EBU

OPERATING EUROVISION AND EURORADIO

R 143

CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES

RECOMMENDATION

Geneva
April 2016

EBU

OPERATING EUROVISION AND EURORADIO

R 143

CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES

Внимание!
Данный перевод **НЕ** претендует на аутентичность
и может содержать отдельные неточности.
Оригинал документа на сайте https://tech.ebu.ch

РЕКОМЕНДАЦИЯ ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ СИСТЕМ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УСЛУГ МЕДИА ПОСТАВЩИКОВ

РЕКОМЕНДАЦИЯ

Женева
Апрель 2016

Рекомендация по кибербезопасности для систем, программного обеспечения и услуг медиа поставщиков

Комитет EBU	*Первый выпуск*	*Переработка*	*Переиздание*
TC	2016		

Ключевые слова: Безопасность, Услуги, Инфраструктура, Вещание, IP.

Рекомендация

EBU, учитывая, что

1. Медиа компании все больше используют третьи стороны для поставки систем, программного обеспечения и услуг.
2. Производственные процессы и инфраструктуры быстро переходят на общие IT технологии.
3. Киберугрозы (например, вредоносные программы) становятся проще в исполнении и постоянно развиваются.
4. Подключенные медиа устройства по-прежнему имеют низкий порог безопасности, унаследованный с эпохи неподключенных вещательных медиа.

Рекомендует медиа компаниям:

1. Применять прилагаемые меры безопасности при планировании и разработке своих систем, программного обеспечения и услуг.
2. Требовать от потенциальных поставщиков систем, программного обеспечения и услуг декларации их способности к соответствию прилагаемым мерам безопасности (путем заполнения колонок A, B & C) во время ответа на тендеры или технологические задания.
3. Определять свой минимальный уровень приемки систем поставщиков на основе данной рекомендации с полным знанием потенциальных рисков.

Примечание

Прилагаемые меры безопасности составлены по материалам признанных европейских институтов безопасности, включая ANSSI[1], BSI[2], вместе с материалами группы европейских вещателей, имеющих недавний трудный опыт в решении проблем безопасности.

[1] Agence Nationale de la Sécurité des Systèmes d'Information (Франция): http://www.ssi.gouv.fr
[2] Немецкий альянс кибербезопасности: https://www.allianz-fuer-cybersicherheit.de/

Приложение: Рекомендованные требования к безопасности

Требование к безопасности для поставщика	A Выполняете ли вы данное требование? (Да или Нет)	B Если вы ответили "Нет" в колонке A, то когда это требование будет удовлетворено / выполнено?	C Ваши вопросы / Примечания
1. Организационные меры безопасности			
1.1 Жизненный цикл продуктов и внутренние процессы			
Следование известной передовой практике или стандартам защиты информации при разработке и реализации мер безопасности			
Стремление к широко принятой сертификации реализованных мер безопасности			
«Реализованная, записанная политика развития (напр. соблюдение OWASP Top 10…)»			
Обязательные этапы испытаний (ворота в системе защиты) в цикле разработки			
Анализ реализованного кода в цикле разработки			
Очистка продуктов, чтобы не осталось никакого тестового кода из процесса разработки			
Регулярный анализ технической безопасности (тесты на проникновение и уязвимость)			
Отслеживание и обработка уязвимости			
Четкое определение жизненного цикла продуктов и гарантия наличия патчей и обновлений в течение жизненного цикла.			
Поддержка обновлений защиты всех сторонних компонентов, включая платформу операционной системы и среду выполнения.			
1.2 Коммуникации			
Назначенные контактные лица или другие варианты контактов по вопросам и инцидентам безопасности			
Информационный процесс для потребителей в случае выявления слабых мест в продукте			
«Поставщик должен поддерживать процедуры доступа потребителей для обслуживания (RAS, VPN, аккаунты, пароль)»			
2. Меры безопасности для продуктов			
2.1 Документация			
Четкая инструкция по смене паролей с установленных по умолчанию при необходимости			
Четкое описание функций безопасности			
«Документация интерфейсов, точек доступа, сетевых коммуникаций и свойств»			
«Включение информации о том, как интегрировать продукт в концепцию безопасности (напр. разные зоны сети, центральная служба аутентификации, рабочие процессы, интерфейсы, открытие только необходимых портов TCP/UDP …)»			
Рекомендация по усилению защиты или передовой практике конфигурации			
Описание процесса управления патчами в обновлении защиты			

Требование к безопасности для поставщика	A Выполняете ли вы данное требование? (Да или Нет)	B Если вы ответили "Нет" в колонке A, то когда это требование будет удовлетворено / выполнено?	C Ваши вопросы / Примечания
2.2 Аутентификация и авторизация			
«Поддержка центральных служб аутентификации (напр. LDAP, активная директория, радиус)»			
Поддержка лимита времени сеанса			
Поддержка контроля доступа на основе ролей			
Поддержка персонализированных аккаунтов			
Принудительная смена паролей, установленных по умолчанию			
Поддержка реализации политики паролей			
Поддержка двухфакторной аутентификации для продуктов с выходом в интернет			
Строгая аутентификация, например, двухфакторная			
Поддержка протоколирования AAA в централизованном сервере регистрации			
2.3 Шифрование			
Хранение и передача шифрованных паролей			
Поддержка новейших технологий шифрования с соблюдением передовых рекомендаций			
«Поддержка шифрованных (напр. на базе TLS) сетевых протоколов (https, ftps, sftp)»			
«Избегание чисто текстовых протоколов (http, telnet, ftp)»			
Поддержка сертификатов и использования PKI			
2.4 Базовая конфигурация			
Поддержка регистрации (как минимум, неудачные и удачные события регистрации AAA)			
«Поддержка централизованной регистрации системных журналов (Syslog, Events Logs)»			
Опция для контроля соединения USB и портативных медиа			
Деактивация ненужных сетевых протоколов и услуг			
«Поддержка эффективной защиты от вирусов / вредоносных программ и использование (напр. Antivirus, EMET) со стороны сервера и клиента.»			
Усиление базовой операционной системы в случае ее обеспечения поставщиком			
Поддержка сканеров уязвимости			
Поддержка мониторинга (мин. SNMPv2)			
Поддержка резервирования / восстановления (установки конфигурации)			
Возможность отделения операционной системы от самого программного обеспечения (с возможностью корректировки OS и среды выполнения)			

Требование к безопасности для поставщика	A **Выполняете ли вы данное требование?** **(Да или Нет)**	B **Если вы ответили "Нет" в колонке A, то когда это требование будет удовлетворено / выполнено?**	C **Ваши вопросы / Примечания**
2.5 Сетевая конфигурация			
«Поддержка достаточно детальной сегментации сетей (MPLS, поддержка Multi VLAN, маршрутизация)»			
Отсутствие прямого соединения компонентов управления с интернетом (вопросы лицензирования)			
«При необходимости соединения с интернетом – поддержка проверки контента (напр. прямой и обратный прокси-сервер, включая механизмы аутентификации)»			
Поддержка точек доступа для обслуживания в демилитаризированной зоне (DMZ) чтобы поставщики или администраторы сначала подключались к DMZ вместо самого приложения. (напр. Jumphosts)			
2.6 Защита приложений			
Реализованная проверка вводимых значений внутри приложения			
Средства управления для межсайтового скриптинга и внесения SQL для клиентских веб-серверов (напр. OWASP Top 10)			
«Поддержка управления выпуском дополнительных плагинов (напр. Flash, Java, PHP, …)"			
Регулярное управление патчами для поставляемых приложений			
Работа приложений не в контексте администратора (с минимальными привилегиями)			
Управление и коммуникации уязвимости нулевого дня			
3. ISMS поставщика			
Имеется документированная политика кибербезопасности			
Создана эффективная организация кибербезопасности			
Назначен начальник управления информационной безопасности, имеющий необходимую компетенцию для выполнения этой роли			
Существует аудиторский план, который включает регулярные проверки и тесты на проникновение для внутренней инфраструктуры			
«Кибербезопасность включена в обучение персонала, проводятся регулярные информационные кампании»			