КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ОРГАНИЗАЦИЙ

КОНТРОЛЬНЫЙ СПИСОК ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ОТНОШЕНИЙ С ТРЕТЬИМИ ЛИЦАМИ

РЕКОМЕНДАЦИИ ПО ВЫБОРУ ПОСТАВЩИКОВ С УЧЕТОМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

При оценке потенциального поставщика вы должны рассмотреть следующие вопросы:

- ☐ **Как они обслуживают клиентов, подобных вашей организации?**
- ☐ **Документировали ли они их соответствие установленным стандартам кибербезопасности, например, модели Национального института по стандартизации и технологии (NIST) или стандарту ISO 27001, а также могут ли они предоставить отчет SOC2?**
- ☐ **Какие из ваших данных и/или активов необходимы им для предоставления своих услуги запрашивают ли они какой-либо явно нецелесообразный доступ?**
- ☐ **Как они планируют обеспечить защиту активов и данных вашей организации, находящихся в их распоряжении?**
- ☐ **Как они управляют собственными киберрисками в отношении третьих лиц, и могут ли они предоставить информацию по обеспечению безопасности цепи поставок?**
- ☐ **Каков их план аварийного восстановления и обеспечения непрерывности бизнеса в случае возникновения инцидента, затрагивающего вашу организацию?**
- ☐ **Как они будут информировать вашу организацию о тенденциях, угрозах и изменениях в своей организации?**

ВЫЯВЛЕНИЕ РИСКОВ В ОТНОШЕНИИ ТРЕТЬИХ ЛИЦ

Оцените киберриски в отношении третьих лиц, выполнив следующие шаги:

- ☐ **Составьте и постоянно обновляйте список всех отношений с поставщиками, а также предоставляемых каждому из них активов и данных.**
- ☐ **Проведите анализ данных, к которым каждый поставщик или третье лицо имеет доступ, следуя принципу предоставления «наименьших привилегий».**
- ☐ **Оцените уровень риска отношений с поставщиками и третьими лицами (низкий, средний, высокий), исходя из последствий получения несанкционированного доступа к их системам, для вашей организации.**
- ☐ **Начиная с поставщиков с самым высоким уровнем риска, оцените возможности обеспечения и соблюдения стандартов кибербезопасности каждого поставщика.**
- ☐ **Разработайте план регулярной оценки безопасности, в том числе оценки на рабочих объектах поставщиков с наивысшим уровнем риска и/или с большим доступом к данным клиентов.**

5_CISO Third Parties_Checklist_RU.indd 1 1/7/21 4:25 PM

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТРЕТЬИХ ЛИЦ

- ☐ Проведите тщательную комплексную проверку. Устанавливайте требования к уровню кибербезопасности для поставщиков в отношении всех предложений, контрактов, непрерывности бизнеса, процедур реагирования на инциденты и соглашений об уровне обслуживания. Согласуйте обязанности и обязательства в случае кибератак.
- ☐ Узнайте о методах обеспечения кибербезопасности финансовых организаций и других организаций, с которыми вы взаимодействуете или обмениваетесь данными, с учетом того, что ваши поставщики и третьи лица должны соблюдать требования кибербезопасности, соблюдаемые вашей организацией.
- ☐ Используйте установленные и согласованные меры для осуществления контроля соблюдения стандартов кибербезопасности вашими поставщиками.
- ☐ Проверьте, предлагают ли ваши поставщики, обрабатывающие конфиденциальные данные, двухфакторную аутентификацию, шифрование и другие меры безопасности для всех используемых ими учетных записей.
- ☐ Убедитесь, что все устанавливаемое вами программное и аппаратное обеспечение оснащено системами безопасности для защиты процессов загрузки с помощью кодов аутентификации и отклонения загрузки в тех случаях, когда коды не распознаются.
- ☐ Если вы столкнулись с продукцией поставщика, которая является поддельной или не соответствует спецификациям, организуйте работу по решению вопроса или, если это невозможно, разработайте стратегию выхода.
- ☐ Проводите ежегодную оценку контрактов с поставщиками и убедитесь, что они продолжают соответствовать вашим стратегическим указаниям и требованиям в отношении безопасности данных. Включите в контракт положения о возврате ваших активов или данных после прекращения его действия, убедитесь, что активы или данные полностью удалены на стороне поставщика, и больше не предоставляйте ему доступ к вашим системам или серверам.

ОБМЕН ИНФОРМАЦИЕЙ

- ☐ Убедитесь, что у вас есть четкие каналы связи и контакты для обмена сведениями о проблемах безопасности с поставщиками и партнерами вашей организации.
- ☐ Своевременно предоставляйте достоверную и актуальную информацию о кибербезопасности внутренним и внешним заинтересованным сторонам (в том числе организациям и государственным органам внутри и за пределами финансового сектора).
- ☐ Следите за актуальными обновлениями и новостями о том, с какими ситуациями сталкиваются другие организации, работающие с третьими лицами, в отношении угроз, уязвимостей, инцидентов и решений проблем безопасности. Для этого вступайте в такие организации, как FS-ISAC, и изучайте прочие источники информации об угрозах.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America®

5_CISO Third Parties_Checklist_RU.indd 2 1/7/21 4:26 PM