**ОПРОСНЫЙ ЛИСТ ПО   
ТЕХНИЧЕСКОМУ АУДИТУ БЕЗОПАСНОСТИ**

**ОБЩИЕ СВЕДЕНИЯ**

|  |  |
| --- | --- |
|  | |
| Наименование организации |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| Email |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |
| --- | --- | --- |
| 1. Цель проведения | | |
|  | | |
| Требования законодательства о защите информации в государственных информационных системах (ФЗ-149, Приказ ФСТЭК России №17)  Требования Положения ЦБ РФ 719-П/683-П об анализе уязвимостей в прикладном ПО (ОУД4)  Требования Положения ЦБ РФ 719-П/683-П о ежегодном тестировании на проникновение и анализе уязвимостей  Оценка действующей системы информационной безопасности  Требования партнеров | | |
| Другое |  | |
|  | *Указать* | |
| *- выбрано;*  *- не выбрано* | | |
|  | | |
|  | | |
| 1. Имеется ли в Вашей организации служба безопасности (в т.ч. информационной)? | | |
|  | | |
| Да  Да, также есть отдельная служба/ сотрудник информационной безопасности  Нет  Затрудняюсь ответить | | |
|  | | |
|  | | |
| 1. Все ли объекты информационного взаимодействия в границах исследования (компьютеры, серверы, сетевое и периферийное оборудование) объединены в одну локальную сеть? | | |
|  | | |
| Да, все компьютеры «видят друг друга»  Нет  Затрудняюсь ответить | | |
| Другое |  | |
|  | *Указать* | |
|  | | |
| 1. Используется ли в границах исследования - Active Directory Domain/LDAP? | | |
|  | | |
| Да, все компьютеры в едином Домене  Да, используется несколько взаимосвязанных Доменов  Да, но используется несколько несвязанных Доменов  Нет  Затрудняюсь ответить | | |
|  | | |
|  | | |
| 1. Имеется ли подключение к сети Интернет внутри границ исследования? | | |
|  | | |
| Да, множество точек входа  Да, единственная точка входа  Нет | | |
|  | | |
|  | | |
| 1. Имеется ли DMZ? | | |
|  | | |
| Да  Нет  Затрудняюсь ответить | | |
|  | | |
|  | | |
| 1. У всех ли пользователей есть выход в Интернет? | | |
|  | | |
| Да | | Нет |
|  | | |
|  | | |
| 1. Ограничен ли доступ к ресурсам сети Интернет? | | |
|  | | |
| Не ограничен  Настроен «чёрный список» ресурсов  Настроен «белый список» ресурсов | | |
|  | | |
|  | | |
| 1. Применяются ли в границах исследования средства защиты информации? | | |
|  | | |
| Да, применяются повсеместно  Да, но только отдельные решения  Нет  Затрудняюсь ответить | | |
|  | | |
|  | | |
| 1. Укажите тип имеющихся СЗИ (антивирусы, средства корреляции (SIEM), DLP и пр.), (не указывается в случае Red Team, AppSec) | | |
|  | | |
|  | | |
| *Указать* | | |
|  | | |
| 1. Находятся ли объекты исследования в зоне ответственности какого-либо SOC? | | |
|  | | |
| Да  Нет  Затрудняюсь ответить | | |
|  | | |
|  | | |
| 1. Укажите количество внешних IP-адресов, подлежащих тестированию | | |
|  | | |
| Количество адресов |  | |
|  | *Указать* | |
| Внешнее тестирование не требуется | | |
|  | | |
|  | | |
| 1. Укажите количество WEB-ресурсов в границах исследования | | |
|  | | |
| Количество ресурсов |  | |
|  | *Указать* | |
| В границах исследования WEB-ресурсы отсутствуют | | |
|  | | |
|  | | |
| 1. Укажите количество серверов (виртуальных и физических, имеющих свои IP) в границах исследования | | |
|  | | |
| Количество серверов |  | |
|  | *Указать* | |
| В границах исследования серверы отсутствуют | | |
|  | | |
|  | | |
| 1. Укажите количество рабочих станций в границах исследования | | |
|  | | |
| Количество АРМ |  | |
|  | *Указать* | |
| В границах исследования рабочие станции отсутствуют | | |
|  | | |
|  | | |
| 1. Используемые типы линий связи в границах исследования | | |
|  | | |
| Затрудняюсь ответить  Ethernet  SFP  Wi-Fi | | |
|  | | |
|  | | |
| **↓ ↓ ↓** | | |

**ПОДХОД К ПРОВЕДЕНИЮ АУДИТА БЕЗОПАСНОСТИ**

|  |  |  |
| --- | --- | --- |
| 1. Формат проведения аудита безопасности | | |
|  | | |
| Тестирование на проникновение  Purple Team  Red Team (APT)  Эвристический анализ ПО (AppSec) | | |
|  | | |
|  | | |
| 1. Формат социальной инженерии (при необходимости) | | |
|  | | |
| Email  Телефон  Очно | | |
|  | | |
|  | | |
| 1. Желаемая форма взаимодействия (не указывается в случае Red Team, AppSec) | | |
|  | | |
| Очная форма проведения  Удалённый доступ с предоставлением необходимых полномочий  Удалённый доступ без прав доступа | | |
| Другое |  | |
|  | *Указать* | |
|  | | |
| 1. Формат проведения аудита безопасности | | |
|  | | |
| Black Box (метод «чёрного ящика»)  Gray Box (метод «серого ящика»)  White Box (метод «белого ящика») | | |
|  | | |
|  | | |
| 1. Сценарии взаимодействия со службой безопасности (при её наличии, не указывается в случае Red Team) | | |
|  | | |
| Black Hat | | White Hat |
|  | | |
|  | | |
| 1. Необходимость/желание тестирования защищенности беспроводных протоколов обмена (при их наличии) | | |
|  | | |
| Да | | Нет |
|  | | |
|  | | |
| 1. Необходимость/желание проведения стресс-тестирования (DDoS) | | |
|  | | |
| Да | | Нет |
|  | | |
|  | | |
| **↓ ↓ ↓** | | |

**СОСТАВ И СОДЕРЖАНИЕ ПРОЦЕДУР**

|  |
| --- |
| 1. Желаемая «глубина» аудита безопасности (не указывается в случае Red Team, AppSec) |
|  |
| По требованиям НПА  Сбор данных из открытых источников  Оценка привлекательности для кибератак  Тестирование конфигураций DNS  Поиск незащищенных информационных каналов  Активное сканирование  Идентификация сервисов/служб/приложений  Анализ внутренней инфраструктуры  Автоматизированный поиск уязвимостей  Эвристический ручной анализ |
|  |
|  |
| 1. Желаемые техники проведения эвристического анализа ПО (не указывается в случае AppSec) |
|  |
| По требованиям НПА (ОУД)  Функциональное тестирование  Нагрузочное тестирование  Фаззинг  Сигнатурный анализ кода  Динамический анализ кода  Обратная разработка  Анализ реализованных механизмов |
|  |
|  |
| 1. Желаемый перечень работ |
|  |
| Внешнее тестирование на проникновение  Внутреннее тестирование на проникновение  Тестирование на проникновение веб-приложений  RED TEAM  Социальная инженерия |
|  |
|  |
| 1. Желаемый перечень сопутствующих работ |
|  |
| Анализ платежного ПО по ОУД4  Разработка модели угроз по новой методике ФСТЭК |
|  |
|  |
| 1. Желаемый перечень иных работ |
|  |
| Приведение в соответствие требованиям 716-П  Аудит организации в направлении обработки/защиты персональных данных  Аудит на соответствие требованиям 719-П, 683-П, 757-П, 747-П, иных источников требований ЦБ/Приведение в соответствие требованиям 719-П, 683-П, 757-П, 747-П, иных источников требований ЦБ  Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580  Независимая внешняя оценка SWIFT  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» |
|  |
|  |

|  |  |
| --- | --- |
| 1. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ | |
|  | |
| Планируется ли поставка решений ИБ/ИТ?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ? | |
|  | |
| Какие решения по ИБ/ИТ вами рассматриваются? |  |
|  | *Указать* |
|  | |
|  | |

Благодарим за уделенное время!