EBU

OPERATING EUROVISION AND EURORADIO

R 144

CYBERSECURITY GOVERNANCE FOR MEDIA COMPANIES

RECOMMENDATION

SOURCE: SP-MCS

Geneva
September 2016

EBU

OPERATING EUROVISION AND EURORADIO

R 144

CYBERSECURITY GOVERNANCE FOR MEDIA COMPANIES

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

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ ДЛЯ МЕДИА КОМПАНИЙ

РЕКОМЕНДАЦИЯ

ИСТОЧНИК: SP-MCS

Женева
Сентябрь 2016

Управление кибербезопасностью для медиа компаний

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

Ключевые слова: Информационная безопасность, Кибербезопасность, IT безопасность, Управление, ISMS

Рекомендация

EBU, учитывая, что:

1. Медиа компании все чаще опираются на такие информационные технологии и сети как интернет.
2. Растет угроза кибератак (и в настоящее время успешно атаковано несколько вещательных компаний);
3. Кибератаки могут вести к ущербу для вещательных компаний, и
4. Нарушения информационной безопасности в целом могут вести к ухудшению передачи услуг, ущербу для репутации, несоответствию законам и нормативам, а также к финансовым штрафам.

Рекомендует:

Создать в медиа компаниях управление кибербезопасностью, которое включает:

1. Административное руководство и отдел управления, занимающийся политикой безопасности[1].
2. Кибербезопасность как часть коммерческих задач и процессов.
3. Определение ролей кибербезопасности, включая финансовые ресурсы. (См. на обороте и **Приложение А**).
4. Объединение действий по информационной безопасности и корпоративному управлению рисками с целью достижения как минимум третьего уровня зрелости кибербезопасности. (Определение см. в **Приложении В**).
5. Реализацию **системы управления информационной безопасностью (ISMS),** которая следует передовой практике, установленной в международных стандартах, например, ISO/IEC 27001, 27002 и в ENISA[2] .

Справочная информация к данной рекомендации по кибербезопасности

Цель информационной безопасности – защита информации от несанкционированного доступа, модификации, рассекречивания, кражи или разрушения, независимо от ее формы (например, электронной, печатной или устной). Кибербезопасность в отношении информационной технологии - это важный поднабор информационной безопасности. В данной рекомендации термины кибербезопасность и информационная безопасность употребляются равноправно.

Каждая (медиа) компания, которая зависит в своем бизнесе от IT и сетей, должна иметь организацию кибербезопасности для управления политикой кибербезопасности компании. Эта организация должна включать как минимум следующие роли:

- CISO - Chief Information Security Officer - главный директор по информационной безопасности
- CSIRT - CyberSecurity Incident Response Team - группа реагирования на нарушение кибербезопасности
- SOC - Security Operational Centre - операционный центр безопасности
- Поддержка первого и второго уровня, включая функции безопасности.

И опционально следующие роли:

- Директоры по IT безопасности региональных или внутренних подразделений
- Отдел информационной безопасности
- Внутренний аудит.

Эти роли и их обязанности полностью объясняются в Приложении А

Информативные приложения А и В – далее.

---

[1] Политика кибербезопасности обычно содержится в кратком документе, утвержденном административным руководством, и включает:

- Область действия
- Заявление об обязательствах административного руководства
- Определение ролей кибербезопасности
- Четко определенные обязанности CISO (главного директора по информационной безопасности)
- Цели защиты CAI (конфиденциальность, готовность, целостность).

[2] ENISA - European Union Agency for Network and Information Security.
https://www.enisa.europa.eu/publications/standardisation-for-smes.

Приложение A: Роли и обязанности в области кибербезопасности

1. Главный директор по информационной безопасности (CISO)

CISO несет полную ответственность за все вопросы, связанные с информационной безопасностью, в вещательной компании. Он имеет компетенцию в принятии решений с бюджетом для выполнения проверок (в зависимости от размера организации с группой) и оценивает риски кибербезопасности. CISO входит в руководство среднего звена и подотчетен члену исполнительного органа или совета директоров (например, COO или CEO). Риски кибербезопасности также включены в корпоративный процесс управления рисками и, следовательно, подотчетны совету директоров. В зависимости от размера организации роль CISO должна выполняться эквивалентом одного сотрудника на полную ставку, имеющего достаточное ноу-хау и сертификацию промышленного стандарта.

CISO также служит для взаимодействия с правительственными органами, ответственными за кибер-защиту.

Кибербезопасность не ограничивается IT системами (офисными, управляющими) а должна включать вещательные системы в целом. Кибербезопасность этих систем – высший приоритет для CISO в вещательной компании. Если IT департамент компании отделен от вещательного департамента, настоятельно рекомендуется, чтобы CISO не принадлежал только IT департаменту.

2. Операционный центр безопасности (SOC)

SOC представляет основные операции для оборудования безопасности, например, файрвол(ы), IDS/IPS, прокси и SIEM (Security Information and Event Management). Он входит в IT департамент предприятия и в роли операционного центра реализует и обеспечивает безопасность, требуемую CISO, а по необходимости – региональными директорами по IT безопасности.

3. Группа реагирования на нарушение кибербезопасности

CyberSecurity Incident Response Team (CSIRT)

Эта роль обычно выполняется в департаменте, ответственном за обнаружение нарушений безопасности и организацию адекватного реагирования на киберугрозу. Она также анализирует объем и уровень уязвимости в информационных системах и технически контролирует соответствие внутренней политике кибербезопасности. Она также гарантирует обзор угроз кибербезопасности и уязвимости из программного обеспечения и систем в компании.

Информация, анализируемая группой CSIRT, не ограничивается информацией и событиями из приборов системы безопасности (файрвол, антивирус, IDS и т.д..) но берется и из других элементов IT инфраструктуры (особенно корпоративной службы доступа к каталогам), а в организациях с высоким уровнем кибербезопасности (см. **Приложение B**) – из бизнес-приложений, таких как системы трафика и автоматизации и системы поддержки для финансового управления, управления HR и т.д.

Рекомендуется, чтобы группа CSIRT не эксплуатировала напрямую приборы системы безопасности или техническое оборудование, связанное с IT производством (например, Firewall). Эту обязанность выполняет SOC, который, тем не менее, управляется CSIRT для контроля нарушений безопасности. Рекомендуется, чтобы CSIRT была функционально подотчетна CISO.

Группа CSIRT также должна безопасно обнаруживать и сообщать о нарушениях внутренних нормативов компании или национальных законов, которые могут привести к дисциплинарным мерам внутри компании вплоть до адвокатского расследования против ответственных лиц.

Рекомендуется установить этические нормы для обеспечения контролируемой работы CSIRT и реализовать в компании процедуру отчетности о нарушениях. Группа CSIRT требует весьма обширных ресурсов и опыта в области кибербезопасности. Эти навыки обычно дефицитны даже в крупных медиа компаниях. Поэтому рекомендуется дополнить или расширить внутреннюю группу CSIRT доверенными внешними компаниями CSIRT, имеющими соответствующую международную и национальную сертификацию.

4. Общая поддержка первого и второго уровня

Для обеспечения безопасности в процессы безопасности обычно включена поддержка первого и второго уровня для достижения гармонизированных и эффективных результатов.

5. Директор по IT безопасности регионального / внутреннего подразделения

Директор по IT безопасности регионального или внутреннего подразделения – опциональная роль, которая может требоваться в зависимости от размера или общей организации компании. Эта роль реализует всю корпоративную политику безопасности в зоне ответственности (организации, филиале или регионе). Этот директор должен быть функционально подотчетен CISO - главному директору по информационной безопасности, но может быть сотрудником региональной организации. Обычно директор по IT безопасности регионального или внутреннего подразделения совмещает работу с другими должностями и отвечает за определение политики кибербезопасности внутри своего периметра.

6. Отдел информационной безопасности

Для организации безопасности внутри медиа компании необходимо создать национальный комитет или отдел информационной безопасности, состоящий из всех директоров по IT безопасности региональных или внутренних подразделений, CISO и дополнительных корреспондентов по кибербезопасности. Сам отдел должен быть подотчетен адекватной дирекции. Задачи, компетенция и нормы эскалации отдела информационной безопасности должны официально утверждаться советом директоров.

7. Внутренний аудит

Роль внутреннего аудита компании обычно находится в специальном департаменте, который гарантирует соответствие различной деятельности юридическим и стандартным требованиям. Внутренний аудит обычно не зависит от компании, но независимость и объективность – его главные принципы, поэтому организационно или функционально он должен быть связан с советом директоров. Рекомендуется, чтобы внутренний аудит также включал кибербезопасность.

Приложение B: Уровни зрелости кибербезопасности

Уровни зрелости кибербезопасности основаны на *модели зрелости функциональных возможностей,* которая определяет общую зрелость по пяти уровням от 1 (хаотичности) до 5 (оптимизации).

Уровень 1 (хаотический):

Ответственность за кибербезопасность не документирована; безопасность в целом организована «ситуативно», обычно неконтролируемо и реакционно. Если роль CISO (главного директора по кибербезопасности) не определена, уровень зрелости кибербезопасности обычно будет 1.

Уровень 2 (повторяемый):

Ответственность за кибербезопасность назначена и документирована. Часть процессов кибербезопасности организована с повторяемостью, как стандартные процедуры. Общее управление кибербезопасностью по-прежнему реакционно.

Уровень 3 (определенный):

Имеется формальная политика кибербезопасности, утвержденная административным руководством, и документированная политика допустимого использования. Многие процессы документированы; могут быть охарактеризованы как «стандартные» и со временем улучшаются.

Процессы кибербезопасности должны охватывать следующие области (следует учитывать передовую практику и международные стандарты, например, ISO/IEC 27001/27002, CSA Star, German BSI IT Grundschutz, NIST SP800-100 или Cobit):

- Управление фондами
- Кибербезопасность для человеческих ресурсов
- Безопасность инфраструктуры (включая сеть, хранение, операционную систему)
- Безопасность платформы (межплатформное ПО, базы данных)
- Безопасность программного обеспечения (включая разработку безопасного ПО)
- Управление аудитом
- Управление непрерывностью бизнеса
- Управление изменениями и конфигурацией
- Управление рисками кибербезопасности
- Управление идентификацией и доступом
- Управление нарушениями безопасности
- Управление угрозами и уязвимостью

Уровень 4 (Управляемый):

Имеется организация кибербезопасности, которая действует упреждающе. Регулярно производится формальная оценка риска кибербезопасности (например, по принципу ISO/IEC 27001). Обычно имеется некоторая метрика для измерения, контроля и оптимизации процессов кибербезопасности. Зрелость процессов кибербезопасности можно доказать регулярными самооценками.

Уровень 5 (Оптимизирующий):

Система управления информационной безопасностью утверждена внешним органом (например, официальной сертификацией ISO/IEC 27001). Главная задача всех процессов кибербезопасности – оптимизация и улучшение.

Вопросы по управляемой самооценке кибербезопасности

Уровень 1:

- Назначена ли в вашей организации роль CISO (главного директора по кибербезопасности)?

Уровень 2:

- Назначена и задокументирована ли в вашей организации роль CISO? Документирование должно включать некоторые ключевые аспекты ответственности роли CISO.
- Задокументированы ли уже в вашей организации процессы или требования кибербезопасности?
- Проводится ли их упреждающий анализ для определения недостатков и улучшения общей кибербезопасности?

Уровень 3:

- Есть ли политика кибербезопасности, формально утвержденная административным руководством организации? Если да, эта политика должна указывать как минимум:
  - Область действия
  - Обязательства
  - Роли
  - Обязанности CISO
  - Цели защиты CAI (конфиденциальность, готовность, целостность)
- Имеется ли и функционирует ли организация кибербезопасности? Организация кибербезопасности должна включать по необходимости следующие роли:
  - CISO (главный директор по информационной безопасности)
  - CSIRT (группа реагирования на нарушение кибербезопасности)
  - SOC (операционный центр безопасности)
  - Поддержка первого и второго уровня, которая включает функции безопасности

опционально

  - Директоры по IT безопасности региональных или внутренних подразделений
  - Отдел информационной безопасности
  - Внутренний аудит

- Задокументированы и эксплуатируются ли их процессы кибербезопасности? Процессы кибербезопасности должны охватывать следующие области (следует учитывать передовую практику и международные стандарты, например, ISO/IEC 27001/27002, CSA, German BSI, NIST или Cobit):
  - Управление фондами
  - Кибербезопасность для человеческих ресурсов
  - Безопасность инфраструктуры (включая сеть, хранение, операционную систему)
  - Безопасность платформы (межплатформное ПО, базы данных)
  - Безопасность программного обеспечения (включая разработку безопасного ПО)
  - Управление аудитом
  - Управление непрерывностью бизнеса
  - Управление изменениями и конфигурацией
  - Управление рисками кибербезопасности
  - Управление идентификацией и доступом
  - Управление нарушениями безопасности
  - Управление угрозами и уязвимостью

Уровень 4:

- Действует ли упреждающе ваша организация кибербезопасности?
- Проводится ли регулярная оценка риска кибербезопасности (например, в соответствии с ISO/IEC 27001)?
- Имеется ли какая-либо метрика для измерения эффективности политики и процессов кибербезопасности?
- Проводится ли регулярная самооценка для измерения зрелости кибербезопасности в вашей организации?

Уровень 5:

- Сертифицирована ли внешним органом ваша система управления информационной безопасностью?