РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ДЛЯ УПРАВЛЕНИЯ НАРУЖНОЙ РЕКЛАМОЙ

Управление конечным устройством/конструкцией

1. Физическая безопасность:

● Дверцы конструкций и блока управления должны быть оборудованы датчиками открытия с настроенным оповещением оператора service Desk в реальном времени.

● Для статусных конструкций (площади, аэропорты), камера, направленная на основную часть конструкции для детектирования попыток физического доступа.

● Возможность удаленного аварийного отключения конструкций/бордов при ЧС для сотрудников уполномоченных органов - “Красная кнопка”.

2. Безопасность сети:

● Сетевая сегментация:

○ DMZ - для публичных сервисов доступных из сети Интернет;

○ IoT - для датчиков, камер, контроллеров;

○ Internal - для внутренних сервисов.

● Фильтрация и инспекция межсетевого трафика конструкции системой предотвращения вторжений (IPS) и сетевым антивирусом (AV).

● Сетевая изоляция конструкций на уровне сети - таким образом компрометация одной конструкции не приводит к компрометации остальных.

● Контроль административного доступа - удаленное подключение для администрирования конструкции должно осуществляться по шифрованному каналу VPN, с подключением администратора через систему контроля привилегированного доступа (PAM) или bastion host, сконфигурированный по принятому в компании стандарту безопасной конфигураций.

● Рекомендационный характер: подключение к сети посредством проводного подключения для исключения ряда векторов атак.

3. Безопасность инфраструктуры:

● Все устройства, обеспечивающие функционирование конструкции должны быть настроены в соответствии с рекомендациями по безопасной настройке от производителей решений (для IoT и сетевых устройств) либо принятым в компании стандартам безопасной конфигураций ОС (для серверов). Настройки должны пересматриваться не реже 1 раза в год, либо при внесении значимых архитектурных изменений.

● Программное обеспечение должно регулярно проверяться на наличие уязвимостей, обнаруженные уязвимости должны быть устранены в срок, согласованный в политике управления обновлениями.

4. Безопасность данных:

● Коммуникации между критичными компонентами (например, управление контентом) должны быть зашифрованы надежными алгоритмами шифрования для защиты от перехвата данных злоумышленником.

● Рекомендуется использовать шифрование диска (Full Disk Encryption) для серверов в недоверенных средах.

5. Мониторинг и логирование:

● Любые изменения на сетевых и инфраструктурных компонентах конструкции, такие как события аутентификации, изменения конфигураций, создание задач по расписанию (cron), изменения файловой системы и реестра, несанкционированное открытие портов должны фиксироваться и направляться в централизованное хранилище для обработки и корреляции.

Требования к платформе управления контентом CMS

1. Контроль доступа и аутентификация:

● Ролевой модели доступа (RBAC)

● Использование многофакторной аутентификации (2FA/MFA) с использованием OTP с длинной не менее 6 символов.

● Усиленная парольная политика (Обеспечьте соблюдение правил использования сложных паролей (например, минимальная длина, сложность, срок действия) для всех пользователей.)

● Управление сеансами: установка времени истечения сеанса и автоматический выход из системы для неактивных пользователей.

● Ограничение доступа администратора по IP-адресу: доступ на основе IP-адресов, диапазонов IP или геолокации IP-адреса.

2. Безопасность данных

● Шифрование в состоянии хранения, обработки и при передаче: использование для конфиденциальных данных как при хранении (например, в базах данных), так и при передаче (например, HTTPS/TLS).

● Резервное копирование и восстановление: обеспечение регулярного резервное копирование данных CMS и процесс восстановления, чтобы снизить потери данных.

3. Журналирование событий и мониторинг

● Регистрация действий: Ведение подробных журналов действий пользователей (входы в систему, создание, изменение, удаление контента и т. д.) для выявления подозрительных действий.

● Оповещение и мониторинг: Настройте мониторинг в режиме реального времени и оповещение о необычных действиях (например, попытках входа в систему, неудачном доступе, загрузке файлов с неизвестных IP-адресов).

4. Безопасность программного обеспечения

● Регулярное обновление программного обеспечения: CMS, ее плагины и базовое программное обеспечение регулярно должны обновляться.

● Уменьшение поверхности атак: применение практик безопасности (отключение ненужных служб, портов сетевого и другого оборудования).

● Безопасная разработка: внедрение инструментов безопасности в процесс разработки (SAST, DAST, SCA).

● Межсетевой экран веб-приложений (WAF): Использование WAF для защиты от распространенных веб-атак.

● Прохождение испытаний/сертификации ПО на предмет соответствия требованиям безопасности РК.

5. Безопасность программных интерфейсов API и интеграции

● Аутентификация API: Использование OAuth, API-ключей или JWT-токены для аутентификации API-запросов и убедитесь, что конфиденциальные конечные точки не находятся в открытом доступе.

● API Rate Limiting: использование механизма контроля количества запросов, которые API может обработать за определенный период времени для предотвращения DDoS атак..

● Безопасные сторонние интеграции (если применимо)

6. Целостность содержимого контента и безопасность

● Журналы аудита: ведение журнал аудита: кто, когда и почему внес изменения в контент.

● Рабочий процесс проверки и утверждения контента: внедрение строгого процесса утверждения контента, включающий в себя согласование уполномоченных органов внутри платформы, чтобы свести к минимуму риск публикации вредоносного контента.

● Цифровые подписи: в сценариях с высоким уровнем безопасности используйте цифровые подписи на опубликованном контенте для проверки его подлинности.

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ТЕЛЕКАНАЛОВ

1. Физическая безопасность вещательного оборудования:

● Аппаратные комнаты, студии, аппаратно-программные комплексы (АПК) должны быть оборудованы датчиками доступа с уведомлением дежурной смены или ИБ-службы при вскрытии.

● В помещениях с вещательными серверами, видеомикшерами и автоматизированными системами необходимо наличие видеонаблюдения с записью архива.

● Обеспечьте физическое разделение студийного оборудования и офисных рабочих мест, а также контроль доступа по индивидуальным картам.

2. Безопасность сетевой инфраструктуры:

● Внедрите сетевую сегментацию:

● VLAN для студийных систем (режиссура, графика, микшеры),

● VLAN для вещательных серверов (Playout/IPTV/RTMP),

● VLAN для монтажных и контентных станций,

● Изолированная сеть для систем безопасности (антивирусы, SIEM, мониторинг).

● Запретите прямой доступ между сегментами, используйте межсетевые экраны и IPS.

● Установите межсетевой экран между производственным контуром и Интернетом, разрешая только необходимые направления (например, CDN, телеметрия).

● Обеспечьте администрирование только через VPN + Jump-host с многофакторной аутентификацией (MFA).

3. Безопасность эфирной и контентной инфраструктуры:

● Обновите ПО студийных систем (видеомикшеры, медиа-серверы, графические комплексы) до актуальных безопасных версий.

● Отключите неиспользуемые сервисы и порты на рабочих станциях и серверах вещания.

● Введите стандарты безопасной конфигурации для всех ключевых компонентов эфирного оборудования.

● Защитите вещательные потоки с помощью TLS (например, SRT over TLS, RTMPS) или аналогичных технологий.

● Для связи с CDN, провайдерами доставки — используйте токенизацию, DRM и цифровую подпись потока.

4. Безопасность данных и доступа к эфирным системам:

● Настройте ролевую модель доступа (RBAC): монтаж, публикация, эфир — разные уровни.

● Используйте MFA/2FA для доступа в CMS, системы плейлистов и графических редакторов.

● Ограничьте административный доступ по IP или геолокации.

● Реализуйте автоматическое завершение сессий при простое, логирование входов, контроль одновременных подключений.

● Зашифруйте трафик между ключевыми компонентами (сервер → encoder, редактор → графика).

5. Защита эфирного контента и CMS:

● Все действия по публикации и изменению контента должны быть журналированы с указанием пользователя, времени, действия и результата.

● Перед выходом в эфир критичных блоков (обращения, экстренные сообщения) должен быть предусмотрен процесс утверждения и цифровой контроль целостности.

● Внедрите репликацию и резервное копирование CMS/контента с быстрым механизмом восстановления.

● Включите ограничение API и внешних интеграций:

● Авторизация API по токенам, rate limiting, whitelisting IP.

● Проверка всех внешних RSS/новостных фидов на предмет целостности.

6. Мониторинг и реагирование:

● Все ключевые системы должны быть подключены к централизованной системе логирования (SIEM).

● Мониторьте:

● события входа и выхода из CMS,

● изменение плейлистов,

● перезапуск потоков,

● вставки рекламных и служебных блоков.

● Настройте автоматическое оповещение при отклонениях (изменение расписания без утверждения, новая сессия с неизвестного IP и т.д.).

● Подготовьте план экстренного переключения на резервный эфир, в том числе ручное переключение на pre-approved поток при признаках атаки.

7. Дополнительные меры на период праздников:

● Проведите внеплановую проверку журналов доступа, статуса обновлений ПО, целостности контента.

● Обеспечьте дежурство ИБ-специалистов или оперативной смены на весь период праздничных трансляций.

● Проведите инструктаж операторов эфирного комплекса по действиям в случае захвата или сбоя трансляции.