Приложение № 1

УТВЪРДИЛ:

(Мартин Банков, директор на дирекция ИКС)

ЗАДАНИЕ

с условията за възлагане на обществена поръчка

1. Наименование на предмета на поръчката: Осигуряване на достъп до интернет и на решение за спиране на DDoS (Distributed Denial of Service) атаки към мрежатана Министерство на външните работи.

2.Пълно описание на предмета на поръчката, включително на обособените позиции, ако има такива, наименование на поръчката:

Настоящата поръчка има за цел да осигури Изпълнител на услуги по предоставяне на достъп до интернет и на решение за спиране на DDoS (Distributed Denial of Service) атаки към мрежата на Министерство на външните работи (МВнР).

Достъпът до интернет на Министерство на външните работи трябва да се осъществява по гарантиран и несподелен с други клиенти канал за достъп с капацитет от минимум 1,5 Gbps, без ограничения по трафик и съотношение на трафика IN : OUT = 1:1. Доставката на услуга до обекта на Възложителя трябва да се извършва през подземна кабелна мрежа по оптична линия през две независими оптични трасета. По вътрешните и външните трасета трябва да се поддържа динамична маршрутизация – Border Gateway protocol 4 (BGP4). Трябва да е предоставена възможност за наблюдение на горепосочените връзки с възможност за ping, traceroute, BGP summary или др. Услугата трябва да е с висока степен на надеждност (непрекъсваемост/uptime на услугата – минимум 99,5% на месечна база; осигурен Център за управление на предоставяните услуги в реално време, работещ в режим 24х7; схема за реакция при проблем с описани ескалационни процедури и евентуални действия/сценарии.). Комуникационните услуги, както и техническото оборудване, предоставено на Възложителя в съответствие с договора, трябва да се обслужва и поддържа 365 дни в годината, 24 часа в денонощието, 7 дни в седмицата чрез сертифицирани специалисти. Услугата трябва да включва и осигуряването на минимум 256 IP адреса и регистрация на автономна система за нуждите на МВнР.

Предложеното решение за спиране на DDoS (Distributed Denial of Service) атаки към мрежата на МВнР трябва да гарантира поддържане в устойчиво състояние на работните процеси при кибер атаки върху ИТ инфраструктурата на министерството. То трябва да осигури защита на вътрешната инфраструктура и мрежа на Възложителя от мрежови атаки, идентифициране и незабавно неутрализиране на нетипичен трафик и наличие на резервна инфраструктура, която може веднага да се използва за защита при отпадане на основната. Резервната и основната инфраструктура да се намират на територията на Европа, което да гарантира незначителни стойности на добавеното времезакъснение при пречистване на трафика. Решението не трябва да изисква инвестиция в оборудване и квалифицирани специалисти от страна на МВнР.

Трябва да бъдат осигурени първоначална инсталация и пускането в действие на услугите.

Поръчката не е разделена на обособени позиции.

3. Позиция на поръчката в утвърдения график на обществените поръчки:

т.т. 18, 21 и 29 от Списъка на поръчките за директно възлагане по чл. 20, ал. 4 от ЗОП за периода от 01.01.2019 г. до 31.12.2019 г.

4. Начин и място на изпълнение на поръчката: Централно управление на Министерство на външните работи на адрес: София 1113, улица "Александър Жендов" № 2.

5. Технически спецификации за изпълнението на поръчката

**Параметри на услугата по доставка на Интернет:**

1. Изпълнителят да осигурява интернет по гарантиран и несподелен с други клиенти канал за достъп, без ограничения по трафик и съотношение на трафика IN : OUT = 1:1.
2. Изпълнителят е необходимо да разполага с технически възел (възли) извън страната (в Европа), което да му позволява да управлява от край до край качеството на предоставяната Интернет свързаност. Следва в техническото си предложение да посочи списък с локацията (страна, град) на техническия възел (възли), както и списък на отделните връзки, входящи и изходящи капацитети/скорости към Tier 1 доставчиците.
3. Изпълнителят да гарантира симетрична скорост за международното и българско Интернет пространство с капацитет от минимум 1,5 Gbps.
4. Изпълнителят да осигури по вътрешни и външни трасета поддържане на динамична маршрутизация – Border Gateway protocol 4 (BGP4)
5. Доставката на услуга до обекта на Възложителя трябва да се извърши през подземна кабелна мрежа по оптична линия през **две независими оптични трасета.**
6. Изпълнителят е необходимо да предостави възможност за наблюдение на горепосочените връзки с възможност за ping, traceroute, BGP summary или др.
7. Изпълнителят е необходимо да осигури адресно пространство минимум 256 IP адреса и да регистрира автономна система за нуждите на Възложителя.
8. Изпълнителят следва да гарантира в техническото си предложение висока надеждност на услугата със следните параметри:

* Достъпност (непрекъсваемост/uptime на услугата) – минимум **99,5%** на средномесечна база;
* Център за управление на предоставяните услуги в реално време (Help desk), работещ 24 часа в денонощието, седем дни в седмицата, 365 дни в годината;

1. Изпълнителят следва да предоставя комуникационните услуги 365 дни в годината, 24 часа в денонощието, 7 дни в седмицата.
2. Изпълнителят следва да извършва обслужване и поддръжка на комуникационните услуги, както и на техническото оборудване, предоставено на Възложителя в съответствие с договора, 365 дни в годината, 24 часа в денонощието, 7 дни в седмицата чрез сертифицирани специалисти.
3. Изпълнителят е необходимо да представи схема за реакция при проблем. В схемата следва да се опишат ескалационни процедури и евентуални действия/сценарии.

**Параметри на услугата DDoS (Distributed Denial of Service):**

Всеки участник е необходимо да осигури и опише решение за спиране на DDoS (Distributed Denial of Service) и DoS (Denial of Service) атаки към мрежата на Възложителя. Предложеното решение от Изпълнителя трябва да отговаря на следните изисквания:

1. Услугата да позволява поддържане на устойчивост на работните процесите при кибератаки върху IT инфраструктурата на Възложителя;
2. Да бъде осигурена пълна защита на вътрешната инфраструктура и мрежа на Възложителя от мрежови атаки. Нетипичния трафик да се идентифицира и незабавно да се неутрализира;
3. Защитата да се извършва в реално време като нетипичния трафик постоянно се рутира и пречиства още на мрежово ниво през DDoS платформа;
4. Към интерфейса на възложителя да се рутира само легитимен трафик;
5. Услугата да се осъществява без необходимост от инвестиция в оборудване и квалифицирани специалисти от страна на Възложителя;
6. Наличие на резервна инфраструктура, която може веднага да се използва за защита при отпадане на основната;
7. Резервната и основната инфраструктура да се намират на територията на Европа, което да гарантира незначителни стойности на добавеното времезакъснение при пречистване на трафика;

**Първоначална инсталация и пускане в действие на услугата:**

Първоначалната инсталация и пускането в действие на услугата включва:

1. Изграждане на физическата свързаност между обекта на Възложителя и инфраструктурата на Изпълнителя.
2. Конфигуриране на услугата.
3. Предоставяне достъп до Интернет – международен и национален.
4. Въвеждане на автономна система.
5. Провеждане на тестове на предоставената услуга за покриване на изискванията на Възложителя.

6. Срок на изпълнение на поръчката и информация относно отделните доставки и/или услуги, етапи и дейности:

Срок за предоставяне на услугите – 12 месеца. Срок за първоначална инсталация и пускане в действие на услугата – 5 работни дни.

7. Прогнозно количество/обем на поръчката: Виж Техническите спецификации.

8. Гаранционни условия (когато е необходимо): Неприложимо.

9. Етапи и критерии за приемане на доставката, услугата и/или строителство, и други специфични изисквания към потенциалните изпълнители и изпълнението на поръчка, ако има такива. Неприложимо.

10. Предложение за критерии за подбор на кандидатите или участниците /изисквания за правоспособност, технически и професионални способности; икономическо и финансово състояние (което е приложимо) и за документите, с които се доказва съответствието:

1. **Годност (правоспособност) за упражняване на професионална дейност на участниците**

Участникът трябва да притежава Удостоверение, издадено от КРС, че лицето е вписано в регистъра по. Чл. 33, ал. 1, т. 1,  от Закона за електронните съобщения за предоставяне на следните услуги, чрез които се осъществяват обществени електрони съобщения: Пренос на данни на територията на Република България  и достъп до интернет на територията на Република България.

1. **Икономическо и финансово състояние на участниците**

Възложителят не поставя изисквания за икономическо и финансово състояние на участниците.

1. **Изисквания към техническите и професионалните способности на участниците**
   1. **Опит в изпълнението на доставки/услуги, идентични или сходни с предмета на поръчката**
      1. Участникът да е изпълнил минимум 1 (една) дейност с предмет, идентичен или сходен с предмета на поръчката през последните три години, считано от датата на подаване на офертата.

Под „дейност, сходна с предмета на обществената поръчка“ следва да се разбира дейност, свързана с доставка на интернет (с минимална скорост 1.5 Gb/s) и защита от мрежови атаки.

Възложителят не изисква обем на доставката.

***Забележка*:** *„Изпълнена“ е тази дейност, която е приключила в рамките на 3-годишния период преди датата на подаване на офертата, независимо от датата на възлагането на услугата и резултатът от нея е надлежно приет от възложителя.*

Информация за опита на участника се попълва в Част IV, Раздел В, за поръчки за доставки: извършени доставки от конкретния вид“ от еЕЕДОП.

Съответствието с минималните изисквания по т. 3.1.1. от този раздел относно опит в изпълнението на доставки, идентични или сходни с предмета на поръчката, се установява съгласно чл. 64, ал. 1, т. 2 ЗОП.

* + 1. Участникът следва да е регистриран от RIPE NCC (https://www.ripe.net/) като LIR (Local Internet Registry) със собствена автономна система и клас С мрежа. Участникът следва да посочи линк и/или приложи разпечатка от сайта на RIPE или/и друг документ, доказващ регистрацията му в RIPE NCC.
    2. Участникът в процедурата трябва да разполага с адресно пространство от минимум 630 000 IP адреса. Като доказателство участникът в процедурата трябва да приложи разпечатка от сайта на RIPE.
    3. Участникът трябва да има сключени договори с минимум два Tier 1 интернет доставчика. Като доказателство, участникът в процедурата следва да приложи декларация, с описание на скоростите към всеки един от доставчиците.
    4. Участникът в процедурата трябва да разполага с минимум два независими наземни двупосочни международни канала за достъп до интернет, опериращи автономно, с общ сумарен симетричен капацитет минимум 70 Gbps. Като доказателство участникът следва да предостави декларация с приложен списък на отделните връзки, входящи и изходящи капацитети/скорости, технология на преноса и връзката, кореспондиращата Автономна система на международния доставчик.
  1. **Изисквания към стандарти за осигуряване на качеството и стандарти за екологично управление** 
     1. Участникът следва да прилага система за управление на качеството, съответстваща на стандарт БДС ЕN ISO 9001:2015 или еквивалентен с обхват, сходен с предмета на поръчката. Поставеното изискване се доказва с копие на документ по чл. 64, ал. 1, т. 10 от ЗОП – сертификат, издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция "Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки.

За установяване на съответствие с изискванията към стандарти за осигуряване на качеството и стандарти за екологично управление, избраният за изпълнител участник представя копие от сертификат за управление на качеството съгласно стандарт БДС ЕN ISO 9001:2015 или еквивалентен с обхват, сходен с предмета на поръчката. Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за осигуряване на система за управление на качеството. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

* + 1. Участникът трябва да прилага сертифицирана система за управление на ИТ услуги, съответстваща на стандарт БДС EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за управление на услугите съгласно стандарта БДС EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката, издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция "Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване.

* + 1. Участникът трябва да прилага сертифицирана система за управление на сигурността на информацията, съответстваща на стандарт БДС EN ISO/IEC 27001:2013 или еквивалент, с обхват сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за управление на сигурността на информацията съгласно стандарта БДС EN ISO/IEC 27001:2013 или еквивалентен, с обхват сходен с предмета на поръчката, издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция "Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване.

* 1. **Минимални изисквания към персонала/екипа за изпълнение на поръчката**

Участникът трябва да разполага с квалифициран екип за изпълнение на поръчката, който да включва най-малко следните видове експерти:

* + 1. Ключов експерт 1: „Ръководител на проекта“ - минимум 1 експерт
* Образование: Висше образование, образователно-квалификационна степен „бакалавър” или по-висока в една от следните области „Природни науки, математика и информатика“, „Социални, стопански и правни науки“ или „Технически науки“ (съгласно Класификатора на областите на висшето образование и професионалните направление, утвърден с ПМС № 125 от 2002 г.) или еквивалентна образователна степен, когато е придобита в чужбина, в еквивалентни на посочените професионални направления – *доказва се с копие от диплома*;
* Специфичен професионален опит: минимум 2 (две) години практически опит като ръководител на проекти – *доказва се със сертификати, референции от работодател/възложител или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава валиден професионален сертификат за прилагане на методология за управление на проекти, издаден от международно призната организация за управление на проекти (Project Management Professional и/или Prince2 Practitioner или еквивалентен) – *доказва се със заверено копие от сертификата*;
  + 1. Ключов експерт 2: „Експерт мрежови технологии“ - минимум 3 експерти
* Образование: Висше образование, образователно-квалификационна степен „бакалавър” или по-висока (съгласно Класификатора на областите на висшето образование и професионалните направление, утвърден с ПМС № 125 от 2002 г.) или еквивалентна образователна степен, когато е придобита в чужбина, в еквивалентни на посочените професионални направления – *доказва се с копие от диплома*;
* Специфичен професионален опит: минимум 5 (пет) години практически опит в областта на мрежовите технологии – *доказва се със сертификати, референции от работодател/възложител или по друг еквивалентен начин*;
* Сертификати: експертът трябва да притежава валиден професионален сертификат CIE (Certified Internetwork Expert) или еквивалентен – *доказва се със заверено копие от сертификата*;

11. Предложение за критерий за възлагане, а при критерий за възлагане оптимално съотношение качество/цена: предложение за методика за определяне на комплексната оценка:

Критерий за възлагане „най-ниска цена“. За целите на оценката на офертата по процедурата за сключване на договор под „най-ниска цена” се разбира най-ниската предложена обща цена от участник за изпълнение на поръчката.

На първо място се класира участникът, предложил най-ниска обща цена за изпълнение на поръчката.

В случай, че най-ниската обща цена е предложена в две или повече оферти, комисията провежда публично жребий за определяне на изпълнител между класираните на първо място оферти.

12. Списък на лицата, които ще бъдат поканени да подадат оферти и обосновка за техния   
подбор, когато това е приложимо според вида на процедурата - попълва се за поръчки на   
договаряне без обявление; за поръчки на стойност под 30 000 лв. без ДДС може да се   
направи предложение за изпълнител/и въз основа на направено проучване: Неприложимо.

13. Обосновка за промяна, при обективна необходимост, в параметрите спрямо посочените в утвърдения график за обществените поръчки (попълва се само при обективна необходимост от промяна, като в случай, че промяната е свързана с финансовите   
параметри, заданието се съгласува от финансовия директор и главен счетоводител чрез добавяне на текст „съгласувал" и подпис в документа):

С оглед спазването на изискванията на чл. 21, ал. 15 от ЗОП и необходимостта от повишаване на нивото на мрежова и информационна сигурност чрез създаване на дълбоко ешалонирана киберзащита, чийто най-външен слой се явява спирането на DDoS (Distributed Denial of Service) и DoS (Denial of Service) атаки към мрежата на МВнР. Най-добра практика е прочистването на трафика да се осъществява от доставчика на интернет към съответната организация.

14. Информация за съдържаща се класифицирана информация: Няма.

15. Финансиране:

Финансирането е със собствени средства от бюджет на МВнР.

16. Други документи и информация, необходими, за определяне характеристиките на поръчката и реда за провеждане на избора на изпълнител: Няма.

Изготвил:

Николай Томов

Външен експерт по договор № 74/ОП-Д/2019