Алианц България Холдинг АД

Съдържание на офертата и критерии за избор за провеждане на конкурс и избор на доставчик на услуга „Комплексна проверка за пробиви на информационната сигурност – Penetration Test" за нуждите на Алианц България Холдинг АД

I. Обща информация

1. Конкурса е за избор на доставчик на услуга за комплексно тестване на информационната сигурност за пробиви и извършване на симулирани кибер атаки към външни и вътрешни ресурси на Алианц България Холдинг. Тестовете ще се провеждат регулярно на годишна база за следващите 3 години.

II. Съдържание на Офертата

1. Кратко представяне на компанията и референтен лист.
2. Списък с изпълнени проекти от подобно естество.
3. Професионални профили на тестерите и предходен опит.
4. Условия за плащане.
5. Допълнителни параметри, услуги и срок на договора.
6. Попълнен въпросник по образец за кандидат за доставчик на услуги.
7. Попълнен Образец 1.
8. Попълнена декларация към фирмата съгласно приложен образец.
9. Ценова част, подлежаща на оценка съобразно приложената в раздел IV методика за оценяване на офертите, и съдържаща еднократни и/или пакетни цени за извършване на посочените в раздел III тестове на годишна база за следващите 3 години.
10. Всички документи по конкурсната процедура, следва да бъдат подписани от лица представляващи компанията по регистрация, или от лица писмено упълномощени по съответният ред за това, като пълномощното следва да бъде представено в пакета документи.

III. Изходни данни:

1. Black Box external penetration test
    a. Откриване и обследване сигурността на публично разположените ресурси на Алианц България Холдинг – уебсайтове, услуги и системи.
    b. Тестване за отворени портове и слабости в потребителските интерфейси и конфигурацията на системите за сигурност, за експлоатация на познати уязвимости с цел достигане до чувствителни данни.
    c. Обхвата на теста е на база предоставен IP range, без да се предоставят други допълнителни данни на тестерите.
2. White Box internal penetration test
    a. Извършване на комплексна проверка на сигурността и възможностите за пробив на защитите на бизнес апликации и инфраструктурни ИТ компоненти, разположени във вътрешната мрежа на компанията.
    b. На тестерите ще бъде предоставен VPN достъп до определени сегменти от корпоративната мрежа, съдържащи системи и компоненти на бизнес апликациите в обхвата на теста. В допълнение ще бъде предоставена базова информация като IP адресите на сървърите и използваните технологии (OS, Application, DB system).

c. В ограничени случаи ще бъдат предоставени и потребителски данни за вход в бизнес апликация, за да се тества сценарии със опит на злонамерен служител/външен доставчик да достъпи неоторизирано данни извън предоставеното ниво на привилегии.
d. Тестване за проникване/неоторизиран достъп до активна директория без предоставени специфични данни за достъп.
e. Предвижда се тестване на до 20 бизнес апликации и 2 активни директории на годишна база, разпределени в 2 отделени ИТ среди.
f. Крайните резултати от тестовете трябва да се предоставят в 2 отделни доклада (спрямо ИТ средата) със следните изисквани за минимално съдържание:
    i. Списък с откритите уязвимости:
    ID: unique identifier for that finding.
    Description: description of the finding and details of how it could affect the system, and which components are impacted.
    Location: where the finding is located (IP address/hostname/path).
    CVSS Score: the score shows the severity of the finding (from 0.0 to 10.0), based on the Common Vulnerability Scoring system (CVSS v3 recommended).
    CVSS rating: CVSS rating shows the qualitative rating of the CVSS Score:

Rating	Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

    Reproduction: guidelines for reproducing the results of the finding.
    Recommendation: provide recommended mitigation measures to close or limit the identified finding.
    Category: identify the vulnerability category of the finding to support further mapping to threat events.
    ii. В допълнение доклада трябва да съдържа обобщение на резултата от проведените тестове (executive summary), детайлна информация за използваната методология за тестване, както и екранни снимки доказващи откритите уязвимости.

3. Retest
    a. Извършване на последващо тестване на откритите уязвимости, с цел валидиране на направените промени или въведените допълнителни защитни мерки за затваряне на дупките в сигурността на приложенията.

IV. Методика за оценяване на офертите

1. На оценка подлежат офертите, отговарящи на изискванията на конкурса и комплектовани с всички изискани документи съгласно раздел II.
2. Класирането на офертите ще се извърши съгласно условията и коефициентите за тежест, в комплексна оценка (КО), формирана по следната формула:
3. **КО = Tb** x **0,2** + **Tw** x **0,5** + **Te** x **0,1** + **Tq** x **0,2** където:

Показател - П (наименование)	Тежест (коефициент)	Максимален брой точки	Символно обозначение (точките по показателя)
П1 - цена за Black Box test + retest	20% (0,20)	20	Tb
П2 - цена за White Box test + retest	50% (0,50)	20	Tw
П3 - опит на компанията	10% (0,10)	20	Te
П4 - компетенции на екипа	20% (0,20)	20	Tq

П1 – Максималният брой точки умножен по съотношението на предложената от участника цена на услугата Black Box external penetration test/retest, спрямо най-ниската такава в конкурса.
П2 – Максималният брой точки умножен по съотношението на предложената от участника цена на услугата White Box internal penetration test/retest, спрямо най-ниската такава в конкурса.
П3 – Броят точки се определя спрямо годините опит в предоставяне на подобни услуги (0-10т.) и портфолиото от изпълнени проекти на компанията (0-10т.).
П4 – Броят точки се определя от годините опит (0-12т.) и притежанието на международно признати сертификати (0-8т.) свързани с Penetration Testing на екипа осъществяващ проверките.

4. На първо място се класира офертата, събрала най-много точки съгласно показателите на комплексната оценка КО.

С уважение,
Дирекция „Информационна Сигурност“