**Раздел:** Жизненный цикл ИБ

**Модуль:** Методологии обеспечения ИБ. Взаимодействие с регуляторами

**Выполнил:** Василий Костюков

**Условие задачи**

Компания ООО «ABC» — финансовая организация.

Руководитель — председатель правления Иванов А. Г.

Начальник отдела информационной безопасности — Петров Б. В.

У компании есть API для подключения партнёров. Подключение партнёров на стороне ООО «АВС» выполняется через админку «Партнёр-API». Админка не содержит карточных данных. Компания уже перешла на стандарт PCI DSS 4.0.

**Что нужно сделать**

Напишите политику аутентификации для внутренней админки управления информацией платёжными интеграциями с партнёрами «Партнёр-API». Политика должна определять условия процедуры аутентификации сотрудников компании в админку и соответствовать требованиям регуляторов.

1. Изучите требования к аутентификации в ГОСТ 57580 и PCI DSS 4.0.
2. Определите требования к паролям, такие как длина, сложность, периодичность смены и т. д.
3. Определите требования к множественной аутентификации, такие как использование двухфакторной аутентификации и т. д.
4. Определите требования к блокировке учётных записей при неудачных попытках входа и к автоматическому отключению неактивных сессий.
5. Определите требования к аутентификации для удалённого доступа к системам и ресурсам компании.
6. Напишите политику аутентификации для личного кабинета «Партнёр-API» в соответствии с определёнными требованиями.

Условия реализации

Пришлите письменный отчёт в формате документа Microsoft Word или в формате PDF.

Подсказки

* Если в админке нет карточных данных, то скорее всего она не входит в область соответствия PCI DSS, и требования PCI DSS на неё могут не распространяться.
* Требования к паролям и аутентификации для информационных систем финансовых организаций для большинства случаев описаны в ГОСТ Р 57580.1-2017.
* Полезно, но не обязательно использовать и другие лучшие практики в области аутентификации.

**Компания «АВС»**

Изучены требования в айтентификации описанные в ГОСТ 57580 и PCI DSS 4.0. Так как компания «АВС» (далее компания) перешла на стандарт PCI DSS 4.0, но при этом не использует карточных данных при подключении к админке «Партнёр-API», то этот стандарт будет задействован не полностью, будут использованны только некоторые элементы для обеспечения безопасности доступа и защиты персональных данных клиентов компании.

1. **Соблюдение стандартов.**

Политика информационной безопасности компании для обеспечения аутентификации доступа в личный кабинет «Партнёр-API», составлена с учётом стандартов ГОСТ 57580 и PCI DSS 4.0.

*Необходимо проводить следующие мероприятия:*

- ежегодное тестирование на проникновение

- ежегодное обучение сотрудников

- ежеквартальное внешнее и внутреннее сканирование на уязвимости

- разграничение доступа

- обработка логов, мониторинг и анализ всех событий

- защита от вредоносного кода

- ведение контроля над всеми учётными записями, при переходе на другоую должность производить изменения уровня доступа, при увольнении сотрудника деактивировать аккаунт незамедлительно

1. **Установить следующие требования к аутентификации:**

*Требования к паролю:*

- срок жизни пароля – 60 дней

- минимальная длина – 10 символов

- пароль должен состоять из комбинации 4 типов символов (большие и маленькие буквы, числа и спец символы)

- пароль не должен повторять простые слова и их комбинации (например, админ123)

- пароль не может повторять 5 ранее использованных

*Двухфакторная аутентификация:*

- осуществить переход на обязательную двухфакторную аутентификацию с использованием мобильного телефона (смс, звонок или 2FA-приложение)

*Требования к блокировке учётной записи:*

- пароль блокируется после 5 неудачных попыток на 60 минут, для срочного разблокирования предусмотреть возможность обращения к администратору, через своего менеджера (для надёжного установления личности)

*Требования для удалённого доступа к системам и ресурсам компании:*

- удалённый доступ осуществляется посредством VPN

- доступ к ресурсам чётко разграничен и структурирован, любые изменения осуществляются по письменному запросу с одобрениея прямого руководителя

1. **Инциденты и ответственность**

- назначить ответственный персонал для ведения мониторинга и реагирования на инциденты связанные с личным кабинетом «Партнёр-API»

- расписать обязанности и мероприяния по реагированию на инциденты, а также процесс уведомления руководства и привлечения IT подразделения к купированию инцидентов

- разработать методы реагирования и ликвидации инцидентов: компрометация учётных данных, утечка информации, несанкционированный доступ

- проводить ежегодные тренинги и team-building events для изучения инцидентов, методов реагирования, и усиления слаженности IT команды

- раз в пол года проводить занятия для всех сотрудников связанных с работой личного кабинета «Партнёр-API»

Ответственность за реализацию технических аспектов и подготовку документации для реализации данной политики доступа к личному кабинету «Партнёр-API» возлагается на начальника отдела информационной безопасности – Петрова Б. В.

Контроль за исполнением осуществляет руководитель – председатель правления Иванов А. Г.