Приложение № 2

към рамков договор № 93-00-97/03.07.2020 г.

Заявка

по рамков договор № 93-00-97 от 03.07.2020 г.

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*20*
Описание на дейност/проект съгласно ПГ:	*Изграждане на допълнителен слой за инспекция и проверка на мрежови трафик*	
CPV код	*30230000-0* *32420000-3*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**	*Обща сума в размер на 476 420,00 лв. без ДДС*[1]	
Срок за плащане: *(еднократно, на части, периодично или др.)*	*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка/дейност и фактура.*	
Плащане с акредитив / Авансово плащане (условия) ДА/НЕ	*НЕ*	
Документи за плащане с акредитив	*неприложимо*	
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Съгласно чл.1 ал. 2 от Договора, заявката следва да бъде изпълнена след осигурено финансиране от страна на Възложителя.* *Срок за осигуряване – до 4 месеца от подписване на заявката.* *Срок за доставка – до 60 дни след получаване на уведомление за осигурено финансиране от страна на Възложителя.*	
Гаранционен срок:	*Съгласно условията на ТС*	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка/дейност.*	
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Техническа спецификация*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		
Ръководител на проект/дейност по заявката (напр.: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		

[1] Заявката се подписва под условие и ще бъде изпълнена при осигурено финансиране от страна на Възложителя.

ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Координатор от „Информационно обслужване“ АД по заявката	
Ръководител на проект/дейност по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

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

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИЯ

За изграждане на допълнителен слой за инспекция и проверка на мрежови трафик

1. Обект на заявката

Обекта на заявката съгласно Общия терминологичен речник – CPV е с код, както следва:

CPV код	Описание
32420000-3	Мрежово оборудване

2. Обща информация

За осигуряване на киберсигурността в Агенция по вписванията се използва защита в дълбочина - Defense in depth, при която се използва многопластово концептуално разделяне на слоеве защита, като на всеки слой се използват различни подходи, технологии и инструменти за осигуряване на сигурност. За Защити на периметъра – това е границата, до която достигат възможностите за управление и контрол в ИТ организацията. След нея е друг доставчик на услуги (Интернет доставчик), партньорска фирма или ненадежден/съмнителен потребител на уеб услугите на компанията. Основната цел при защитата на периметъра е да опитаме да спрем ненужното и да контролираме и наблюдаваме всичко останало. Основни инструменти за защита на това ниво са защитните стени на мрежово и приложно ниво (NGFW и WAF), както и системите за превенция на атаки от тип разпределен отказ от услуга - DDoS (Distributed Denial of Service). На тези системи се създават правила за достъп, да се прилагат профили за инспекция на трафика и да се блокират нежелани и открити опити за атаки, източници на зловредни заявки и други.

За Мрежови защити – Следващият слой на защита е вътрешната комуникационна мрежа. Добрите практики са за разделяне на отделни виртуални мрежи спрямо предназначението – потребителски, администраторски, сървърни мрежи, управление на устройствата, продукционни среди и тестови среди и т.н. в зависимост от организационните нужди. Между отделните мрежови сегменти се прилагат различни нива на достъп, ако е необходим такъв. Защитата се осигурява основно посредством мрежовите устройства – защитни стени, маршрутизатори и комутатори, но е добра практика да се инсталират и системи за детекция и превенция на зловреден трафик (Intrusion Detection/Prevention System).

Необходимо е да бъде изграден допълнителен слой за инспекция и проверка на мрежовия трафик и навременно предотвратяване на пробив в мрежата на Агенция по вписванията.

3. Предмет

Настоящата заявка обхваща:

- **Доставка гранични стени от следващо поколение (защитни стени втори слой),** както следва:

Обща информация	
REQ.1.	Количество – 4 броя.
Спецификация – минимални изисквания	
REQ.2.	Минимална пропускателна способност с активирана функция за идентификация на приложенията - 11 Gbps
REQ.3.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/Firewall/Application Control – 5.1 Gbps
REQ.4.	Минимална производителност за IPsec VPN – 6.7 Gbps
REQ.5.	Минимален брой сесии - 1 400 000
REQ.6.	Минимален брой нови сесии в секунда - 145 000
REQ.7.	Разпознати и поддържани приложения (минимум) - 3 650 броя
REQ.8.	Минимален брой мрежови интерфейси: • Да разполага 12x1/2.5/5/10G Base-T ports • Да разполага с 10x1/10G SFP/SFP+ интерфейса • Да има възможност за допълнителни минимум 4x25G SFP28
REQ.9.	Режими на работа на интерфейсите: • L2 • L3 • Tap • Transparent • едновременно/микс да се използват върху едно устройство.
REQ.10.	Машрутизиращи протоколи: • OSPFv2/v3 • BGP with graceful restart • RIP • Static routing • Policy-based forwarding • Point-to-Point Protocol over Ethernet (PPPoE) • Bidirectional Forwarding Detection (BFD)
REQ.11.	Минимални изисквания към IPSec имплементация: • Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) • Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

REQ.12.	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи) - 1000 SSL VPN потребителя,
REQ.13.	Минимален брой IPSec Site-to-Site VPN - 2000 отдалечени точки.
REQ.14.	Устройството да поддържа виртуални таблици за маршрутизация минимум 11 броя.
REQ.15.	Устройството да има възможност да поддържа виртуализация (виртуални контексти) – 11 броя.
REQ.16.	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.17.	Системата следва да декриптира и инспектира SSL като поддържа : TLS v1.1, TLS v1.2, TLS v1.3
REQ.18.	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
REQ.19.	Режим на надеждност: • Active-Passive • Active/Active Клъстер до 6 устройства разпределени в отдалечени центрове за данни.
REQ.20.	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): • 1 x 10/100/1000 out-of-band management port • 2 x 100/1000Mbps, 1 x 10Gbps SFP+ интерфейси за отказоустойчивост • 1 x RJ-45 конзолен порт
REQ.21.	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 1U
REQ.22.	Резервирано, 100-240VAC (50-60Hz)
Функционални изисквания към системата	
REQ.23.	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
REQ.24.	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.25.	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време;
REQ.26.	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis, Bare metal analysis
REQ.27.	Предлаганата защитна стена трябва да може да изпраща минимум 2000 файла на час към системата за анализ на Zero Day;
REQ.28.	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.29.	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;
REQ.30.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;
REQ.31.	NGFW възможностите и прилежащите бази данни като Antivirus, Sandboxing трябва да използват сигнатури и съдържание на производителя на защитната стена – Не се приема OEM или интеграция с трети страни;

REQ.32.	Управлението на устройството трябва да се реализира че физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.33.	Решението да използва вътрешните ресурси на защитната стена за да анализира и открива зловреден JavaScript с цел кражба на корпоративни потребителски имена и пароли чрез Phishing;
REQ.34.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.35.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2, TLSv1.3);
REQ.36.	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.37.	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина;
REQ.38.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, Linux, macOS, Android, iOS, Raspbian, Ubunto
REQ.39.	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.40.	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
REQ.41.	Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
REQ.42.	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.43.	Да предоставя възможност за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.44.	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
REQ.45.	Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
REQ.46.	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.
REQ.47.	Анализът на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс, без да необходима инсталация на допълнителен софтуер.
REQ.48.	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
REQ.49.	Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
REQ.50.	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на АГКК или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.

REQ.51.	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
REQ.52.	Решението да предоставя механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително възможност да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA));
REQ.53.	Системата да има възможност за надграждане с допълнителен лиценз за филтриране на уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мулти категоризация на URL съгласно тип на съдържанието и риск. Да има възможност да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request, включително да може да идентифицира новорегистрирани домейни и ограничава достъпа до тях;
REQ.54.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, чрез който да осъществява отдалечен защитен достъп от телефони и таблети (с операционни системи iOS, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
REQ.55.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
Гаранция и поддръжка:	
REQ.56.	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ.57.	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.58.	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.59.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя, както и с всички необходими мрежови и захранващи кабели.

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка и предоставяне на гаранционна поддръжка на предлаганите софтуерни и хардуерни продукти на територията на Република България.

4. Други условия:

В рамките на две седмици да се осигурят до 2 онлайн семинара до 4 часа всеки, с цел базово запознаване на експерти (екип до петима служители) от Агенция по вписванията с основни функционалности на продукта.

5. Място на изпълнение

Място на изпълнение: гр. София, ул. „Елисавета Багряна“ № 20 и ул. „Лъчезар Станчев“ № 11.