Наращивание потенциала кибербезопасности Набор инструментов для финансовых организаций

Инструкции для директора по информационной безопасности: Защита отношений с третьими лицами

Рекомендации по выбору поставщиков с учетом обеспечения кибербезопасности

Задайте потенциальным поставщикам следующие вопросы, чтобы оценить их готовность и осведомленность в сфере кибербезопасности и, следовательно, влияние на профиль риска вашей организации:

1. **Какой опыт у них имеется?** Узнайте об истории поставщика в сфере обслуживания клиентов. Обслуживали ли они ранее клиентов, схожих с вашей организацией?

2. **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?

3. **Какие из ваших данных и/или активов им необходимы для предоставления своих услуг?** Запрашивают ли они какой-либо явно нецелесообразный доступ?

4. **Как они планируют обеспечить защиту активов и данных вашей организации, находящихся в их распоряжении?**

5. **Как они управляют собственными киберрисками?** Могут ли они предоставить информацию о своей цепочке поставок?

6. **Каков план аварийного восстановления и непрерывности бизнеса** в случае инцидента, касающегося активов и/или данных вашей организации?

7. **Как они будут информировать вашу организацию?** Каков их план передачи данных о тенденциях, угрозах и изменениях в своей организации?

Выявление рисков через третьих лиц

⇒ Создайте и сохраните обновленный список всех отношений с поставщиками, а также всех предоставленных в них активов и данных.
⇒ Проверьте данные, к которым у каждого поставщика или третьей стороны имеется доступ. Убедитесь, что этот уровень доступа соответствует принципу «минимальных привилегий».
⇒ Оцените уровень риска отношений с поставщиками и сторонними организациями (низкий, средний, высокий), исходя из последствий получения несанкционированного доступа к их системам, для вашей организации.
⇒ Начиная с поставщиков с высоким уровнем риска, оцените возможности систем кибербезопасности каждого поставщика. Хорошей отправной точкой является соблюдение соответствующих стандартов. Разработайте план регулярной оценки безопасности. Возможно, вы запланируете периодические выездные оценки поставщиков с наивысшим уровнем риска и/или более открытым доступом к данным клиентов.

Управление безопасностью третьих сторон

⇒ Проведите тщательную комплексную проверку. Разработайте требования к системам кибербезопасности в запросах вашей организации на предложения, контракты, непрерывность бизнеса, реагирование на инциденты и соглашения об уровне обслуживания с поставщиками. Согласуйте обязанности и обязательства в случае кибератак.
•Узнайте о методах обеспечения кибербезопасности других третьих сторон, таких как финансовые организации, с которыми вы осуществляете операции или обмениваетесь данными. Кроме того, ваши поставщики и любые другие организации, с которыми вы обмениваетесь данными, должны соблюдать все требования к обеспечению кибербезопасности, которые соблюдает ваша организация.

⇒ 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 действенную информацию о кибербезопасности внутренним и внешним заинтересованным сторонам (включая организации и государственные органы внутри и за пределами финансового сектора).
⇒ Отслеживайте актуальные новости об опыте других организаций в работе с третьими сторонами в отношении угроз, уязвимостей, инцидентов и реакций, чтобы улучшить защиту своей организации, повысить ситуационную осведомленность и расширить возможности обучения. Членство в предоставляющих обмен информацией организациях, например, FS-ISAC, также способствует получению самых новых данных.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE