ТЕНДЕРНОЕ ЗАДАНИЕ

На работы по тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры в рамках требования 382-П

1. ПРЕДМЕТ КОНКУРСА:

1.1. Работы по тестированию на проникновение и анализу уязвимостей информационной безопасности объектов информационной инфраструктуры в рамках требования 382-П.

1.2. Целью работ является независимое обследование, позволяющее оценить текущее состояние информационной безопасности корпоративной информационной системы (далее – КИС) АО КБ «ЮНИСТРИМ» (далее -Заказчика), выявить существующие уязвимости, оценить угрозы, спланировать дальнейшие шаги по их минимизации и выработать рекомендации по повышению уровня защищенности.

1.3. Выполняемые работы реализуют требования Положения Банка России от 9 июня 2012 г. № 382-П в части ежегодного тестирования на проникновение и анализа уязвимостей.

1.4. Задачи, решаемые в ходе выполнения работ:

- проведение внешнего теста на проникновение в КИС;
- проведение внутреннего теста на проникновение в КИС;
- тестирование на проникновение через беспроводные сети и анализ их защищённости;
- разработка перечня рекомендаций и предложений по повышению уровня обеспечения ИБ, совершенствованию технических и организационных мер.

2. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ

2.1. Исполнитель работ должен обладать большим практическим опытом выполнения проектов по проведению аудитов ИБ.

2.2. Профильной деятельностью Исполнителя должно являться оказание услуг по оценке уровня защищенности и тестированию на проникновение.

2.3. Исполнитель должен иметь:

- опыт проведения работ по тестированию на проникновение не менее 3 лет;
- опыт проведения работ для организаций с разветвленной инфраструктурой и количеством АРМ и серверов, превышающим тысячи единиц;

2.4. Исполнитель должен по запросу предоставить на рассмотрение Заказчику:

- данные о квалификации и опыте работ, соответствующие описанным выше требованиям;
- отзывы клиентов о проведении работ по анализу защищенности (не менее 3);
- примеры отчетов по результатам работ по анализу защищенности;
- резюме предполагаемых участников проектной команды;
- описание подходов к контролю качества проделанных работ.

2.5. Наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

2.6. Исполнителю запрещается передавать работы на субподряд.

3. Описание границ оказания услуг ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ

3.1. Услуги оказываются Исполнителем в г. Москва в рабочее время.

3.2. В ходе выполнения работ рассмотрению подлежат:

- доступные из сети Интернет компоненты КИС Заказчика (включая веб-сайты);
- хосты, находящиеся в локальной вычислительной сети Заказчика;
- компоненты беспроводных сетей Заказчика.

3.3. Исполнитель использует для оказания услуг фиксированные IP-адреса, которые он предоставляет Заказчику до начала проекта.

4. Требования к составу и содержанию услуг

4.1. В рамках оказания услуг Исполнителем проводятся:

- согласование с Заказчиком деталей процесса тестирования на проникновение;
- согласование модели имитируемого злоумышленника;
- согласование сроков выполнения всех этапов проекта;
- согласование узлов КИС, входящих в область проекта;
- согласование контактных лиц Заказчика и порядка взаимодействия с ними.

4.2. Внешний тест на проникновение в КИС

При проведении теста на проникновение в КИС Заказчика из сети Интернет Исполнитель выполняет:

- поиск общедоступной информации о Заказчике с помощью поисковых систем, сбор и анализ информации, полученной через регистрационные базы данных;
- сбор информации о ресурсах КИС Заказчика, доступных из сети Интернет (доступные сетевые сервисы их версии и версии операционных системах, на которых установлены данные сервисы);
- выявление уязвимостей на ресурсах компании, способных привести к нарушению конфиденциальности, целостности или доступности данных ресурсов;
- выявление уязвимостей веб-приложений, включая оценку по OWASP Top 10;
- разработку векторов атак на основе анализа данных, полученных в результате выполнения предыдущих этапов;
- согласование и реализация выбранных векторов атак;

4.3. Внутренний тест на проникновение в КИС

При проведении теста на проникновение в КИС Заказчика из локальной сети Исполнитель выполняет:

- пассивный и активный сбор информации в локальной сети Заказчика;
- анализ сегментации локальной сети в КИС Заказчика;
- поиск уязвимостей в КИС Заказчика посредством автоматизированного и ручного анализа и их валидация;
- попытки получения несанкционированного доступа к серверам, базам данных, компьютерам пользователей с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей;
- разработка векторов атак на основе анализа данных, полученных в результате выполнения предыдущих этапов.

4.4. Оценка защищенности беспроводных сетей

Для оценки защищенности беспроводных сетей Исполнитель проводит работы по выявлению недостатков в использовании точек доступа и клиентских устройств Wi-Fi (для диапазонов 2,4 и 5 ГГц с использованием технологий 802.11a/b/g/n/ac), позволяющих нарушителю реализовывать следующие угрозы:

- несанкционированное подключение к беспроводным сетям Банка;
- перехват информации, передаваемой по беспроводным сетям Банка;

- организация атак на клиентские беспроводные устройства Банка путем навязывания подключения к точке беспроводного доступа нарушителя.

Используемые в ходе оценки защищенности беспроводных сетей инструменты и методики должны обеспечивать:

- обнаружение точек беспроводного доступа, подключенных к ЛВС Банка;
- проверка настроек точек беспроводного доступа на предмет несоответствия рекомендациям производителей и исследователей в области ИБ (использование нестойких алгоритмов шифрования, отсутствие механизмов защиты и т.п.);
- обнаружение ошибок в конфигурации клиентских устройств беспроводных сетей.

4.5. Разработка отчетной документации

По результатам исполнения п.п. 4.2 – 4.4 Исполнитель разрабатывает отчетную документацию. Требования к отчетной документации указаны в п. 5 данного Технического Задания.

5. ТРЕБОВАНИЯ К ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

5.1. По итогам оказания услуг Исполнителем должен быть разработан документ «Отчет по результатам тестирования на проникновение в корпоративные информационные системы Заказчика», содержащий:

- краткую информацию об объекте тестирования;
- описание используемой методики тестирования и применяемой модели нарушителя;
- перечень использованного в процессе работ ПО;
- обобщенные результаты теста на проникновение, резюме для руководства;
- описание всех выявленных уязвимостей, их степеней риска, ограничений по их эксплуатации, а также рекомендации по их устранению;
- подробное описание векторов реализованных атак;

5.2. Разработка отчета выполняется на русском языке.

5.3. Отчет предоставляются Заказчику, как в бумажной форме, так и в электронной форме в формате *.doc(x).

6. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

6.1. Исполнитель после анализа внешнего периметра, должен согласовать перечень целевых ip-адресов с Заказчиком.

6.2. До начала проведения работ по проведению тестов на проникновение Заказчик предоставляет перечень электронных адресов, адресов компьютеров или фамилий, которые не могут быть затронуты при выполнении работ.

6.3. Использование атак типа “человек посередине” (Man in the middle) и других типов атак, которые могут привести к нарушению штатного функционирования КИС, предварительно согласовывается с Заказчиком.

6.4. Работы этапа «Оценка защищенности беспроводных сетей» выполняются на одной площадке Заказчика в Москве.

6.5. Тестирование защищенности веб-приложений в области оценки осуществляется методом «черного ящика», без использования учетных записей для данных веб-приложений.

6.6. По предварительному согласованию с Заказчиком могут быть проведены дополнительные мероприятия по тестированию на проникновение и анализу защищенности, не указанные в техническом задании.

6.7. Исполнитель должен предпринимать все разумные меры предосторожности, чтобы не нарушить нормальное функционирование КИС Банка. Исполнитель не должен предпринимать атаки типа “Отказ в обслуживании” (DoS) или “Распределенный отказ в обслуживании” (DDoS).

7. ПЛАНОВАЯ ДЛИТЕЛЬНОСТЬ АУДИТА

7.1. Плановая длительность аудита 30 рабочих дней;

8. СТОИМОСТЬ

8.1. Стоимость, руб., включая НДС – до 1 000 000 руб. В стоимость предложения должны быть включены все расходы, в том числе расходы на страхование, уплату налогов, сборов и иных обязательных платежей. **Желательна 100%** оплата предоставленных услуг после (по факту) выполнения всех работ, предусмотренных договором.

9. Компании-участники должны предоставить по запросу следующие документы:

- Устава.
- Учредительного договора.
- Выписки из реестра акционеров (для акционерных обществ).
- Свидетельства о государственной регистрации юридического лица.
- Свидетельства о постановке на учет в налоговом органе юридического лица.
- Свидетельства о внесении в реестр юридических лиц.
- Приказа о вступлении в должность руководителя юридического лица.
- Приказа о назначении главного бухгалтера.
- Информационного письма об учете в Статрегистре Росстата (коды статистики).
- Лицензий.
- Бухгалтерского баланса и ОПУ (формы № 2) на последнюю отчётную дату и дату предшествующую ей.
- Сведения об отсутствии невыполненных обязательств перед государственными внебюджетными фондами РФ и бюджетами всех уровней.
- Сведения о не проведении в отношении участника конкурса процедуры банкротства.
- Всех страниц паспорта руководителя и/или лица, которое будет подписывать договор.
- Всех страниц паспорта главного бухгалтера.

10. Для получения разъяснений по вопросам, связанным с предметом тендера просьба отправлять запрос на адрес: tender@unistream.com