CHARLTONS

SOLICITORS

Законодательство Гонконга Май 2020

Руководство SFC для лицензированных корпораций по управлению рисками кибербезопасности в связи с удаленной работой из-за COVID-19

Руководство SFC для лицензированных корпораций по управлению рисками кибербезопасности в связи с удаленной работой из-за COVID-19

Комиссия по ценным бумагам и фьючерсам (**SFC**) выпустила циркуляр для лицензированных корпораций по управлению рисками кибербезопасности в связи с удаленной работой[1] 29 апреля 2020 года (**Циркуляр о рисках кибербезопасности SFC**) с напоминанием о том, что корпорации, имеющие лицензию SFC, должны оценить свои операционные возможности и принять соответствующие меры по управлению рисками, связанными с организацией удаленной работы. Стимулом для руководства SFC стало более широкое использование дистанционной работы в условиях пандемии COVID-19.

Дистанционная работа позволяет сотрудникам получать доступ к внутренним сетям и системам лицензированных корпораций SFC за пределами офиса. Она также предусматривает проведение встреч посредством видеоконференций. Циркуляр о рисках кибербезопасности SFC содержит неисчерпывающие примеры мер контроля и процедур, которые помогают лицензированным SFC корпорациям защищать свои внутренние сети и данные.

Параграф 4.3 Кодекса поведения SFC для лиц, лицензированных или зарегистрированных SFC, требует, чтобы лицензированные корпорации имели процедуры внутреннего контроля, а также финансовые и операционные возможности, которые, как ожидается, должны защитить их деятельность и их клиентов и других лицензированных или зарегистрированных лиц от финансовых убытков в связи с кражей, мошенничеством и другими инцидентами, профессиональными проступками или упущениями. Лицензированные корпорации, таким образом, обязаны внедрять и поддерживать методы управления и процедуры, которые они считают соответствующими масштабам и степени сложности своей деятельности.

1. SFC. 29 April 2020. Circular to licensed corporations on the management of cybersecurity risks associated with remote office arrangements. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=20EC

Удаленный доступ к внутренним сетям лицензированных корпораций SFC

Как правило, сотрудники получают удаленный доступ к внутренним сетям лицензированных корпораций SFC с помощью программного обеспечения виртуальной частной сети (**VPN**), которое обеспечивает зашифрованное соединение через Интернет, позволяя сотрудникам получать удаленный доступ к внутренним сетям, обеспечивая при этом защиту конфиденциальных данных во время передачи. Циркуляр о рисках кибербезопасности SFC отмечает недавний инцидент с обеспечением кибербезопасности, о котором сообщила лицензированная корпорация, в котором подчеркивалось, как киберпреступники могут использовать известные недостатки VPN для доступа к внутренним сетям лицензированных корпораций SFC и данным клиентов и осуществлять несанкционированные переводы средств.

Методы и процедуры контроля по снижению рисков кибербезопасности

В Циркуляре о рисках кибербезопасности SFC перечислены следующие элементы управления и процедуры как средства снижения рисков кибербезопасности удаленного доступа:

1. Внедрение качественных VPN решений, обеспечивающих надежное шифрование и два или более уровня защиты данных, передаваемых между устройствами удаленного доступа и внутренними сетями лицензированных корпораций;
2. Внедрение нескольких VPN-серверов для дополнительной защиты;
3. Своевременный мониторинг, оценка и внедрение исправлений безопасности или исправлений, выпущенных поставщиками программного обеспечения VPN. Специалисты по IT-безопасности выразили обеспокоенность тем, что организации с недостаточно защищенным программным обеспечением VPN могут быть легко взломаны, ставя под угрозу их внутренние сети;
4. Требование использования надежных паролей и двухфакторной аутентификации для входа в систему удаленного доступа сотрудниками, агентами и поставщиками услуг, особенно для доступа к привилегированным учетным записям и конфиденциальным данным;
5. Не допускать предоставления постоянного доступа третьим лицам и разрешать доступ к конкретным системам только в течение заранее определенных периодов времени;
6. Внедрение различных уровней удаленного доступа, таких как обеспечение того, чтобы компьютеры и мобильные устройства, предоставляемые лицензированными корпорациями, имели лучшие возможности, чем устройства, принадлежащие сотрудникам;
7. Внедрение мер безопасности для предотвращения несанкционированной установки аппаратного и программного обеспечения на компьютеры и устройства, предоставляемые корпорациями, имеющими лицензию SFC; а также
8. Внедрение активной сегментации сети для разделения системных серверов и баз данных на основе критичности для лучшей защиты важных и конфиденциальных данных, таких как личные данные клиентов.

Использование видеоконференцсвязи лицензированными SFC корпорациями

Время от времени сообщалось о проблемах безопасности видеоконференцсвязи. SFC предлагает, чтобы лицензированные корпорации использовали следующие методы и процедуры контроля для снижения риска нарушения безопасности и утечки важных или конфиденциальных данных:

1. Проведение обзора функций безопасности платформы видеоконференцсвязи перед использованием;

2. Требование к участникам зарегистрироваться для участия в видеоконференциях;
3. Разрешать только авторизованным пользователям участвовать в видеоконференциях, например, путем подтверждения их адресов электронной почты или использования функций «комнаты ожидания», которые дают организатору видеоконференции возможность подтвердить участие только тех, кому разрешено участвовать;
4. Проведение видеоконференций со случайным идентификатором, а не с личным идентификатором встречи;
5. Рассылка приглашений участникам через программное обеспечение для видеоконференций или другие соответствующие каналы, такие как рабочие электронные письма, и при этом неразглашение приглашений на платформах социальных сетей;
6. Включение функции пароля на платформах видеоконференций;
7. Блокировка видеоконференций после присоединения всех участников; а также
8. Обеспечение использования последней версии программного обеспечения для видеоконференций с установленными обновлениями, касающимися безопасности.

Другие меры по снижению рисков кибербезопасности при удаленной работе

SFC также рекомендует корпорациям, имеющим лицензию SFC, принять следующие меры для улучшения операционных возможностей и механизмов мониторинга удаленной работы:

1. Возможности системы: оценка адекватности и улучшение существующих IT-систем, программного обеспечения (например, удаленных компьютерных устройств, пропускной способности сети и лицензий на программное обеспечение) и аппаратного обеспечения (например, ноутбуков и мобильных устройств) для поддержки организации удаленного офиса;
2. Наблюдение и обработка нарушений: внедрить механизмы мониторинга и наблюдения для выявления несанкционированного доступа к внутренним сетям и системам, например, для проверки попыток несанкционированного доступа и обнаружения использования неутвержденных приложений. Создать и поддерживать эффективный механизм управления инцидентами и сообщения о них; а также
3. Обучение и оповещения по кибербезопасности: обеспечить соответствующее обучение по кибербезопасности для всех пользователей внутренней системы и регулярно выпускать напоминания и оповещения для клиентов по таким вопросам, как угрозы кибербезопасности и тенденции фишинга [2] и вымогательства [3] и использование безопасные сети Wi-Fi для доступа к внутренней сети и для платформ видеоконференций.

С ростом числа рабочих мест на дому в условиях пандемии COVID-19 механизмы удаленного офиса могут стать более распространенными, и корпорации, имеющие лицензию SFC, должны оценить и пересмотреть свои средства контроля и меры кибербезопасности, чтобы убедиться, что они соответствуют применимым законам и правилам.

SFC приглашает лицензированные корпорации обращаться к своим контактным лицам, если у них есть какие-либо вопросы по тому, что содержится в циркуляре.

2. Фишинг происходит, когда хакеры пытаются обмануть пользователей, заставляя их совершать «неправильные поступки», такие как переход по плохой ссылке, которая приведет к загрузке вредоносных программ, или перенаправление их на фальшивый веб-сайт.
3. Тип вредоносного ПО, которое шифрует файлы, что делает их недоступными и требует выкуп за их расшифровку.

CHARLTONS

Лучшая юридическая бутик-компания по сопровождению сделок 2017 года
по версии Asian Legal Business Awards

Офис в Гонконге
Dominion Centre
12th Floor
43-59 Queen's Road East
Hong Kong
Тел: + (852) 2905 7888
Факс + (852) 2854 9596

www.charltonslaw.ru