dazu beitragen, dass die von ihnen ausgeschriebene Ware oder Dienstleistung über einen verstärkten Schutz vor Cyber-Angriffen verfügt. Das ist auf verschiedenen Wegen möglich. Die Cyber-Integrität des zukünftigen Vertragspartners lässt sich im Rahmen der Eignungsprüfung durch entsprechende Anforderungen (hierzu unter 1) und den Ausschluss von Bietern (hierzu unter 2) sicherstellen. Die Cyber-Integrität des Beschaffungsgegenstands wiederum lässt sich durch entsprechende Vorgaben in der Leistungsbeschreibung bzw. des Vertrags sowie in den Zuschlagskriterien berücksichtigen (hierzu unter 3). Die Integrität des Vergabeverfahrens selbst kann mittels entsprechender Regeln in den Verfahrensbedingungen verstärkt werden (hierzu unter 4).

1. Cyber-Integrität des Vertragspartners

Die Eignungsprüfung bietet die Möglichkeit, Anforderungen an die Person des Auftragnehmers zu stellen und somit auch, dessen „Cyber-Integrität“ sicherzustellen. So können von den Bietern besondere Erfahrungen und Referenzen im Bereich der IT-Sicherheit und des Datenschutzes verlangt werden. Ebenso vorausgesetzt werden kann ausreichend qualifiziertes und geschultes Personal sowie eine moderne Ausstattung auf dem Gebiet der IT-Infrastruktur. All diese Faktoren stellen bei Aufträgen, welche die Verarbeitung von schützenswerten Informationen umfassen, einen Teil des Eignungskriteriums der technischen und beruflichen Leistungsfähigkeit gem. § 122 Abs. 2 S. 2 GWB dar und können somit vom Auftraggeber als Mindestanforderung oder zu bewertendes Eignungskriterium festgelegt werden.

Doch auch in weniger komplexen Beschaffungsvorhaben können sich öffentliche Auftraggeber eine erhöhte Sicherheit hinsichtlich der Cyber-Integrität des potenziellen Vertragspartners verschaffen und gleichzeitig einen hohen Prüfaufwand vermeiden. So können sie im Rahmen der Eignungsprüfung auch generelle Nachweise zur Cyber-

Sicherheit der teilnehmenden Unternehmen anfordern, etwa in Form bereits ausgearbeiteter Sicherheitskonzepte oder anerkannter Zertifizierungen auf Grundlage der Standards des Bundesamts für Informationssicherheit (BSI). Ebenfalls denkbar – aber mit einem höheren Aufwand verbunden – ist die Aufstellung eines eigenen Präqualifikationssystems im Bereich der Cyber-Sicherheit nach US-amerikanischem Vorbild (vgl. beispielsweise: https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance). Ein solches könnte helfen, die fallspezifische Eignungsprüfung effizienter und kostengünstiger zu gestalten, ohne auf hohe Standards der Cyber-Integrität verzichten zu müssen.

2. Ausschluss von Bietern

Im Zuge der Eignungsprüfung vom Vergabeverfahren ausschließen kann der Auftraggeber unter Umständen jene Bieter, in deren Unternehmen es bereits in der Vergangenheit zu Datenlecks und Sicherheitslücken gekommen ist oder die anderweitig gegen rechtliche oder vertragliche Pflichten im Kontext der Informationssicherheit verstoßen haben. Ausreichend ist in diesem Zusammenhang bereits, dass der Bieter grob fahrlässig handelte und das Fehlverhalten nicht nur unerhebliche Auswirkungen zur Folge hatte. Eine solche Pflichtverletzung wird zumeist als „schwere Verfehlung“ im Sinne des § 124 Abs. 1 Nr. 3 GWB zu werten sein und damit einen Ausschluss vom laufenden Verfahren rechtfertigen.

Erfolgten die angesprochenen Verstöße gegen Cyber-Security-Verpflichtungen im Kontext eines früheren Auftragsverhältnisses, so kommt zusätzlich der Ausschlussgrund gem. § 124 Abs. 1 Nr. 7 GWB in Betracht. Hiernach kann ein Bieter ausgeschlossen werden, der eine wesentliche Anforderung eines öffentlichen Auftrags in der Vergangenheit erwiesenermaßen dauerhaft oder in erheblichem Maße mangelhaft ausgeführt hat.

In der Praxis lassen es öffentliche Auftraggeber zum Nachweis, dass keine Ausschlussgründe vorliegen, häufig genügen, wenn Bieter eine entsprechende Eigenerklärung abgeben. Besteht bei einem Beschaffungsvorgang indes eine besondere Sicherheitsrelevanz, sollte ein solches Vorgehen überdacht werden. Der öffentliche Auftraggeber kann bei einzelnen Bietern überdies Nachfragen stellen oder diese zu einer gesonderten Erläuterung auffordern, wenn begründete Zweifel an der Richtigkeit der Eigenerklärung bestehen. Dieses Vorgehen sollte insbesondere bei Bietern in Betracht gezogen werden, bei denen Meldungen aus der Presse oder andere Anhaltspunkte darauf hindeuten, dass sie im Bereich Cyber-Integrität durch Verstöße und Fehlverhalten aufgefallen sind.

3. Cyber-Integrität des Beschaffungsgegenstands

Öffentliche Auftraggeber können in verschiedener Hinsicht versuchen, die Cyber-Integrität des Beschaffungsgegenstandes sicherzustellen. Relevante Instrumentarien

sind insbesondere eine durchdachte Leistungsbeschreibung, auftragsspezifische Zuschlagskriterien und entsprechende vertragliche Regelungen.

Die Leistungsbeschreibung dient dazu, den Beschaffungsgegenstand festzulegen. Dementsprechend können öffentliche Auftraggeber die Möglichkeit nutzen, dem Auftragnehmer Vorgaben an den Beschaffungsgegenstand mit dem Ziel des Schutzes sensibler Informationen im Bereich der Cyber-Security zu machen. Die nachgefragte Beschaffungsleistung muss gem. § 121 Abs. 1 S. 1 GWB so eindeutig und erschöpfend wie möglich beschrieben werden. Regelmäßig kommt dabei eine funktionale Leistungsbeschreibung in Betracht, in der die technischen Anforderungen aufgeführt werden, die das Produkt oder die Dienstleistung im Mindestmaß zu erfüllen hat. Im Rahmen der Leistungsbeschreibung kann in begründeten Fällen vom Bieter verlangt werden, dass er bestimmte, potentiell gesondert zertifizierte, Komponenten in das Produkt integriert. Alternativ kann der öffentliche Auftraggeber auch spezielle Abläufe für die Leistungserbringung vorgeben.

Öffentliche Auftraggeber können überdies gem. § 127 Abs. 1 S. 3 GWB neben dem Preis auch qualitative Aspekte als Zuschlagskriterien berücksichtigen, wenn sie mit dem Auftragsgegenstand in Verbindung stehen. So darf ein öffentlicher Auftraggeber von den Bietern beispielsweise ein Konzept zur Cyber-Sicherheit verlangen. Ein solches muss aber nicht nur in die Angebotsbewertung einfließen. Es könnte zudem auch zum Vertragsgegenstand erklärt werden und so die zu erbringende Leistung konkretisieren.

Der Auftraggeber kann in den Vergabeunterlagen gem. § 128 Abs. 2 S. 1 GWB schließlich auch Bedingungen für die Ausführung des Auftrags festlegen, sofern diese mit dem Auftragsgegenstand in Verbindung stehen. Solche Ausführungsbedingungen, etwa in Form verpflichtender regelmäßiger „Stresstests“ der unternehmenseigenen IT-Infrastruktur, sind ausdrücklich auch zum Schutz der Vertraulichkeit von Informationen zulässig. Ebenso ist es beispielsweise möglich, vertraglich die Stationierung der verwendeten Server in Europa oder sogar in Deutschland zu verlangen.

4. Cyber-Integrität des Vergabeverfahrens

Letztlich stehen dem Auftraggeber verschiedene Instrumentarien zur Verfügung, um die Cyber-Integrität des Vergabeverfahrens selbst sicherzustellen. Hierzu gehört nicht nur die generelle gesetzliche Verpflichtung der Parteien des Verfahrens zur Vertraulichkeit. Öffentliche Auftraggeber können darüberhinausgehende Maßnahmen ergreifen, um die Sicherheit der Datenflüsse und -aufbewahrung während des Verfahrens sicherzustellen. Besondere Vorsicht ist dabei im Kontext der Kommunikation von Bieterfragen und den darauffolgenden Antworten der öffentlichen Auftraggeber geboten. Die Wahrung der Informationssicherheit ist hierbei insbesondere deshalb erforderlich, weil die Antworten der öffentlichen Auftraggeber nach dem Gleichbehandlungsgrundsatz allen Bietern zur Verfügung zu stellen sind.

Die Kommunikation zwischen den Parteien bei Vergabeverfahren ohne besondere Relevanz für die Verteidigung oder Sicherheit erfolgt während des gesamten Verfahrens grundsätzlich auf elektronischem Wege. Neben der zwingend verschlüsselten Angebotsabgabe kann der öffentliche Auftraggeber das Sicherheitsniveau für die elektronische Kommunikation selbst festlegen, beziehungsweise fortgeschrittene oder qualifizierte elektronische Signaturen oder Siegel für die Kommunikation voraussetzen. Wenn schutzwürdige Daten betroffen sind, die bei Verwendung allgemein verfügbarer oder alternativer elektronischer Mittel nicht angemessen geschützt werden können, kann der öffentliche Auftraggeber zudem eine schriftliche Angebotsabgabe verlangen.

Zusätzlich zu den oben genannten Möglichkeiten sind vom Auftraggeber im Rahmen von Ausschreibungen mit Sicherheits- oder Verteidigungsrelevanz, insbesondere im Zusammenhang mit Verschlusssachen, noch weitergehende Maßnahmen zu ergreifen, um die Daten- und Informationssicherheit zu gewährleisten. So ist von den Bietern in Fällen, in denen bereits der Teilnahmeantrag den Zugang zu Verschlusssachen der Stufe „VS-Vertraulich“ oder höher erfordert, bereits vor Gewährung dieses Zugangs ein Sicherheitsbescheid des BMWi einzuholen. Im Falle von im Ausland ansässigen Bietern kann das Ministerium zusätzlich die jeweilige nationale Sicherheitsbehörde ersuchen, Auskünfte über die Sicherheit der genutzten Räumlichkeiten oder des eingesetzten Personals zu übermitteln. Im Austausch mit dem Bieter steht dem Auftraggeber die Wahl des nach einschlägigen Sicherheitserwägungen angemessenen Kommunikationsmittels von vornherein ebenso offen wie die Entscheidung, die Vergabeunterlagen aus Vertraulichkeits- und Datenschutzgründen nur zur Einsicht zur Verfügung zu stellen.

5. Fazit

Den öffentlichen Auftraggebern stehen im Ergebnis zahlreiche Möglichkeiten zur Verfügung, im Vergabeverfahren auf die gewachsene Relevanz der Cyber-Integrität zu reagieren und diese sicherzustellen. Die Vergabestelle kann die informationstechnische Sicherheit des Vergabeprozesses und der daraus resultierenden Beschaffungsleistung dabei durch spezifische Anforderungen an den Vertragspartner, den Beschaffungsgegenstand und die Verfahrensbedingungen garantieren.

BLOMSTEIN wird die weiteren 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