

Заявка

по рамков договор № РД-14-40 от 29.05.2023 г.
(вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД)

Позиция от ПГ-2024 г.:	№ по ред от ПГ	17.1
Описание на дейност/проект съгласно ПГ:	Услуга по предоставяне на DDoS защита и защита на уеб приложения за НЗОК	
CPV код	72222300-0	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (стойността следва да съответства на заложената в План-графика) без ДДС	238 000,00 лв., от които: За 2024 г. – 70 000 лв. За 2025 г. – 84 000 лв. За 2026 г. – 84 000 лв.	
Начин за плащане: (еднократно, на части, периодично, авансово или др.)	<p>Периодично, както следва:</p> <ul style="list-style-type: none"> • За периода от стартиране на услугата до 30.06.2024 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за съответния период и фактура на стойност 28 000,00 лв. без ДДС за съответния период; • За периодите 01.01.2025 г. - 30.06.2025 г., 01.01.2026 г. - 30.06.2026 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за съответния шестмесечен период и фактура на стойност 42 000,00 лв. без ДДС за съответния шестмесечен период; • За периода 01.07.2024 г. – 31.12.2024 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за периода 01.07.2024 г. – 08.12.2024 г. и фактура на стойност 42 000,00 лв. без ДДС за периода 01.07.2024 г. - 31.12.2024 г.; • За периода 01.07.2025 г. - 31.12.2025 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за периода 01.07.2025 г. - 08.12.2025 г. и фактура на стойност 42 000,00 лв. без ДДС за периода 01.07.2025 г. - 31.12.2025 г.; • За периода 01.07.2026 г. - 31.12.2026 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за периода 01.07.2026 г. - 08.12.2026 г. и фактура на стойност 42 000,00 лв. без ДДС за периода 01.07.2026 г. - 31.12.2026 г. 	
Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Срок за предоставяне на услугата – от стартиране на изпълнението до 31.12.2026 г.	
Гаранционен срок:	неприложимо	
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	<p>На части, както следва:</p> <p>1. За 2024 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга, както следва:</p> <ul style="list-style-type: none"> • За периода от стартиране на услугата до 30.06.2024 г. • За периода 01.07.2024 г. - 08.12.2024 г. 	

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните – Регламент (ЕС) 2016/679.

	<p>Дейностите по предоставяне на услугата за периода 09.12.2024 г. - 31.12.2024 г. се отчитат заедно със следващия отчетен период 01.01.2025 г. - 30.06.2025 г., като за тях не се дължи заплащане.</p> <p>2. За 2025 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга, както следва:</p> <ul style="list-style-type: none"> • За периода 01.01.2025 г. - до 30.06.2025 г. • За периода 01.07.2025 г. - 08.12.2025 г. Дейностите по предоставяне на услугата за периода 09.12.2025 г. - 31.12.2025 г. се отчитат заедно със следващия отчетен период 01.01.2026 г. - 30.06.2026 г., като за тях не се дължи заплащане. <p>3. За 2026 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга, както следва:</p> <ul style="list-style-type: none"> • За периода 01.01.2026 г. - до 30.06.2026 г. • За периода 01.07.2026 г. - 08.12.2026 г. • За периода 09.12.2026 г. - 31.12.2026 г. (без финансов ангажимент)
<p>Приложения: (напр: технически параметри, образци на отчетни документи)</p>	<p>Технически параметри</p>
<p>Настоящата заявка да се изпълни при условията на приложените Технически параметри.</p>	
<p>ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:</p>	
<p>Координатор по заявката:</p>	<p>_____</p>
<p>Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):</p>	<p>_____</p>
<p>ЗАЯВКАТА е ОДОБРЕНА ОТ:</p>	
<p>Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:</p>	<p>_____</p>
<p>ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:</p>	
<p>Координатор от „Информационно обслужване“ АД по заявката</p>	<p>_____</p>

Ръководител на проект/дейност по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

Услуга по предоставяне на DDoS защита и защита на уеб приложения за НЗОК

1. ПРЕДМЕТ

Предметът на заявката е услуга по предоставяне на защита от Distributed Denial of Service (DDoS) атаки и защита на уеб приложения за НЗОК. Услугата включва следното решение:

REQ. 1.	Тип решение: Хибридно решение под формата на облачна услуга и физически устройства за DDoS защита в мрежата на доставчика на услугата.
REQ. 2.	Компоненти за хибридна DDoS защита на мрежови слоеве 3 и 4, както и компоненти за Web DDoS защита и защита на уеб приложения (WAF) на мрежови слой 7.
REQ. 3.	Облачна услуга за защита.
REQ. 4.	Инспекция и защита от DDoS в реално време в режим „Постоянно активна“ (Always on).
REQ. 5.	Капацитет от минимум 600 Mbps чист трафик.
REQ. 6.	Функции за защита от криптирани flood атаки на база поведение, TLS инспекция, защита на приложения и информация за заплахи (threat intelligence).
REQ. 7.	Защита от уеб-базираны атаки срещу приложения по OWASP Top10 модела, стандартни уеб атаки, атаки с фокус върху данни и данни за достъп, както и непознати 0-day атаки.
REQ. 8.	Функции за WAF модула: използване на негативен или позитивен модел на сигурност, защита на API, управление на ботове, контрол на достъпа, геополитики за IP адреси, лимитиране на обема трафик към приложенията, използване на напреднали правила за сигурност, използване на ERT Active Attackers Feed (EAAF) технология за защита.
REQ. 9.	Инспектиране на криптиран (SSL) трафик.
REQ. 10.	Функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението.
REQ. 11.	Автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging).
REQ. 12.	Синхронизиране на политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението.
REQ. 13.	Показване на референтно сравнение на обема мрежови трафик по времето, когато няма активни атаки с обема на трафика при протичаща атака, с възможност за предприемане на автоматични защитни мерки срещу атаките според обемите им.
REQ. 14.	Автоматично известяване при настъпила атака (като да има опция за автоматично генериране на rsar файл след завършване на атаката). Да може да се предоставя информация за параметрите на наложената политика за сигурност на решението, която е спомогнала за спирането на дадена атака.

REQ. 15.	Автоматично издаване на различни отчети по подразбиране в различни формати по зададен график (седмични, месечни).
REQ. 16.	Предоставяне на детайлни отчети със следствени данни (forensics) относно възникналите предишни атаки и настоящите такива.
REQ. 17.	Извършване на анализ на поведението на ИТ мрежата (network behavioral analysis). Решението да може да използва механизми за самообучение и засичане на заплахи според промените на обема мрежови трафик и други негови параметри.
REQ. 18.	Засичане на заплахи на базата на собствена база от данни с репутации на IP адреси, която да се поддържа и обновява от производителя на решението в периода на поддръжката.
REQ. 19.	Функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентизиране на източника на трафика.
REQ. 20.	Предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението.
REQ. 21.	Поддържане използването на ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението.
REQ. 22.	Анализиране на поведението на DNS трафик. Да може да се изграждат сигнатури в реално време за възникнали атаки и да се автентизират източниците на мрежовия трафик за справяне с water-torture атаки, DNS flood атаки и Amplification атаки.
REQ. 23.	Засичане и да блокиране на непознати до момента заплахи (0-day защита).
REQ. 24.	Засичане и блокиране на burst атаки и botnet атаки.
REQ. 25.	Задаване и регулиране автоматично прагови стойности за брой: пакети в секунда (PPS), транзакции в секунда (TPS).
REQ. 26.	Функционалност за автоматично създаване на динамични сигнатури посредством анализиране на трафика.
REQ. 27.	Осигуряване на защита от UDP атаки, TCP атаки, DNS атаки., волуметрични атаки, ICMP атаки, HTTP атаки.
REQ. 28.	Осигуряване на защита от следните типове атаки, пропускайки легитимния потребителски трафик: SYN Floods , RST Flood, TCP ECE Flood, TCP NULL Flood.
REQ. 29.	Решението трябва да предоставя възможност за автоматично блокиране на цели списъци/категории от IP адреси източници на заплахи, динамично поддържани от вендора.
REQ. 30.	Решението трябва да осигурява защита от следните атаки: Misused Application Attack, Slow Read.
REQ. 31.	Решението следва да предоставя възможност за засичане на http-базирани heavy URLs с цел справяне с атаки фокусирани върху URL-и консумиращи значителни сървърни ресурси.

2. ИЗИСКВАНИЯ ЗА СТАРТИРАНЕ НА УСЛУГАТА

За стартиране на услугата по предоставяне на DDoS защита и защита на уеб приложения за НЗОК, предоставяна от ИО АД, е необходимо:

1. НЗОК да изиска и организира доставчикът на интернет свързаност на НЗОК да премести логическите връзки от текущо изградените в центъра за данни на ИО АД, находящ се на адрес: София, ул. Поручик Неделчо Бончев №33 (Equinix SO2). В случай, че доставчикът на интернет услуга на НЗОК, няма изграден cross-connect до комуникационен шкаф на ИО АД, то цената за изграждането му и месечният абонамент е за негова сметка.
2. Предоставяне на разрешение от Възложителя, IP адресите на НЗОК да се пуснат през облачна услуга за DDoS защита. Образец на разрешението се предоставя от Изпълнителя и следва да бъде подписано от управителя на НЗОК.

При изпълнение на описаното по-горе ИО АД се ангажира в рамките на двудневен срок да стартира предоставянето на услугата.