Технічне завдання

до тендеру

з вибору постачальника для надання послуг
зовнішньої оцінки захищеності інформаційних систем АТ«ОТП БАНК»

(тестування на проникнення)

Предмет закупівлі

Проведення зовнішньої оцінки захищеності інформаційних систем АТ«ОТП БАНК» (тестування на проникнення):

- Тестування зовнішнього периметру комп'ютерної мережі та веб-додатків на наявність вразливостей;
- Аналіз можливості використання знайдених вразливостей для проникнення в мережу банку;
- Збір інформації для проведення поглибленого тестування за допомогою методів «соціальної інженерії»[1].

За результатами тестування повинні бути розроблені Виконавцем та погоджені із Замовником наступні документи (українською та англійською мовами):

- Звіт за результатами тестування;
- Звіт за результатами збору інформації, яка була набута за допомогою методів соціальної інженерії;
- Рекомендації щодо усунення недоліків з не менше ніж двома (де це можливо) детальними пропозиціями по кожному недоліку;
- План усунення виявлених недоліків (Action Plan), який повинен включати експертну оцінку визначених в процесі сканування потенційно вразливих ділянок системи, а також рекомендацій щодо їх усунення.

1. Специфікація

На розгляд повинна бути представлена пропозиція на нижче вказані послуги (виходячи з принципу **«чорного ящика»***, тобто без отримання будь-якої інформації про наявність та конфігурації засобів захисту периметра інформаційної мережі та за принципом **«сірого ящика»****, тобто із використанням відомих даних про обліковий запис та пароль користувача).

№ п/п	Найменування послуги
1.1.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг сканування зовнішнього периметру мережі та веб-додатків з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.2.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг тестування корпоративного сегменту Wi-Fi з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.3.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг тестування USB-портів корпоративних робочих станцій із увімкненими та ввімкненими засобами захисту з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.4.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг тестування захищеності корпоративної електронної пошти (вкладені файли, посилання тощо) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.5.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг аналізу вразливостей мобільного додатку OTP SMART (платформи iOS, Android) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.6.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг аналізу програмного коду на предмет виявлення вразливостей, дотримання технологій та принципів безпечної розробки для веб-додатків OTP Online/Pay (iFOBS) та OTP SMART (iFOBS) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
1.7.	Надання послуг виходячи з принципу «чорного ящика»*: Надання послуг тестування CI / CD оточення з використанням інструментів статичного (SAST) і динамічного (DAST) тестування безпеки коду, що виконується.
2.1.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг сканування зовнішнього периметру мережі та веб-додатків з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
2.2.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг тестування корпоративного сегменту Wi-Fi з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.

[1] *Соціальна інженерія - це метод управління діями людини без використання технічних засобів. Метод заснований на використанні людського фактору.*

2.3.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг тестування USB-портів корпоративних робочих станцій із увімкненими та ввімкненими засобами захисту з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
2.4.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг тестування захищеності корпоративної електронної пошти (вкладені файли, посилання тощо) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
2.5.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг аналізу вразливостей мобільного додатку OTP SMART (платформи iOS, Android) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
2.6.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг аналізу програмного коду на предмет виявлення вразливостей, дотримання технологій та принципів безпечної розробки для веб-додатків OTP Online/Pay (iFOBS) та OTP SMART (iFOBS) з наданням детального звіту по виявлених недоліках та рекомендаціях щодо їх усунення.
2.7.	Надання послуг виходячи з принципу «сірого ящика»**: Надання послуг тестування CI / CD оточення з використанням інструментів статичного (SAST) і динамічного (DAST) тестування безпеки коду, що виконується.

2. Вимоги до технології тестування захищеності периметра інформаційної мережі

2.1. У результаті проведення проекту Учасник повинен:

- Провести оцінку можливості отримання несанкціонованого доступу та/або порушення нормального функціонування веб-додатків в процесі моделювання зовнішніх атак;
- Виявити максимальну кількість вразливостей в системі захисту мереж та веб-додатків;
- Зібрати якісні дані, які можуть бути використані в подальшому для проведення атак з метою проникнення за допомогою методів «соціальної інженерії».

2.2. Пропозиції повинні включати наступні етапи, визначені окремими методиками:

- Збір даних щодо корпоративної інформаційної системи з відкритих джерел;
- Збір даних щодо корпоративної мережі Wi-Fi;
- Інструментальний аналіз захищеності зовнішнього периметра корпоративної інформаційної системи та веб-додатків по діапазону зовнішніх IP-адрес, узгоджених з замовником;
- Пошук та аналіз вразливостей зовнішнього периметра корпоративної інформаційної системи та веб-додатків, не виявлених на етапі інструментального аналізу;
- Пошук та аналіз вразливостей ресурсів корпоративної інформаційної мережі, доступних через корпоративну мережу Wi-Fi;
- Використання методів «соціальної інженерії» для отримання привілейованих прав доступу до корпоративних систем та сервісів, а також до конфіденційної інформації про клієнтів і співробітників Банку;
- Аналіз CI / CD оточення з використанням інструментів статичного (SAST) і динамічного (DAST) тестування безпеки коду, що виконується;
- Моделювання атак на хости зовнішнього периметра корпоративної інформаційної системи, що включають в себе наступне:
  - Аналіз захищеності активного мережевого обладнання;
  - Аналіз захищеності служби DNS;
  - Аналіз захищеності служби HTTP;
  - Аналіз захищеності системи «ЦСК ІІТ», що використовується для клієнт-банк OTPay;
  - Аналіз захищеності сервера взаємодії;
  - Аналіз вразливостей у WEB-додатках та WEB-сервісах;
  - Аналіз захищеності системи електронної пошти;
  - Аналіз захищеності USB-портів робочих станцій;
  - Аналіз захищеності корпоративного сегменту Wi-Fi;
  - Аналіз захищеності DMZ;
  - Аналіз захищеності системи «BPM Online (Creatio)»;
  - Аналіз захищеності мобільного додатку BPM Online;
  - Аналіз захищеності учбового порталу MOCCO;

- Аналіз захищеності веб-сайту банка;
- Аналіз захищеності сервісу віддаленого доступу WEB RDP;
- Аналіз захищеності сервісу віддаленого доступу DirectAccess;
- Аналіз захищеності сервісу віддаленого доступу Checkpoint VPN Gate;
- Аналіз захищеності системи «Sibel»;
- Аналіз захищеності системи «OTPPay»;
- Аналіз захищеності системи «OTP SMART»;
- Аналіз захищеності мобільного додатку «OTP SMART»;
- Аналіз захищеності від DoS атак (на сервіси: веб-сайт, кліент-банк).

Всі етапи повинні виконуватися тільки після отримання відповідного дозволу на початок робіт від замовника. У тому випадку, якщо виконання певного виду тестування може призвести до виведення з ладу або деградації продуктивності того чи іншого сервісу інформаційної мережі, або у разі успішного отримання доступу до конфіденційної інформації замовника, виконання робіт повинно припинятися до отримання формального дозволу на продовження таких робіт з боку замовника.

3. Інформація про статус Замовника

- Кількість зовнішніх IP адрес для сканування – мережа класу С;
- Кількість зовнішніх IP адрес для валідації вразливостей – близько 50;
- Біля 100 філій та відділень;
- Обробка та збереження даних ІКС здійснюється централізовано.

4. Критерії оцінки: 70% - цінові (фінансові) показники; 30% - нецінові (кваліфікаційні) показники

4.1. Перелік нецінових (кваліфікаційних) критеріїв:

- Умови оплати – 100% постоплата (по факту надання послуг та звіту);
- Терміни надання послуг та звіту – протягом 1 місяця з дати підписання договору;
- Фіксація ціни у гривні без будь-яких прив'язок на термін дії договору;
- Досвід проведення тестів на проникнення відповідно до міжнародних методиками для банківської сфери (не менше двох банків);
- Наявність відпрацьованої методики збору інформації методами «соціальної інженерії».
- Досвід консалтингових робіт в області інформаційних технологій та інформаційної безпеки (не менше 3-х років);
- Наявність сертифікату ASV (Approved Scanning Vendor);
- Наявність кваліфікованого персоналу з досвідом виконання тестів на проникнення;
- Наявність необхідних матеріальних ресурсів та інструментарію для виконання тесту на проникнення;
- Електронний документообіг з використанням ЕЦП;
- Відкриття рахунку в АТ «ОТП БАНК» для обслуговування договору;
- Підтвердження всіх вимог вказаних в Технічному завданні.

5. Інші вимоги щодо надання послуг:

5.1. Вартість послуг необхідно вказувати в гривнях без будь-яких прив'язок з урахуванням усіх передбачених законом податків. Оплата послуг здійснюється по факту їх надання (без передоплати).
5.2. Переможець буде обраний на підставі визначення кращої пропозиції по сумі цінових (фінансових) та нецінових (кваліфікаційних) критеріїв.
5.3. Термін проведення тесту на проникнення з урахуванням підготовки звіту – не більше 1 місяця.
5.4. Звіт щодо результатів проведення тесту на проникнення має містити наступну інформацію:

- Загальний опис проведених тестів, перелік перевірених ділянок, методика тестування;
- Виявлений недолік або вразлива ділянка;
- Метод за допомогою якого було виявлено недолік або вразливу ділянку;
- Де її було виявлено (система, об'єкт, IP адреса, людина тощо);

- Варіанти усунення (бажано запропонувати не менше 2-х варіантів реалізації та/або компенсаційний захід);
- Експертний висновок щодо ймовірного ризику, який несе знайдений недолік або вразлива ділянка;
- Загальний висновок щодо виявлених недоліків по всіх напрямках тестування;
- Звіт повинен бути оформлений українською та англійською мовами у двох примірниках кожний.

6. Умови та терміни подачі комерційних пропозицій

Для участі у тендері потрібно підготувати комерційну пропозицію та пакет необхідних документів (згідно вимог Технічного завдання) та надати через майданчик APS-tender не пізніше **21 липня 2020 року 17-00 за київським часом**.

Всі запитувані матеріали повинні бути надані Замовнику Претендентом у вигляді файлів в електронній системі торгів, завірених печаткою та підписом уповноваженої особи.

Пакет документів включає:

1. Тендерну пропозицію по формі (Додаток №1 до Технічного Завдання) разом з документами, які необхідно надати згідно Розділу 3 Форми тендерної пропозиції.
2. Заповнену заявку-реєстрацію по формі (Додаток №2 до Технічного завдання).

Мова надання тендерних пропозицій: українська.

Питання щодо роботи APS-Tender можна задати за ел. адресою: support@aps-ua.com або за телефоном: +38 (044) 337-79-18.
У разі виникнення питань по Технічному завданню прохання звертатися за наступним контактом: Болдинюк Сергій Володимирович, Serhii.BOLDYNIUK@otpbank.com.ua.
З усіх інших питань прохання звертатись за наступним контактом: Пронін Олександр Володимирович, Oleksandr.PRONIN@otpbank.com.ua.

7. Склад робочої групи:

Голова робочої групи:
Бібіч О.В., Директор Департаменту внутрішнього аудиту;

Члени робочої групі:
Болдинюк С.В., Провідний IT аудитор Департаменту внутрішнього аудиту;
Янішевський Д.О., Начальник Управління інформаційної безпеки;
Коржанюк В.В., Директор Департаменту IT інфраструктури та експлуатації;
Пелішенко Л.В., Директор департаменту розвитку та забезпечення;
Пронін О.В., Провідний фахівець управління закупівель департаменту розвитку та забезпечення.

8. Додатки:

1. Додаток №1 до ТЗ - Форма Тендерної пропозиції;
2. Додаток №2 до ТЗ - Форма заявки-реєстрація.

Голова робочої групи _____ **Бібіч О.В.**