



РЕПУБЛИКА БЪЛГАРИЯ
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

ДО
ВСИЧКИ ЗАИНТЕРЕСОВАНИ ЛИЦА

| |
|--|
| ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“ София 1000, ул. „Гурко“ № 6 |
| Рег. № <u>ДАЕУ - 3576</u> |
| Дата: <u>11.08.17г.</u> |

Относно: Представяне на индикативни ценови предложения за определяне на прогнозната стойност на обществена поръчка с предмет: „Надграждане на портала за мрежова и информационна сигурност на националния център за реакция при инциденти във връзка с информационната сигурност с допълнителни функционалности“ чрез провеждане на пазарна консултация по смисъла на чл. 44, ал. 1 от Закона за обществените поръчки.

УВАЖАЕМИ ДАМИ И ГОСПОДА,

На основание чл. 44 ал. 1 от Закона за обществените поръчки във връзка с подготовката за възлагане на обществена поръчка с предмет: „Надграждане на портала за мрежова и информационна сигурност на националния център за реакция при инциденти във връзка с информационната сигурност с допълнителни функционалности“ и изчисляването на прогнозната ѝ стойност Държавна агенция „Електронно управление“ (ДАЕУ) кани всички заинтересовани лица, които извършват посочените в настоящото писмо дейности, да представят индикативно ценово предложение.

Индикативното ценово предложение се представя съгласно приложенията към настоящата покана - Приложение № 1 и в таблична форма - Приложение № 1.1, и следва да съдържа: прогнозна стойност без ДДС и прогнозна стойност с ДДС. В стойността следва да бъдат включени всички разходи, свързани с изпълнението на поръчката, в съответствие с изискванията и условията на възложителя.

Индикативното ценово предложение се изпраща по един от следните начини:

- по електронен път – на e-mail: mnanovska@e-gov.bg до Миряна Нановска, старши експерт в Дирекция „Обществени поръчки“; сл. тел. 02/ 949 2433; или
- на адрес: гр. София 1000, ул. Ген. Й.В. Гурко № 6, в деловодството на Държавна агенция „Електронно управление“, всеки работен ден от 9:00 ч. до 17:30 ч. За час на получаване се приема часът, отбелязан при издаване на входящ номер.

Краен срок за подаване на индикативно ценово предложение: 21.08.2017 г. 17:30 ч.

Участниците в пазарната консултация могат да отправят запитвания относно пазарната консултация на електронна поща: bradeva@e-gov.bg до Бисерка Радева - началник на отдел CERT в срок до 17.08.2017 г. Разясненията по всички запитвания ще бъдат качени на профила на купувача в сайта на ДАЕУ - <https://e-gov.bg/bg/90> в рамките на 1 (един) работен ден след получаване на отправеното запитване.

Индикативните ценови предложения и всякаква друга информация, предоставена като резултат от пазарната консултация, ще бъдат публикувани на профила на купувача в интернет страницата на Държавна агенция „Електронно управление“ - <https://e-gov.bg/bg/90> съгласно принципите за защита на конкуренцията, недискриминация, публичност и прозрачност, заложили в ЗОП, както и принципът за равнопоставеност на потенциалните участници в предстояща процедура за възлагане на обществена поръчка.

С подаване на индикативно ценово предложение, всеки от участниците в пазарната консултация се съгласява, че предложението, както и всякаква друга информация, предоставена от участника като резултат от пазарната консултация, ще бъдат публично достъпни в интернет страницата на ДАЕУ, с оглед спазването на изброените принципи и изисквания на българското законодателство.

Важно! В случай че не може да се осигури спазване на принципа за равнопоставеност, независимо от съблюдаването на изискванията на чл. 44, ал. 3 от Закона за обществените поръчки, кандидатът или участникът, участвал в пазарната консултация, се отстранява от процедурата, ако не може да докаже, че участието му не води до нарушаване на този принцип (чл. 54, ал.1 т. 5 ЗОП). Преценката за необходимостта от отстраняване от участие е на възложителя, но тежестта на доказване спазването на принципите на ЗОП, е на кандидатите и участниците в обществената поръчка.

Поканата за представяне на индикативни ценови предложения не представлява покана за участие в процедура за възлагане на обществена поръчка по смисъла на Закона за обществените поръчки. Пазарната консултация се извършва с цел определяне на прогнозната стойност на обществена поръчка на етап подготовка на процедурата и представлява елемент от предварителните действия на възложителя при подготовката и изготвянето на документацията по процедурата за възлагане на обществена поръчка. Провеждането на пазарна консултация осигурява спазването на принципите за публичност и прозрачност при този процес и формирането на прогнозните стойности на обществените поръчки.

ИЗИСКВАНИЯ И УСЛОВИЯ ЗА ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ

Важно функционално звено от Държавна агенция „Електронно управление“ (ДА ЕУ) е Център за реакция при инциденти във връзка с информационната сигурност (CERT Bulgaria), който има национален статут.

Голяма част от задачите си CERT Bulgaria изпълнява чрез портала за мрежова и информационна сигурност govcert.bg.

Достъпността и правилното функциониране на портала са един от основните критерии за ефективното функциониране на CERT Bulgaria, а също така е и едно от основните изисквания на Trusted Introducer – международна организация, която е акредитирана за сертифициране на Национални CERTs.

Обновяване на информационната система, с която работи CERT Bulgaria, е направено при изпълнение на проект „Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство“ с рег. № K11-32-1/20.09.2011г., осъществен с финансовата подкрепа на Оперативна програма „Административен капацитет“.

Порталът за мрежова и информационна сигурност на CERT Bulgaria (Портал за МИС) се състои от следните компоненти:

- Ядро (вътрешни модули) на системата – състои се от 7 модула;
- Административна информационна система и приложение за предоставяне на електронни административни услуги;
- Публичен портал на CERT Bulgaria.

Порталът за МИС използва следния базов софтуер и технология:

- Сървър за приложения – GlassFish Server
- База данни – MySQL
- Портален сървър – Liferay Portal,
- Език за програмиране – Java.

За постигане на пълнота и цялостност на единната информационно-комуникационна среда е необходимо да се разработят допълнителни функционалности и интеграционни компоненти, като за целта е допустимо Изпълнителят, при необходимост, да предложи и друг софтуер.

Индикативното ценово предложение трябва да съдържа прогнозната стойност за изпълнението на следните основни дейности:

1. Разработване на модул за обработване на постъпващи външни заявки и доклади

Процесът на обработка на сигналите за нарушение от и във българското интернет пространство започва с получаване на самия сигнал. Съществуват няколко комуникационни канала, по които сигналите за инциденти постъпват в CERTbg, като най-голям е дялът на постъпващите сигнали чрез електронната поща. Това е причината да се пристъпи към разработване на модул за автоматично обработване на постъпващи външни заявки и доклади, интегриран с вътрешните модули на системата.

Модулът ще подпомогне обслужването на пристигащите по e-mail заявки чрез въвеждане на автоматизиран подход за създаване на инцидент (e-mail към инцидент). Автоматизирането на процеса (Внедряването на модула) трябва да се направи така, че в мейл сървъра да остане следа за всички получени и изпратени мейли през портала. Агенцията използва Microsoft Exchange server 2016.

Функционирането на тикет системата (модула за обработка на външни заявки) трябва напълно да отговаря на утвърдената процедура за обработка на инциденти в Дирекция МИС.

2. Добавяне на нови функционалности и доработка на съществуващи в модул „Инциденти“

2.1. Разработване на типови шаблони за инциденти в модул „Инциденти“

Да се разработи нова функционалност „шаблон за типови инциденти“, чрез която автоматично се попълват данни в съответствие с разработения шаблон за съответния тип инцидент.

2.2. Автоматична обработка едновременно на множество IP адреси на засегнати системи

Към модул „Инциденти“ трябва да се добави нова функционалност за автоматична обработка на IP адреси на засегнати системи:

- Импорт на списък с IP адреси на засегнати системи от файл със структурирана информация при обработка на инциденти.
- Автоматична проверка за обхвата на въведените IP адреси на засегнатите системи – в адресите на конституентите на CERT България и на интернет доставчиците чрез съпоставяне на данните, налични в портала и тези, фигуриращи в база данните за ISP-тата в RIPE.
- Автоматично въвеждане на данните на засегнатите страни, установени от проверката по т.2 – наименование на засегната страна, засегнати IP адреси, e-mail и др. полезна информация.
- Възможност за изпращане на автоматични уведомления по електронна поща до участниците по предварително зададен шаблон с обобщени данни за всички IP адреси участващи в конкретния инцидент от неговата мрежа.
- Възможност за едновременно прикачване на множество файлове при изпращане на уведомление.
- Регистриране на всички изпратени в хронологията на инцидента.
- Изпратените уведомления трябва да оставят копие/следа в мейл сървъра на ДА ЕУ.
- Промяна на формата на въвеждане на данните в поле „IP адрес“.
- Трябва да се разшири функцията за търсене по IP адрес посредством обединяване на резултати от различни масиви с информация.
- Разработване на функционалност за проверка и подходяща обработка (създаване на нов инцидент или добавяне на последващ доклад към регистриран такъв) въз основа на повтаремостта на постъпилите сигнали за докладваните IP адреси.

2.3. Модифициране на „Хронология“

В модул „Инциденти“, в раздел „Хронология“ се отбелязват всички извършени операции от отговорника, обработващ инцидента, както и да се записват действията по разрешаването му. Необходимо е да се разграничат действията по обработка на инцидента от хронологичните операции в системата, като по този начин се гарантира логичната последователност на процесите и хронологична подредба на регистрираните събития.

2.4. Модифициране на информацията в някои от екраните / отделните менюта

- Извеждане на информация за засегнатите IP адреси в меню „Инциденти“
- Извеждане на данни за засегнатата страна в модул „Инциденти“
- Извеждане на информация за засегнати IP адреси в модул „Инциденти“
- Възможност за избор на участници (един, повече, всички) при изпращане на автоматични уведомления в модул „Инциденти“, секция „Участници“.
- Въвеждане на промени по отношение на извеждане на данни за e-mail адрес на участниците в модул „Инциденти“, секция „Участници“

- Указване на IP адреса (един или повече), засегнат от свързания инцидент - модул „Инциденти“, секция „Свързани инциденти“

2.5. Оптимизация на форми, редизайн

С оглед оптимизиране на работата по обработка на инцидента в портала, в модул „Инциденти“:

- Необходимо да се промени статута на някои от задължителните полета за попълване.
- Да се предвиди възможност за автоматично попълване на данни (в една или повече форми) в случай на констатирана необходимост в процеса на бизнес анализ.
- Въвеждане на промени по отношение на подредбата на елементите в модални прозорци (един или повече) с цел оптимизация на „полезното“ пространство, извеждане на допълнителни бутони за основни действия – запис, отказ.
- Необходимо от реструктуриране на секция „Хронология“ в модул „Инциденти“ с оглед интегриране на тикет системата.
- Оптимизация на други форми, включително редизайн по искане на Възложителят и при констатирана необходимост в етап Бизнес анализ и проектиране.

3. Реструктуриране на интерфейса за навигация на уязвимости в портала, модул „Уязвимости“

3.1. Разработване на процедури

В модул „Уязвимости“ на портала за МИС автоматично се навигат уязвимостите, ползвайки като източник National Vulnerability Database (NVD) на САЩ. В този модул се осъществява и връзката между уязвимостите и базата данни със софтуера и хардуера, използван от конституентите, което позволява на потребителите да виждат, както всички налични уязвимости, така и само тези, които се отнасят конкретно за тяхната инсталационна база. При промяна структурата на информацията подавана от NVD се налага корекция на схемата на съпоставяне с полетата от базата в портала, затова е необходимо системата да е гъвкава и адаптивна при промени на входните данни. За целта трябва да се разработят процедури за:

- събиране на информацията за уязвимостите в базата;
- съпоставянето на уязвимостта с инсталационната база данни на конституентите.

Трябва да бъде обучен екипът на CERT BG да прилага съответните процедури.

Трябва да се осъществи връзка с мейл сървъра, за предоставяне на ЕАУ и автоматично известяване по e-mail (до отговорниците по МИС) през системата за новорегистрирани уязвимости (Винаги трябва да остава следа в пощенската кутия за изпратените писма).

3.2. Адаптиране към обновената структура на данните в CVE списъците (Common Vulnerabilities and Exposures List)

В рамките на обхвата на поръчката, Изпълнителят следва да извърши необходимите корекции в схемата на съответствие между полетата от базата в портала и данните, съдържащи се в актуализираните CVE списъци, като по този начин осигури възможност за периодично обновяване на CVE списъка.

4. Доразвиване на функционалността за изпращане на информационни бюлетини

Изпращането на информационни бюлетини за новооткрити уязвимости е една от четирите ЕАУ, които CERT България предоставя на своите конституенти. В сегашната си реализация се изпраща e-мейл с информация за новоизлезлите уязвимости, отговарящи на използвания софтуер и хардуер от конституентите, само ако се е абониран. Да се предвиди активиране по подразбиране за всички регистрирани конституенти, а ЕАУ да е за отказ от абонамент. На потребител с роля Администратор на системата да се даде право на редакция на тази функционалност.

5. Доразвиване на функционалността „Сортиране по колони“

Необходимо е да бъде доразвита функционалността за сортиране на всички колони във всички модули.

6. Оптимизиране на формата за докладване на инциденти

Необходимо да се преработят полетата във формата за докладване на инциденти до гарантиране на пълно съответствие с полетата в системата. След изпращане на успешно попълнена форма за докладване, въведената от потребителя информация следва автоматично да се попълва в системата.

Необходимо е да се надгради функционалността чрез:

- извеждане на уведомително съобщение за потвърждение на успешно реализирана операция или указване на причините за грешка, в случай че е констатирана такава;
- в пощенската кутия cert@govcert.bg да се получи известие за постъпил сигнал в портала.

7. Осигуряване на връзка с Автоматизираната информационна система(АИС) за инвентаризация на информационни и комуникационни инфраструктурни (ИКИ) ресурси.

АИС за инвентаризация на ИКИ ресурсите ще бъде внедрена по проект: „Инвентаризация на информационно-комуникационната инфраструктура за нуждите на електронното управление“, финансиран от Оперативна програма „Добро управление“ с конкретен бенефициент Държавна агенция „Електронно управление“.

Интеграцията на данните с данните от АИС за инвентаризацията ще даде възможност на нашите конституенти да получават актуална информация за уязвимостите в техните информационни активи, защото първоначалната информация в базата е събирана през 2013 г. Осъществявайки основната идея на електронното управление, а именно веднъж въведени данни да се използват многократно, е необходимо да се осъществи връзка между портала за МИС и проекта за инвентаризация на информационните активи в държавната администрация.

Зареждането на данни (upload) ще се осъществява посредством WEB сервиз и SOAP XML протокол. Изпълнителят на обществена поръчка следва да подготви необходимия вход към портала, съответстващ на залегналите в анализа изисквания за осъществяване на обмен на данни между двете системи. Допълнително ще бъде уточнена динамиката на извършваните промени и нуждата от периодична актуализация, както и интервалите на нейното обновяване.

8. Подобряване на бързодействието на системата

В Етап 1: Анализ и проектиране Изпълнителят трябва да проведе необходимите тестове за натоварване на система, да анализира получените резултати и да направи съответните препоръки за подобряване на бързодействието. След реализиране на новите функционални изисквания, преди окончателното им внедряване, процедурата трябва да се повтори и да се гарантира минимално време за отговор на заявки, като средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките.

За тестовите, проведени с участието на CERT BG, да бъдат подписани констативни протоколи.

9. Справочна система - Разработка на генератор на справки и отчети

Изпълнителят на поръчката трябва да внедри, работещо решение за генериране на справки и отчети. Справочният модул трябва да предостави интерфейс на потребителите за задаване на критерии и представяне на резултатите от изпълнението на конкретни справки.

9.1. Справочната система трябва разполага със следната функционалност:

- Задаване на филтри по различни критерии преди извличане на резултатите;
- Задаване на начин на сортиране на резултатите;
- Представяне на резултатите от справка в табличен вид;
- Представяне на резултатите от справка във вид на диаграма;
- Комбинирани справки, включващи резултати в табличен вид и диаграми;
- Да се указват колоните, които да бъдат включени в справката и техните параметри;
- Възможност за отпечатване по предварително дефинирани образци;
- Справките трябва да могат да се експортират във файлове в стандартен формат. Справките трябва да могат да се визуализират по прегледен начин на екран, а също така да се съхраняват локално на компютър, минимум в следните формати:
 - ✓ Структурирана Excel – таблица за справките, чиито резултат представлява табличен списък с резултати за повече от един обект на индустриалната собственост;
 - ✓ PDF – документ
- Възможност за създаване на логическа връзка между различни таблици и изгледи;
- Възможност за съхраняване на предефинирани справки - филтри, колонии, сортиране, образец, вид диаграма и др. параметри.

9.2. Справочният модул трябва да включва като минимум следните работни места:

- Създаване и редакция на шаблони за отчети – минимум две работни места;
- Изпълнение и преглед на отчети – минимум пет работни места.

В случай, че предлаганото решение изисква използването на базов софтуер, то кандидатът трябва да достави необходимите лицензи."

9.3. Изготвяне на документация

Така създадените справки трябва да бъдат добре документирани и служителите на отдела, трябва да бъдат обучени как да променят тяхната дефиниция при необходимост, и/или да създават нови справки.

10. Обновяване дизайн на публичната част на портала за МИС www.govcert.bg

В публичната част на портала да има възможност за търсене по израз, дума и/или дата на публикуване в разделите „Предупреждения“, „Съвети“, „Новини“.

Ограничението в обема и формата на материалите, които са в публичната част на портала в разделите „Предупреждения“, „Съвети“, „Новини“ да може да се контролира. Да има гъвкавост при избор на език, на който ще се публикуват материалите в разделите „Предупреждения“, „Съвети“, „Новини“ и адекватна визуализация.

Кандидатите трябва да представят подходящ дизайн на уеб сайта, който трябва да бъде лесен за използване, интуитивен и лесен за възприемане.

11. Разработване на експлоатационна документация

Изпълнителят трябва да изготви и предаде следните кратки инструкции и процедури:

- Инструкция за инсталиране на SSL сертификат;
- Процедура за паливане на уязвимости;
- Обновяване на CVE версията, която се ползва при въвеждане на инсталационната база данни на конституентите;
- Процедура за съпоставяне на инсталационната база данни с уязвимостите;
- Инструкция за RSS – на вируси и уязвимости, реализирана на уеб сайта;
- Процедура за спиране и пускане на вътрешния модул и уеб сайта;
- Процедура за възстановяване на системата от архив;
- Процедура за архивиране на системата;
- Инструкции за прилагане на актуализации на всеки един от софтуерните компоненти, изграждащи портала;
- Процедура за обработка на множество IP адреса;
- и за всички разработени функционалности, които не са споменати в предишните точки.

В тестовият период, преди внедряване на новите функционалности в продукционна среда, трябва да бъдат проиграни всички гореспоменати процедури от персонала на CERT BG и за резултатите да се състави констативен протокол, подписан от двете страни.

12. Гаранционна поддръжка

Периодът на гаранционната поддръжка да бъде минимум една година след приемане на разработката и да се използва online система за регистриране и проследяване на заявката.

За целта да бъде разработена процедура за гаранционно обслужване, която да съдържа:

- Срок на гаранционната поддръжка
- Обхват на гаранционната поддръжка
- Организация на поддръжката
- Дейности по поддръжката
- Методология за извършване на поддръжката
- Система за проследяване и регистриране на инциденти

Гаранционното поддръжане започва да тече от деня на подписване на окончателния приемо-предавателен протокол.

Гаранционната поддръжка трябва да включва минимум следното:

- Отстраняване на всички установени от възложителя несъответствия при функционирането на модулите с изискванията на техническата спецификация;
- Несъответствия на експлоатационната документация и функционирането на модулите.

При възлагане на обществена поръчка с посоченият по-горе предмет максималният срок за изпълнение на дейностите ще бъде до 4 месеца, считано от датата на подписване на договор.

Всички авторски и сродни права върху продуктите, изготвени и създадени като резултат от изпълнението на поръчката, възникват за ДАЕУ в пълен обем, без ограничения в използването, изменението и разпространението им.

Приложения:

1. Индикативно ценово предложение (Приложение 1);
2. Индикативно ценово предложение в таблична форма (Приложение № 1.1).

С уважение, заличено на
основание чл. 233Д

Йовка Захариева Иванова
Директор на Дирекция „Обществени поръчки“
Държавна агенция „Електронно управление“,

Възложител съгласно Заповед № ДАЕУ-2012/15.05.2017 г.