ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

Вх.
№30-00-320/15.11.2024
София

ЗАЯВКА

по рамков договор № РД-06-12 от 10.01.2024 г.
(вх. № ПО-16-309/10.01.2024 г. на „Информационно обслужване“ АД)

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*22*
Описание на дейност/проект съгласно ПГ:	*Предоставяне на Интернет свързаност и DDoS защита за МЗ и РЗИ*	
CPV код	*64210000-1 Услуги по пренос на данни и съобщения*	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (*стойността следва да съответства на заложената в План-графика* **) без ДДС**		***118 080,00 лв.**, от които:* *за 2025 г. – 57 600,00 лв.* *за 2026 г. – 60 480,00 лв.*
Срок за плащане: *(еднократно, на части, периодично или др.)*		*Периодично, както следва:* • *За периода от стартиране на услугите до 30.06.2025 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода и фактура на стойност 28 800,00 лв. без ДДС;* • *За периода 01.07.2025 г. - 31.12.2025 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода 01.07.2025 г. - 10.12.2025 г. и фактура на стойност 28 800,00 лв. без ДДС за периода 01.07.2025 г. - 31.12.2025 г.;* • *За периода 01.01.2026 г. - 30.06.2026 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода и фактура на стойност 30 240,00 лв. без ДДС;* • *За периода 01.07.2026 г. - 31.12.2026 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане предоставените услуги за периода 01.07.2026 г. - 10.12.2026 г. и фактура на стойност 30 240,00 лв. без ДДС за периода 01.07.2026 г. - 31.12.2026 г.*
Плащане с акредитив ДА/НЕ		*Не е приложимо*
Документи за плащане с акредитив		*Не е приложимо*

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

Срок на изпълнение: (*от дата - до дата или в месеци, ако не е обвързан с конкретна дата*)	*Срок за предоставяне на услугите от стартиране на изпълнението[1] до 31.12.2026 г. За стартиране на изпълнението Изпълнителят информира Възложителя.*	
Гаранционен срок:	*Неприложимо*	
Отчитане: *(периодично - посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Периодично, както следва:* • *За периода от стартиране на услугите до 30.06.2025 г. и за периода 01.01.2026 г. - 30.06.2026 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за съответния период;* • *За периода 01.07.2025 г. – 10.12.2025 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода. Извършените услуги за периода 11.12.2025 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;* • *За периода 01.07.2026 г. – 10.12.2026 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода;* • *За периода 11.12.2026 г. – 31.12.2026 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставените услуги за периода (без финансов ангажимент).*	
Приложения: (*напр.: технически параметри, образци на отчетни документи*)	*Технически параметри*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		*Подпис:*

[1] Изпълнението на заявката стартира след изпълнение на дейностите по инсталация на защитни стени по проект по ред 16 от ПГ 2024.

Ръководител на проект/дейност по заявката *(напр.: представител на дирекцията - Заявител):*		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		*Подпис:*
Ръководител на проект/дейност по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно		*Подпис:*

обслужване“ АД		

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ПРЕДОСТАВЯНЕ НА ИНТЕРНЕТ СВЪРЗАНОСТ И DDOS ЗАЩИТА ЗА МЗ И РЗИ

2024 г.

1. ОБХВАТ

Обхватът на проекта, включва:

1.1. Предоставяне на Интернет свързаност с минимална скорост 600 Mbps и диапазон от минимум 64 реални статични адреса. Услугата се предоставя до колокираното оборудване на РЗИ в технически център на „Информационно обслужване“ АД в София.

1.2. Предоставяне на защита от Distributed Denial of Service (DDoS) атаки

DDoS услугата трябва да е в режим „Винаги налична“ и да осигурява неутрализирането на атаки от Интернет пространството към мрежата и изчислителните ресурси на МЗ и РЗИ, които могат да доведат до консумиране на честотна лента на атакуваната мрежа или да претоварят изчислителните ресурси на атакуваните устройства.

В обхвата на услугата Изпълнителят извършва проактивен мониторинг за установяване на DDoS атаки към мрежата на МЗ и РЗИ, както и осигурява 24/7 активни телефон и мейл за връзка с посочено от Изпълнителя лице за контакт при установени от Възложителя атаки или проблеми в предоставяната услуга.

Услугата по предоставяне на защита от Distributed Denial of Service (DDoS) атаки, включва следното решение:

Общи изисквания	
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-базирани 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, гео-политики 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 pcap 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 IT 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 автентикиране 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 автентикират източниците на мрежовия трафик за справяне с water-torture атаки, DNS flood атаки и Amplification атаки.
REQ. 23.	Засичане и 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 на 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.	Предоставяне на възможност за автоматично блокиране на цели списъци/категории от IP адреси източници на заплахи, динамично поддържани от вендора.
REQ. 30.	Осигуряване на защита от следните атаки: Misused Application Attack, Slow Read.
REQ. 31.	Предоставяне на възможност за засичане на http-базирани heavy URLs с цел справяне с атаки фокусирани върху URL-и консумиращи значителни сървърни ресурси.

2. ПАРАМЕТРИ НА КАЧЕСТВОТО

2.1. Заявки за обслужване (тикети) се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ.

2.2. Време за реакция - до 1 час след регистриране на проблем.

Времето за реакция е времето от момента на уведомяване за възникнал проблем до обратна реакция (обаждане или пристигане на място*).*

2.3. Време за отстраняване на проблем - до 4 часа след регистриране на проблем.