УТВЕРЖДАЮ

Председатель Правления
АО «Молдовагаз»

_____
Вадим ЧЕБАН

«___»_____2024 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на закупку услуги по тестированию на
проникновение информационных систем
Cod CPV 72800000-8

Разработал:

Начальник Управления
информационных технологий
АО «Молдовагаз» _____ В.П. Бурковски

мун. Кишинэу – 2024 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на закупку услуги по тестированию на проникновение

информационных систем, используемых в АО «Молдовагаз»

1. Наименования предприятия:

АО «Молдовагаз»

2. Предмет закупки:

2.1. Цель теста на проникновение

Цель тестирования на проникновение заключаются в том, чтобы определить, может ли злоумышленник или авторизованный пользователь получить несанкционированный доступ к ключевым информационным системам, которые влияет на безопасность ИТ-инфраструктуры, файлов, журналов, паролей, данных пользователей и/или потребителей, и если да, то каким образом.

2.2. Целевые системы для теста на проникновение

CRM

Skype for Business

MS Exchange OWA

Mail Ex

Active Directory

Directum RX

Приложение 1С, БД MS SQL

Приложение Oracle CC&B, БД Oracle

Операционные системы, в которых размещены эти приложения.

Пользовательские компьютеры

Проводная сеть

Беспроводная сеть

2.3. Внешний тест на проникновение

Внешний тест на проникновение должен быть проведен в отношении открытых к доступу из вне служб и приложений: CRM, Skype for Business, Exchange, Корпоративный сайт, Cabinet personal, VPN.

2.4. Тестирование в режиме «grey-box»

Тестирование должно быть выполнено в режиме «grey-box» с частичным информированием тестировщика о целевых системах.

2.5. Тестирование на уровне сайта и на сетевом уровне

Эта оценка помогает выявить уязвимости, которые возникают в результате неправильного, с точки зрения безопасности, проектирования или настройки приложений, а также в результате использования

небезопасных методов кодирования или уязвимостей безопасности, которые могут возникнуть в результате небезопасной реализации, настройки, использования или обслуживания программного обеспечения.

2.6. Тесты OWASP TOP 10

Тестирование должно включать как минимум на 10 уязвимостей OWASP TOP 10 и включать в себя, тестирование аутентификации, тестирование авторизации, тестирование управления сессиями.

2.7. Проверка сегментации

Тестирование на проникновение должно подтвердить, что элементы управления и методы сегментации являются работоспособными, эффективными и изолируют целевые системы от остальных, не имеющих отношения к ним.

2.8. Тестирование должно проводиться в 2 этапа

Первичное тестирование, результатом которого должен быть отчет по уязвимым системам и демонстрацией найденных в них уязвимостей. Повторное тестирование после устранения выявленных уязвимостей, результатом которого должен быть анализ эффективности принятых мер по защите систем.

2.9. Тестирование не должно повлиять на непрерывность, целостность и доступность целевых систем и данных.

Все работы по тестированию должны быть согласованными и проводиться в заранее определенное время, чтобы минимизировать влияние на рабочие процессы. Тестирования на проникновение не должно повлиять на непрерывность, целостность и доступность целевых систем и данных.

2.10. Обеспечение конфиденциальности и безопасности данных, полученных в процессе выполнения тестирования и после.

Все данные полученные в процессе проведения работ, включая персональные данные, учетные данные, данные о уязвимостях, данные о целевых системах, ИТ-инфраструктуре, конфигурации должны быть соответственно защищены и не могут быть разглашены третьим сторонам.

3. Требования к участнику тендера:

- Иметь в портфолио минимум 5 завершенных проекта по тестированию на проникновение.
- Участник конкурса должен продемонстрировать опыт успешного проведения 3-х тестов на проникновение в организациях, работающих в публичной и банковской финансовой сфере.