See the notice on TED website

Deutschland-Berlin: Softwarepaket und Informationssysteme
OJ S 201/2023 18/10/2023
Vorinformation
Lieferungen

Rechtsgrundlage:
Richtlinie 2014/24/EU

Abschnitt I: Öffentlicher Auftraggeber

I.1. Name und Adressen

Offizielle Bezeichnung: Johanniter HealthCare-IT Solutions GmbH
Postanschrift: Finckensteinallee 123
Ort: Berlin
NUTS-Code: DE300 Berlin
Postleitzahl: 12205
Land: Deutschland
Kontaktstelle(n): PwC Legal AG
E-Mail: ilya.levin@pwc.com
Internet-Adresse(n):
Hauptadresse: https://www.johanniter.de/johs/

I.3. Kommunikation

Weitere Auskünfte erteilen/erteilt die oben genannten Kontaktstellen

I.4. Art des öffentlichen Auftraggebers

Andere: Juristische Person des privaten Rechts

I.5. Haupttätigkeit(en)

Gesundheit

Abschnitt II: Gegenstand

II.1. Umfang der Beschaffung

II.1.1. Bezeichnung des Auftrags

IT-Security_Markterkundung
Referenznummer der Bekanntmachung: 2/2023

II.1.2. CPV-Code Hauptteil

48000000 Softwarepaket und Informationssysteme

II.1.3. Art des Auftrags

Lieferauftrag

II.1.4. Kurze Beschreibung

Sehr geehrte Damen und Herren,
die Johanniter HealthCare-IT Solutions GmbH beabsichtigt, Software zur Verbesserung der IT-Sicherheit zu beschaffen ("Beschaffungsvorhaben").
Zur Vorbereitung des Verfahrens führt der Auftraggeber die vorliegende Markterkundung durch.

Der Auftraggeber ist einer der führenden HealthCare-IT-Spezialisten im deutschen Gesundheitswesen und selbstständige Dienstleistungsgesellschaft der Johanniter. Seit über 20 Jahren berät und unterstützt sie konfessionelle Träger sowie Dienstleistungsunternehmen unter ebenfalls konfessioneller Trägerschaft.
Zur Vorbereitung des Verfahrens führt der Auftraggeber die vorliegende Markterkundung durch.
1. Verfahrensablauf:
a. Art der Teilnahme
Sie können durch Beantwortung des Fragenkatalogs, vgl. Ziff. VI.3) an der Markterkundung teilnehmen.
Soweit erforderlich behält sich der Auftraggeber vor, ein Vertiefungsgespräch durchzuführen.
b. Teilnahmefrist
Für die Teilnahme (Elektronische Übersendung des beantworteten Fragenkatalogs und/oder Vereinbarung eines Markterkundungsgesprächs) gilt die folgende Frist: 3. November 2023.
2. Ausfüllbarer Word-Fragenkatalog
Den unter Ziff. VI.3) aufgelisteten Fragenkatalog (ebenso wie die Beschreibung des Vorhabens) stellen wir Ihnen sehr gerne als ausfüllbare Word-Version zur Verfügung. Hierfür bitten wir Sie, formlos eine Anfrage unter der folgenden E-Mail-Adresse zu stellen:
ilya.levin@pwc.com
Wir danken Ihnen für Ihre Teilnahme und verbleiben mit freundlichen Grüßen

II.1.5. Geschätzter Gesamtwert

II.1.6. Angaben zu den Losen

Aufteilung des Auftrags in Lose: nein

II.2. Beschreibung

II.2.3. Erfüllungsort

NUTS-Code: DE300 Berlin

II.2.4. Beschreibung der Beschaffung

I. I. Ausgangslage und technische Rahmenbedingungen
Die Johanniter GmbH ("Johanniter") koordiniert seit 2004 als Trägergesellschaft des stationären Johanniter-Verbundes deutschlandweit 125 Gesundheits- und Pflegeeinrichtungen. Der Verbund umfasst neun Krankenhäuser, neun Fach- und Rehabilitationskliniken, sieben Medizinische Versorgungs- und Therapiezentren, 94 Seniorenhäuser, drei Hospize, drei Pflegeschulen sowie drei zentrale Dienstleistungsgesellschaften. In den Einrichtungen sind rund 17.000 Mitarbeitende, davon über 7.300 Pflegekräfte beschäftigt.
Der Auftraggeber ist einer der führenden HealthCare-IT-Spezialisten im deutschen Gesundheitswesen und selbstständige Dienstleistungsgesellschaft der Johanniter. Seit über 20 Jahren berät und unterstützt sie konfessionelle Träger sowie Dienstleistungsunternehmen unter ebenfalls konfessioneller Trägerschaft.
Die IT-Landschaft der Auftraggeberin wurde 2008 in zwei redundant ausgelegten Rechenzentren in der Finckensteinallee 123 in Berlin zentralisiert.
Die Rechenzentren sind folgendermaßen ausgelegt:
- Kältegänge zur optimalen Kühlung der Serversysteme
- Wasserdichte verkofferte Rohre und Flutungsraum im doppelten Boden
- Zwei redundante Klimaanlagen (Wechselbetrieb).
- Die Unterlagen befinden sich in einem separaten Ordner in der Produktion.

Zwei redundante USV (zwei Stromkreise) und ein Notstromgenerator (Diesel) im Außenbereich. Die Wartung der USV findet jährlich statt. Der Notstromgenerator wird einem monatlichen Simulationstest, sowie einem jährlichen "Black Building Test" unterzogen.
Innerhalb der IT-Landschaft betreiben die Johanniter im Rechenzentrum und zum kleinen Teil an den Standorten ca. 1500 Serversysteme. Mit diesen Systemen werden ca. 7500 Benutzer und 6500 Clients bedient. Über ein zentrales Mobile Device Management System werden zusätzlich ca. 1000 mobile Endgeräte verwaltet. Außerdem werden ca. 4000 Druckgeräte zentral verwaltet. Das Storage-System hat ein genutztes Gesamtvolumen von ca. 300TB und das Backupvolumen beträgt derzeit ca. 1,2 PB.
Primäre Zielsetzung des Beschaffungsvorhabens ist, dass der Auftraggeber in die Lage versetzt wird, die Aktivitäten aller Benutzerkonten, auch die der Administratoren, in eigener Infrastruktur zu überwachen und aufzeichnen zu können. Perspektivisch sollen auch Microsoft 365, Azure Active Directory, SharePoint Online und Exchange Online überwacht werden können.
Dabei soll die Lösung vollständig unabhängig sein von externen Diensten, wie z. B. Clouds, oder anderen extern gehosteten Diensten. Sie soll nur auf lokalen Servern im zentralen Rechenzentrum installiert werden und muss auch verteilte, über WAN verbundene Standorte überwachen können.

II.2.14. Zusätzliche Angaben

Im Bereich des Datenschutzes strebt der Auftraggeber eine Lösung an, die ihn in die Lage versetzt, sehr schnell Auskunft über die ggf. kriminellen Aktivitäten und Datenmissbrauch zu erlangen.
Darüber hinaus soll die zu beschaffende Lösung über eine Alarmierungsfunktion verfügen. Der Auftraggeber möchte, dass die zu beschaffende Lösung den Auftraggeber über bestimmte Aktivitäten alarmiert. Dazu gehören z. B.:
- Änderungen an Benutzergruppen, über die administrative Zugriffsberechtigungen erteilt werden,
- ungewöhnliche Benutzerzugriffe (gemäß den bis dahin aufgezeichneten Aktivitäten), wie z. B.
- potentielle Ransomware-Aktionen
- Löschen und/ oder Kopieren vieler Dateien in kürzester Zeit
- Zugriffe auf Dateien, auf die nie zuvor zugegriffen wurde
- Potentielle Sicherheitsrisiken, wie z. B.
- Benutzerkonten ohne Passwort oder mit abgelaufenem Passwort
- ungenutzte aber aktive Benutzerkonten
- Überwachung der Dienstkonten für Kerberos
- leere Benutzergruppen, über die Zugriffsberechtigungen erteilt sind

Die Aufzeichnungen müssen für mind. 1 Jahr im schnellen Zugriff verfügbar sein. Darüber hinaus sollen die Aufzeichnungen für mind. 5 Jahre verfügbar sein, ohne dass diese erst wieder importiert oder "aktiviert" werden müssen.
Der Zugriff auf die Aufzeichnungen muss eingeschränkt werden können, sodass bestimmte Personen nur bestimmte Aufzeichnungen einsehen und auswerten können.
Der Zugriff auf die Aufzeichnungen und Alarme soll über eine einheitliche GUI erfolgen. Die Aufzeichnungen sollen auch Aussagen über die Datennutzung ermöglichen, z. B.
- Wer ist technischer Besitzer?
- Wer ist "de facto" Besitzer (arbeitet am meisten oder fast ausschließlich damit)?
- Wer greift auf welche Daten zu? (über einen bestimmten Zeitraum)

Es sollen Alarme zu allen aufgezeichneten Aktivitäten erzeugt werden können. Die Lösung sollte möglichst Vorlagen für gängige Standardalarme mitliefern sowie die Erstellung und Speicherung eigener Alarme ermöglichen. Alarme sollen zeitnah und automatisch erzeugt,

gespeichert, in einer GUI übersichtlich dargestellt und an zu alarmierende Empfänger versendet werden können. Außerdem sollen Reporte über alle aufgezeichneten Aktivitäten und die resultierenden Alarme erstellt werden können. Die Lösung sollte möglichst Vorlagen für gängige Standardreporte mitliefern sowie die Erstellung und Speicherung eigener Reporte ermöglichen. Reporte sollen zeitgesteuert automatisch erstellt und abgelegt und/ oder versendet werden können.
Der Zugriff auf die einzelnen Funktionen der GUI muss eingeschränkt werden können, sodass bestimmte Personen nur bestimmte Aufgaben in der GUI tätigen können. Die dafür erforderlichen Berechtigungen sollen an Active-Directory-Gruppen erteilt werden.
Die Abfrage und Aufzeichnung der Ereignisse von den Datenquellen soll weitestgehend ohne auf den Datenquellen zu installierende Agenten erfolgen. Zusätzlich muss die Lösung skalierbar sein, ohne dass es dabei zu Einbußen bei der Performance kommt, und das für einen Zeitraum von mind. 5 Jahren.
Der Anbieter sollte mit der Lösung einhergehen Support liefern, der bei (potenziellen) Cyber-Angriffen ohne zusätzliche Kosten zeitnah involviert werden und helfen kann.

II.3. Voraussichtlicher Tag der Veröffentlichung der Auftragsbekanntmachung
01/12/2023

Abschnitt IV: Verfahren

IV.1. Beschreibung

IV.1.8. Angaben zum Beschaffungsübereinkommen (GPA)
Der Auftrag fällt unter das Beschaffungsübereinkommen: ja

Abschnitt VI: Weitere Angaben

VI.3. Zusätzliche Angaben
I. Fragenkatalog
Der vollständige Fragenkatalog kann von der unter Ziffer II.1.4) 2. benannten Stelle als ausfüllbare Word-Version angefordert werden. Nachfolgend erfolgt lediglich eine allgemeine Darstellung der zu erläuternden Fragen. Die Teilnehmer werden gebeten, den ausgefüllten Fragenkatalog beim Auftraggeber einzureichen.
1) Unternehmensbezogene Informationen
2) Technische Informationen
a) Allgemeine Fragen im Hinblick auf die von Ihnen angebotene Lösung
b) Fragen zum Berechtigungsmanagement in Zusammenhang mit Datenklassifizierung
c) Fragen im Zusammenhang mit Ermittlung Datenbesitzer und Umsetzung
d) Fragen zu Reports
e) Fragen zur Alarmierung
f) Fragen zur webbasierten grafischen Oberfläche
g) Fragen zur Fileservice Sicherheit
h) Fragen zur Exchange Sicherheit
i) Fragen zur Active Directory Sicherheit
j) Fragen zu den Logs
II. Hinweise:
Bei dieser Markterkundung handelt es sich nicht um ein förmliches Vergabeverfahren nach den §§ 97 ff. GWB. Mit dieser Markterkundung ist keine Verpflichtung des Auftraggebers verbunden, ein förmliches Vergabeverfahren einzuleiten, die Teilnehmer der Markterkundung

zur Angebotsabgabe aufzufordern oder ihnen einen Zuschlag zu erteilen. Zudem ist diese Markterkundung keine Voraussetzung für eine
Angebotsabgabe und weder eine Aufforderung zur Interessenbekundung noch eine Aufforderung zur Abgabe eines Teilnahmeantrags oder zur Einreichung eines Angebots. Darüber hinaus erwartet der Auftraggeber keine verbindlichen Angebote und wird keine unaufgeforderten Vorschläge annehmen. Des Weiteren erfolgt keine Rückmeldung bzw. Kommunikation der Ergebnisse der Markterkundung an die teilnehmenden Unternehmen. Kosten oder Aufwendungen, die im Zusammenhang mit der Teilnahme an dieser Markterkundung entstehen, werden vom Auftraggeber nicht erstattet.
Sofern der Auftraggeber im Anschluss an die Markterkundung den Auftrag in einem öffentlichen Verfahren vergibt, wird eine Auftragsbekanntmachung im Amtsblatt der Europäischen Union veröffentlicht.
Bekanntmachungs-ID: CXP4Y8L6T66

VI.5. Tag der Absendung dieser Bekanntmachung

13/10/2023