See the notice on TED website

Deutschland-Uelzen: Antivirensoftwarepaket
OJ S 45/2023 03/03/2023
Freiwillige Ex-ante-Transparenzbekanntmachung
Lieferungen

Rechtsgrundlage:
Richtlinie 2014/24/EU

Abschnitt I: Öffentlicher Auftraggeber/Auftraggeber

I.1. Name und Adressen

Offizielle Bezeichnung: IT-Verbund Uelzen
Ort: Uelzen
NUTS-Code: DE93A Uelzen
Land: Deutschland
Kontaktstelle(n): IT-Verbund Uelzen
E-Mail: sandra.betker@it-verbund-uelzen.de
Internet-Adresse(n):
Hauptadresse: https://www.it-verbund-uelzen.de/bekanntmachungen/

I.4. Art des öffentlichen Auftraggebers

Einrichtung des öffentlichen Rechts

I.5. Haupttätigkeit(en)

Andere Tätigkeit: Informationstechnologie

Abschnitt II: Gegenstand

II.1. Umfang der Beschaffung

II.1.1. Bezeichnung des Auftrags

Erweiterung Antiviren Lizenzen und Managed Service mit KI basierter Netzwerküberwachung

II.1.2. CPV-Code Hauptteil

48761000 Antivirensoftwarepaket

II.1.3. Art des Auftrags

Lieferauftrag

II.1.4. Kurze Beschreibung

Aufgrund der wachsenden globalen Bedrohungslage plant der IT Verbund Uelzen die Erweiterung der bestehenden Antiviren Lizenzen auf ein Managed Detection and Response System (MDR) und die Anschaffung einer Netzwerküberwachung auf KI Basis. Diese zusätzliche Absicherung soll ungewöhnliche Aktivitäten (zB. Crypto Trojaner) erfassen und im Bedrohungsfall über ein externes Security Operating Center (SOC) selbstständig oder nach Rücksprache mit dem IT-Verbund Uelzen Aktionen setzen. Wichtigster Faktor für den Wechsel auf ein MDR System ist die 24/7/365 Verfügbarkeit eines externen Security Operating Centers. Durch die neue Lizensierung auf MDR Basis erfolgt die Überwachung eventueller Attacken nicht nur lokal im Administratoren Bereich des IT-Verbundes Uelzen, sondern auch im SOC des Anbieters.

II.1.6. Angaben zu den Losen

Aufteilung des Auftrags in Lose: nein

II.1.7. Gesamtwert der Beschaffung

Wert ohne MwSt.: 610 172,00 EUR

II.2. Beschreibung

II.2.3. Erfüllungsort

NUTS-Code: DE93A Uelzen

II.2.4. Beschreibung der Beschaffung

Aufgrund der wachsenden globalen Bedrohungslage plant der IT Verbund Uelzen die Erweiterung der bestehenden Antiviren Lizenzen auf ein Managed Detection and Response System (MDR) und die Anschaffung einer Netzwerküberwachung auf KI Basis. Diese zusätzliche Absicherung soll ungewöhnliche Aktivitäten (zB. Crypto Trojaner) erfassen und im Bedrohungsfall über ein externes Security Operating Center (SOC) selbstständig oder nach Rücksprache mit dem IT-Verbund Uelzen Aktionen setzen. Wichtigster Faktor für den Wechsel auf ein MDR System ist die 24/7/365 Verfügbarkeit eines externen Security Operating Centers. Durch die neue Lizensierung auf MDR Basis erfolgt die Überwachung eventueller Attacken nicht nur lokal im Administratoren Bereich des IT-Verbundes Uelzen, sondern auch im SOC des Anbieters.

II.2.5. Zuschlagskriterien

Preis

II.2.11. Angaben zu Optionen

Optionen: nein

II.2.13. Angaben zu Mitteln der Europäischen Union

Der Auftrag steht in Verbindung mit einem Vorhaben und/oder Programm, das aus Mitteln der EU finanziert wird: nein

II.2.14. Zusätzliche Angaben

Abschnitt IV: Verfahren

IV.1. Beschreibung

IV.1.1. Verfahrensart

Verhandlungsverfahren ohne vorherige Bekanntmachung

Erläuterung:

Im Kontext der Ukraine Krise hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 15.03.2022 eine ausdrückliche Warnung vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky ausgesprochen. Das BSI hat dringend empfohlen, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen. Aufgrund dessen, sah sich der IT-Verbund Uelzen gezwungen, kurzfristig die bisherigen Produkte aus Sicherheitsgründen durch andere Produkte zu ersetzen. Es stand zu befürchten, dass diese Produkte als Eintrittstor genutzt werden. Im Bereich der Mobilen Endgeräte wurde nur ein Teil der Geräte mit der zentral verwalteten Lösung von Sophos zu Testzwecken ausgestattet.

Durch die während der Corona Pandemie massiv vergrößerten Möglichkeiten zum Homeoffice hat sich der Bedrohungsvektor zusätzlich verstärkt. Die massiv gestiegene Anzahl an

Cyberattacken im Kontext der Ukraine Krise hat das Bedrohungspotenzial multipliziert. Die abgefangenen Cyber-Angriffe auf das System des IT-Verbundes Uelzen haben sich von Januar 2022 bis Januar 2023 mehr als verzehnfacht. Mit diesem Anstieg konnte nicht in dem Maße gerechnet werden. Diese Entwicklung, ließ die Einhaltung der Mindestfristen z. B. bei Vergabeverfahren mit Teilnahmewettbewerb, nicht zu. Die Anschaffung der getesteten Produkte für den gesamten Bereich war unverzüglich vorzunehmen.
Ein Teilnahmewettbewerb war zudem nicht möglich, da es sich um sicherheitsspezifische Fragestellungen handelt, die einer besonderen Vertraulichkeit unterliegen. Im Rahmen dieser Ausschreibung mussten sehr sensible Informationen über die aktuell eingesetzten Sicherheitsprodukte, deren Versionen und die Anzahl bekannt gegeben werden. Die zur Angebotslegung benötigten sensiblen Informationen hätten bei einer Veröffentlichung eventuelle Cyberattacken begünstigt und das Sicherheitsrisiko für den IT-Verbund Uelzen massiv erhöht. Es wurde so vermieden, dass Informationen zur Sicherheitstechnik des IT-Verbundes Uelzen veröffentlicht werden.
Aus den genannten Gründen wurde die Ausschreibung als Verhandlungsverfahren ohne Teilnahmewettbewerb gemäß §14 Abs. 4 Nr. 3. VgV und mit einer Angebotsfrist von 10 Tagen aufgrund der Dringlichkeit gemäß Rundschreiben des BMWK v. 13.4.22 durchgeführt.

- Dringende Gründe im Zusammenhang mit für den öffentlichen Auftraggeber unvorhersehbaren Ereignissen, die den strengen Bedingungen der Richtlinie genügen

IV.1.3. Angaben zur Rahmenvereinbarung

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

IV.2. Verwaltungsangaben

Abschnitt V: Auftragsvergabe/Konzessionsvergabe

V.2. Auftragsvergabe/Konzessionsvergabe

V.2.1. Tag der Zuschlagsentscheidung
27/02/2023

V.2.2. Angaben zu den Angeboten
Der Auftrag wurde an einen Zusammenschluss aus Wirtschaftsteilnehmern vergeben: nein

V.2.3. Name und Anschrift des Auftragnehmers/Konzessionärs
Offizielle Bezeichnung: Netgo Nord GmbH
Ort: Hannover
NUTS-Code: DE929 Region Hannover
Land: Deutschland
Der Auftragnehmer/Konzessionär wird ein KMU sein: nein

V.2.4. Angaben zum Wert des Auftrags/Loses/der Konzession
Gesamtwert des Auftrags/des Loses/der Konzession: 610 172,00 EUR

V.2.5. Angaben zur Vergabe von Unteraufträgen

Abschnitt VI: Weitere Angaben

VI.3. Zusätzliche Angaben

VI.4. Rechtsbehelfsverfahren/Nachprüfungsverfahren

VI.4.1. Zuständige Stelle für Rechtsbehelfs-/Nachprüfungsverfahren

Offizielle Bezeichnung: Vergabekammer Lüneburg
Ort: Lüneburg
Land: Deutschland

VI.5. Tag der Absendung dieser Bekanntmachung

28/02/2023