Пазарна консултация № 44126 с предмет „Модернизация на модулите към системата за Интернет комуникация и повишаване на киберсигурността в информационната инфраструктура на "АЕЦ Козлодуй" ЕАД”

„АЕЦ Козлодуй” ЕАД уведомява всички заинтересовани лица, че във връзка с подготовката за възлагане на обществена поръчка и определяне на прогнозна стойност, на основание на чл. 44 от ЗОП набира индикативни предложения за „Модернизация на модулите към системата за Интернет комуникация и повишаване на киберсигурността в информационната инфраструктура на "АЕЦ Козлодуй" ЕАД”.

Предложението следва да включва:

- подробно описание, съгласно приложените по-долу техническо задание + техническа спецификация - Приложение №1;
- единична цена и обща стойност без ДДС, валута;
- информация за срок и условие на доставка, гаранционен срок / срок на годност;
- съпроводителна документация при доставка;
- точен адрес и лице за контакт, телефон, факс, e-mail, интернет адрес;
- ако участникът не е производител да се представи документ за представителство /оторизационен документ от производителя, даващ разрешение за продажба на предлаганата стока.

Запитвания във връзка с провежданите пазарни консултации може да бъдат отправяни до 07.08.2020 г. на e-mail: commercial@npp.bg, като разясненията ще бъдат публикувани на Интернет страницата на „АЕЦ Козлодуй” ЕАД в раздел Актуално / Обществени поръчки / Пазарни консултации.

Краен срок за подаване на индикативни предложения: 14.08.2020 г. на e-mail: commercial@npp.bg

Цялата информация, разменена по повод проведените пазарни консултации, ще бъде публикувана в профила на купувача.

С подаване на индикативно предложение, всеки участник в пазарните консултации се съгласява, че предложението и всякаква друга информация, предоставена като резултат от пазарните консултации, ще бъде публично достъпна в профила на купувача.

Възложителят си запазва правото да използва индикативни предложения, получени при проведени пазарни консултации, за възлагане на обществени поръчки до стойностните прагове на чл. 20, ал. 4 от ЗОП.

Допълнителна информация може да бъде получена от Христо Пачев - Експерт „Маркетинг”, тел. +359 973 7 6140, e-mail: HPatchev@npp.bg

Приложения:

1. Техническо задание + техническа спецификация - Приложение №1

Блок: **Информационни технологии**

Система:

Подразделение: **П**

ТЕХНИЧЕСКО ЗАДАНИЕ

№ 20.П.ТЗ.148/01

За доставка

ТЕМА: Модернизация на модулите към системата за Интернет комуникация и повишаване на киберсигурността в информационната инфраструктура на „АЕЦ Козлодуй” ЕАД

Настоящото техническо задание съдържа техническа спецификация съгласно Закона за обществените поръчки.

1. Описание на доставката

Доставка и въвеждане в експлоатация на устройства, повишаващи надеждността и защитата на Интернет свързаността на дружеството, отговарящи на съвременните условия за защита и киберсигурност.

1.1. Материали, консумативи, машини и оборудване (СМЗ-стоково материални запаси), които трябва да се доставят.

Съгласно приложена техническа спецификация (Приложение 1).

1.2. Нестандартни/специализирани елементи, резервни части и инструменти към доставката

Към оборудването да се доставят нужните интерфейсни и захранващи кабели, монтажни елементи, инструменти, специализиран софтуер, драйвери и лицензи, необходими за монтаж и интегриране на компонентите в съответните системи.

2. Основни характеристики на оборудването и материалите

Минимални функционални изисквания:

1. Обособяване на зони с различна степен на доверие, като разделя мрежата на отделни сегменти според функционалните им характеристики;
2. На база на акредитация от Активната Директория контролира поведението на всеки един потребител при достъпа му до Интернет и вътрешните ресурси.
3. Инспекция на трафика и идентификация на приложенията.
4. Защита от мрежови атаки чрез система за превенция на атаките (IPS).
5. Системата да анализира съдържанието за наличие на зловреден код (AntiVirus и AntiSpyware). Да се прилагат различен анализ на база категория от URLs или група от приложения.
6. Системата да има възможност за надграждане с допълнителен лиценз, който да позволява анализ на Zero Day зловреден код чрез стартиране на файла във защитената среда. Да се прилагат различен анализ на база приложения, група от приложения и типове файлове.
7. Филтриране на уеб сайтовете по категории с цел да се ограничи достъпа на потребителите на вътрешни за мрежа до ресурси до опасно съдържание в Интернет.
8. Решението трябва да предоставя възможност за мултикатегоризация на URL съгласно тип на съдържанието и риск.
9. Решението трябва да предоставя възможност за идентифициране на ново регистрирани домейни и ограничаване на достъпа до тях.
10. Наличие на DLP (Data Loss Prevention) функционалност, като по този начин ще се осъществява идентификация на файлове по име и разширение, изпращани и/или получавани в мрежовия трафик.
11. Инспекция на HTTPS и HTTP 2.0 протокола - декриптиране и инспекция на входяща и изходящ SSL мрежова комуникация.
12. Декриптиране на SSL мрежова комуникация, която транспортира в себе си криптирани SMTP, IMAP, POP3, FTP.
13. Декриптирането на SSL трафика, прозрачно за всички функционални компоненти на системата: IPS, AntiVirus, AntiSpyware, инспекция на данни и файлове, и URL филтриране.
14. Политиката за декриптиране трябва да има възможност да се настройва на база на URL категория.
15. Политиката за декриптиране трябва да има възможност да блокира достъпа до даден Web Site в случай, че отсрещната страна не използва необходимо ниво на криптиране или валиден сертификат.
16. Системата да предоставя възможност за надграждане с допълнителен лиценз, който да позволява отдалечен VPN достъп от мобилни устройства (iOS, Android) и Clientless SSL VPN. Включително инспекция (compliance check) на крайно клиентската машина преди изграждането на отдалечен достъп.
17. Блокиране на всички приложения, които не са изрично указани като разрешени за използване в конфигурираните в системата политики, да бъдат блокирани.
18. Идентификация на приложенията без оглед на използвания от тях комуникационен порт и протокол.
19. Възможност за конфигурация на политиките за сигурност чрез дефиниране на източника на мрежовата комуникация, крайната цел на мрежовата комуникация (посока), приложението и/или приложенията, за които се отнася политиката, дефиниране на мрежовите услуги както и каква да бъде активната реакция ако критериите бъдат

изпълнени.

20. Препращане на подозрителните DNS заявки към специално подбран произволен адрес с цел бърза идентификация и блокиране на комуникацията на заразени хостове от вътрешната мрежа (DNS sinkholing).
21. Възможност за дефиниране на VLAN-и за Layer 2 и Layer 3 интерфейсите с цел да се осигурят гъвкави механизми за инспекция на трафика, които да поддържат създадените за нуждите на организацията мрежови сегменти.
22. Възможност за изграждане на site-to-site VPN тунели на база IPSec и IKE стандартите.
23. Възможност за управление и приоритизиране на трафика (QoS) според типа приложение.
24. Прозрачна идентификация на потребителите без изискване да се предоставят потребителско име и парола.
25. 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).
26. Възможност за дефиниране на индивидуални маршрутизиращи таблици с цел осигуряване на маршрутизиращи функционалности за различните мрежови сегменти.
27. Възможност за конфигурация устройства да работят в режим на отказоустойчивост (High-availability), чрез конфигуриране Active-Active или Active-Passive.
28. Възможност за мониторинг, анализ на логовете и репортинг от самото устройство.
29. Уеб базиран интерфейс за управление на устройството и индивидуално дефинируеми в системата полета за показване на различни статистики на база време, приложение, категории, потребители и заплахи.
30. Логовете на устройството да са достъпни в уеб интерфейса с възможност за контекстуално филтриране или филтриране на база ключова дума. Информацията следва да е обогатена контекстуално с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и др.).
31. Възможност за интеграция с облачна услуга на същия производител за анализ и отчет на текущите атаки/заплахи както за организацията така и за сходни с нея. Показване на тенденции, анализи и методи за превенция в световен мащаб.
32. Решението да инспектира DNS трафика на организацията и да реализира превенция на атаки базирани на DNS Tunneling.
33. Решението да разполага с механизъм за следене и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA)).
34. Предложените устройства да имат възможност за интеграция с решение за SD-WAN от същия или друг производител.

2.1. Класификация на оборудването

Към заявеното оборудване няма специални изисквания и не се класифицира по сеизмоустойчивост.

2.2. Квалификация на оборудването

Заявеното оборудване няма отношение към безопасността. Няма специални изисквания по отношение на радиация, пожар, корозия, взрив и т.н.

2.3. Физически и геометрични характеристики

Съгласно приложена техническа спецификация (Приложение 1).

2.4. Характеристики на материалите

Няма отношение.

2.5. Химични, механични, металургични и/или други свойства

Няма отношение.

2.6. Условия при работа в среда с йонизиращи лъчения

Няма отношение.

2.7. Нормативно-технически документи

Предлаганото оборудване трябва да съответства на съществените изисквания по отношение на генерираните електромагнитни смущения на актуалната Наредбата за съществените изисквания и оценяване съответствието за електромагнитна съвместимост - изпълнявайки приложимите изисквания на БДС EN 55032:2015 "Устройства за обработка на информация. Характеристики на радиочестотно смущаващо въздействие. Гранични стойности и методи за измерване" или еквивалентен, както и да съответства на Наредбата за съществени изисквания и оценяване на съответствието на електрически съоръжения, предназначени за използване в определени граници на напрежението, изпълнявайки всички приложими изисквания на БДС EN 62368-1:2014 "Устройства/съоръжения за информационни технологии. Безопасност. Част 1: Общи изисквания" или еквивалентен.

2.8. Изисквания към срок на годност и жизнен цикъл

Заявените оборудване и материали трябва да имат дата на производство не по-стара от 01.10.2019 г.

3. Опаковане, транспортиране, временно складиране

3.1. Изисквания към доставката и опаковката

Заявените оборудване и материали трябва да бъдат доставени в складовете на „АЕЦ Козлодуй" ЕАД в оригиналната опаковка на производителя.

3.2. Условия за съхранение

Заявените оборудване и материали трябва да бъдат съхранявани при указаните от производителя параметри на околната среда.

4. Изисквания към производството

Няма отношение.

4.1. Правилници, стандарти, нормативни документи за производство и изпитване

Няма отношение.

4.2. Тестване на продуктите и материалите по време на производство

Няма отношение.

4.3. Контрол от страна на „АЕЦ Козлодуй" ЕАД по време на производството

Няма отношение.

5. Входящ контрол, монтаж и въвеждане в експлоатация

Въвеждането в експлоатация на устройствата ще се осъществи, съгласно одобрена програма от възложителя и изпълнителя съобразено с установения ред в "АЕЦ Козлодуй" ЕАД.

Изпълнителят се задължава да предостави кратко Ръководство на администратор за администратиране на въведените в експлоатация устройства.

5.1. Тестване на продуктите и материалите при входящ контрол при приемане на доставката, след монтаж и по време на експлоатация.

При доставката на оборудването се проверява съответствието му със заявените параметри по спецификацията от договора за доставка. Общият входящ контрол се извършва, съгласно „Инструкция по качество за провеждане на входящ контрол на доставените суровини, материали и комплектуващи изделия в АЕЦ "Козлодуй"", Ид.№ ДОД.КД.ИК.112.

5.2. Отговорности по време на пуск

Няма отношение.

5.3. Мерки за безопасност против замърсяване с радиоактивни вещества и опасни продукти

Няма отношение.

5.4. Здравни и хигиенни изисквания

Няма отношение.

5.5. Условия за демонтаж, монтаж и частичен монтаж

Няма отношение.

5.6. Условия на състоянията на повърхностите

Няма отношение.

5.7. Полагане на покрития

Няма отношение.

5.8. Условия за безопасност.

Няма отношение.

5.9. Документи, които се изискват при доставка, монтаж и въвеждане в експлоатация

Заедно със специфицираните изделия е необходимо е да се доставят:

- Декларация за произход;
- Спецификация на доставеното оборудване и софтуер;
- Пълен комплект документация за доставения софтуер и хардуер (приема се и в електронен вид);
- Лицензи, абонаментна поддръжка /subscriptions/ на името на "АЕЦ Козлодуй" ЕАД, вкл. и хартиено копие (приема се и разпечатка от интернет сайт) за срок от 3 години, съгласно техническата спецификация (Приложение 1) към техническото задание.

6. Гаранции, гаранционно обслужване и следгаранционно обслужване

6.1. Услуги след продажбата

След доставката на оборудването, съгласно спецификацията (Приложение 1) към техническото задание, изпълнителят се задължава за следното:
- да направи първоначална инсталация и конфигурация на устройствата, съгласувано с изискванията на възложителя;
- да подсигури обучение на най-малко двама /2/ служители на възложителя в сертифициран център (или еквивалентен такъв, като се допуска и виртуална сертификационна среда на обучение) за обучение на български език от сертифициран от производителя преподавател.
- да предостави кратко "Ръководство на администратор", съдържащо направените конфигурации на устройствата и начина за администриране на същите.

6.2. Гаранционно обслужване

Минимум 3 години оригинална (от производителя) гаранция. Допълнителна гаранция (хардуерна и софтуерна) с време за отстраняване на повреда на следващия работен ден след заявяването – според приложена техническа спецификация (Приложение 1).

7. Изисквания за осигуряване на качеството

7.1. Система за управление (СУ) на Изпълнителя

Изпълнителят трябва да прилага сертифицирана система за управление на качеството в съответствие с БДС EN ISO 9001:2015 или еквивалентен, с обхват покриващ дейностите по настоящото ТЗ, за което да представи копие на валиден сертификат.

7.2. Програма за осигуряване на качеството (ПОК)

Няма отношение.

7.3. План за контрол на качеството (ПКК)

Няма отношение.

7.4. Одит от страна на „АЕЦ Козлодуй" ЕАД (одит от втора страна)

Няма отношение.

7.5. Управление на несъответствията

Няма отношение.

7.6. Специфични изисквания по осигуряване на качеството

Изпълнителят трябва да е оторизиран от производителя на оборудването за продажба и сервиз на предложеното оборудване, съгласно Приложение 1.

7.7. Обучение и квалификация на персонала на „АЕЦ Козлодуй" ЕАД

7.7.1 Изпълнителят се задължава да подсигури обучение на най-малко двама /2/ служители на възложителя в сертифициран център (или еквивалентен такъв, като се допуска и виртуална сертификационна среда на обучение) за обучение на български език от сертифициран от производителя преподавател.

7.7.2 Изпълнителят се задължава да предостви сертификат за инженер по мрежова сигурност, издаден от производителя на предлаганото оборудване или от упълномощен от него представител.

7.7.3 Изпълнителят се задължава да предостви сертификат за инструктор по мрежова сигурност, издаден от производителя на предлаганото оборудване или от упълномощен от него представител.

7.7.4 Изпълнителят се задължава да издаде сертификат на завършилите успешно курса.

7.8. Приемане на доставката

Доставката подлежи на входящ контрол, съгласно изискванията на Инструкция по качеството за провеждане на входящ контрол на доставените суровини, материали и комплектуващи изделия в "АЕЦ Козлодуй" ЕАД, ДОД.КД.ИК.112. Доставката се приема след успешно преминат входящ контрол и издаден Протокол за входящ контрол без забележки.

7.9. Спазване на реда в „ АЕЦ Козлодуй" ЕАД

Няма отношение.

8. Изисквания към Изпълнителя при използване на подизпълнители/трети лица

При използване на подизпълнители/трети лица, основният Изпълнител по договора:

- носи отговорност за изпълнението на изискванията на ТЗ от подизпълнителите /трети лица за изпълняваните от тях дейности, както и за качеството на тяхната работа;
- определя линиите за комуникация и взаимодействие с неговите подизпълнители/трети лица и начините на контрол върху дейностите, които са им превъзложени и отговорните лица за изпълнение на този контрол;
- определя по подходящ начин и в необходимата степен приложимите изисквания на ТЗ за подизпълнители/трети лица по договора, в зависимост от дейностите, които изпълняват;
- включва в документацията на договора с подизпълнители/трети лица, всички определени по-горе изисквания.

ПРИЛОЖЕНИЯ:

ПРИЛОЖЕНИЕ 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

към Техническо задание 20.П.ТЗ.148 за „Доставка и въвеждане в експлоатация на устройства, повишаващи надеждността и защитата на Интернет свързаността на дружеството“, отговарящи на съвременните условия за защита и киберсигурност със следните минимални изисквания:

Брой на устройства в клъстер конфигурация		2 (два) броя
1.	**Минимални технически параметри**	**Минимална стойност**
1.1	Минимална пропускателна способност с активирана функция за идентификация на приложенията	18 Gbps
1.2	Минимална пропускателна способност с активирани функционалности за IPS/AntiVirus/ AntiMalware защита, URL филтриране и идентификация на файлове и чувствително съдържание в трафика	8.8 Gbps
1.3	Минимален брой TCP сесии	3 800 000
1.4	Минимален брой нови сесии в секунда	132 000
1.5	Минимален брой на разпознати и поддържани приложения	3 183
1.6	Минимален брой интерфейси	Да разполага 4 x 1000 / 10000 Base-T ports Възможност за надграждане допълнителни минимум 16 x 10Gbit/s SFP+ 4 x 40Gbit/s QSFP
1.7	Режими на интерфейсите	L2, L3, Tap, Transparent mode
1.8	Маршрутизиращи функции	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD)
1.9	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
1.10	Минимален брой конкурентни SSL VPN потребителя включени в системата	10 000 SSL VPN потребителя
1.11	Минимален брой IPSec Site-to-Site VPN	3000 отдалечени точки
1.12	Устройството да поддържа виртуални контексти	мин. 10 броя
1.13	Устройството да поддържа виртуални таблици за маршрутизация минимум	20 броя
1.14	Минимален брой поддържани VLAN	4,094 броя IEEE 802.1q VLAN маркера (tags), конфигурируеми за всеки интерфейс и общо за устройството
1.15	IPv6 поддръжка	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
1.16	Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL
1.17	Управление на канала	Управлението на канала (QoS) следва да е налично и приложимо за всяко идентифицирано приложение
1.18	Управление на устройството	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
1.19	Режим на надеждност	Active/Active, Active/Passive
1.20	Минимален брой интерфейси за управление	1 x 10/100/1000 out-of-band management port 1 x 40 Gbit/s интерфейси за отказоустойчивост 1 x RJ-45 конзолен порт
1.21	Монтаж и размери	Предназначена за вграждане в 19“ шкаф с максимален размер 3U
1.22	Захранване и входно напрежение (Входяща честота)	Резервирано, 100-240VAC (50-60Hz)
1.23	Софтуерна и хардуерна гаранционна поддръжка 365x24x7	Мин. 36 месеца. Изпълнителя следва да предостави всички необходими лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер.