

COVID-19

Что могут сделать CIO и CISO, чтобы помочь

Март 2020

Обеспокоенность по поводу масштабов и воздействия пандемии COVID-19 растет, что заставляет организации обдумывать свои ответные действия, которые им необходимо предпринять для поддержания своего бизнеса. ИТ-директор и CISO играют жизненно важную роль в обеспечении того, чтобы организация могла функционировать при реализации мер по сдерживанию пандемии.

Может ли ваш бизнес эффективно функционировать благодаря удаленной работе?

Вы должны быть уверены, что ваш бизнес может работать удаленно и гибко, и что сотрудники осведомлены об этой возможности. Это может потребовать пересмотра решений о правах доступа и рисков, связанных с удаленной работой.

Вопросы к рассмотрению:

- Масштабировали ли вы свои VPN-концентраторы, порталы и шлюзы для работы с большим количеством людей, работающих удаленно?
- Рассматривали ли вы потенциальных ключевых поставщиков и подрядчиков, которым потребуется доступ, что приведет к дополнительной нагрузке?
- Протестировали ли вы инфраструктуру, чтобы выяснить, сможет ли она справиться с ожидаемой нагрузкой?
- Есть ли единая точка отказа в инфраструктуре, и можете ли вы обеспечить дополнительную устойчивость?
- Нужно ли вам ослабить контроль доступа или предоставить дополнительные учетные записи для удаленного входа?
- Достаточно ли ресурсов и компетенций службы поддержки для обработки любых запросов от пользователей, которые не могут войти или не знакомы с удаленной работой?
- Если сотрудникам требуется доступ к ноутбукам для удаленной работы, имеется ли достаточное количество ноутбуков или их можно приобрести и установить для удовлетворения спроса, и как распределить приоритеты?
- В случаях, когда количество оборудования ограничено, рассматривали ли вы основные услуги и разделение доступа к ним с помощью альтернативных решений доступа (например, O365 и One Drive) по сравнению с собственными приложениями?
- Рассматривали ли вы возможность вносить в белый список только определенные приложения в течение этого периода и блокировать все второстепенные услуги?
- Есть ли у вас ограничения на видео- и аудиоконференции, и можете ли вы сделать что-нибудь для масштабирования этой инфраструктуры?
- Нужно ли вам рассмотреть альтернативные облачные решения для конференц-связи и дистанционной работы?
- Все ли сотрудники имеют необходимые ссылки для доступа к организации конференций, доступны ли учебные материалы, следует ли вам установить телефон доверия?
- Можете ли вы удаленно управлять своей службой поддержки, если персонал службы поддержки вынужден работать из дома?
- Подготовили ли вы простые руководства для сотрудников по ключевым вопросам, связанным со службой поддержки:
 - Как мне войти?
 - Как я могу изменить свой пароль?
 - Как я могу получить доступ к ключевым сервисам?
 - Как я могу получить помощь от службы поддержки?
 - Кто мои ключевые контакты в кризисных ситуациях?

Можете ли вы масштабировать цифровые каналы для удовлетворения спроса?

Ограничения на поездки и распространение вируса могут привести к появлению новых моделей спроса и увеличению трафика на цифровых каналах.

- Все больше клиентов могут рассчитывать на операции с вами по цифровым каналам. Можете ли вы масштабировать эти системы и услуги для удовлетворения меняющегося спроса?
- Как вы будете отслеживать нагрузку и производительность, и кто может принимать решения о масштабировании нагрузки или создавать динамический выбор приоритетов, если пропускная способность является проблемой?
- Понимаете ли вы, как восприятие клиентов может измениться, если системы перегружены?
- Зависимы ли вы от ключевых центров обработки вызовов, и если эти центры обработки вызовов закрыты или недоступны, могут ли клиенты взаимодействовать с вами по другим каналам?
- Есть ли возможность разрешить персоналу колл-центра работать удаленно или перевести их в другое место?
- Рассматривали ли вы взаимодействие между колл-центрами и службами поддержки/услуг и влияние каких-либо внешних соглашений?
- Обсуждали ли вы договоренности с ключевыми поставщиками этих услуг и как они будут определять ваши потребности по сравнению с потребностями других клиентов?

Зависимы ли вы от ключевого ИТ-персонала?

К сожалению, сотрудники могут заразиться или оказаться неспособными к перемещениям или выполнять обязательства по уходу за семьей; Вы должны планировать посещаемость своих сотрудников.

- Что произойдет, если ключевой ИТ-персонал (включая подрядчиков) не сможет выйти на работу или заболел - зависите ли вы от небольшого числа ключевых людей?
- Как можно уменьшить эту зависимость, например, гарантируя наличие процедур экстренного реагирования, чтобы другие администраторы могли получить доступ к критически важным системам?
- Что насчет команды безопасности? Кто является ключевыми лицами, и если CISO недоступен, то кто будет отчитываться о состоянии безопасности и о приемлемых рисках для фирмы?



Что будет, если произойдет сбой в центре обработки данных?

- Вирус может повлиять и на центры обработки данных. Положительный тест может привести к эвакуации и глубокой очистке здания. Нарушение транспортной инфраструктуры может помешать доступу, а персонал центра обработки данных может оказаться неспособным работать.
- В случае эвакуации одного из ваших центров обработки данных, есть ли у вас планы аварийного восстановления для устранения сбоев и проверяли ли вы эти планы?
- Как быстро вы можете перейти на альтернативный ресурс и кто управляет этим процессом?
- Зависимы ли вы от ключевых лиц (включая поддержку подрядчиков) в работе центра обработки данных, и как вы можете управлять этой зависимостью?

Можете ли вы масштабировать возможности облака?

К облачным сервисам могут предъявляться дополнительные требования, требующие масштабирования доступной вычислительной мощности, что может повлечь дополнительные расходы. Отдельные услуги могут показывать снижение спроса.

- Можете ли вы отслеживать спрос на услуги облачных вычислений и эффективно управлять распределением ресурсов?
- Приняли ли вы меры для покрытия любых дополнительных расходов, которые могут возникнуть из-за масштабирования или предоставления других облачных услуг?

Зависимы ли вы от конкретных поставщиков?

Ваши поставщики и партнеры будут находиться под давлением, и их деятельность также будет нарушена.

- Кто ваши основные поставщики и как вы будете предоставлять услуги, если они не смогут работать?
- Есть ли какие-либо шаги, которые вы могли бы предпринять сейчас, чтобы уменьшить эту зависимость, включая использование ресурсов вашей команды?
- Обсуждаете ли вы последствия со своими ключевыми поставщиками, и есть ли у вас правильные точки соприкосновения с этими поставщиками?
- Определили ли вы, какие поставщики ИТ могут оказаться под финансовым давлением, и какова будет ваша альтернативная стратегия поиска поставщиков, если они потерпят неудачу?

Что будет, если произойдет инцидент по информационной безопасности?

Группы организованной преступности используют страх перед COVID-19 для проведения целенаправленных кампаний по фишинг-атакам и созданию поддельных веб-сайтов, что ведет к повышенному риску инцидента с кибербезопасностью.

- Сообщали ли вы сотрудникам, где получить доступ к достоверной информации о пандемии COVID-19 и реакции вашей фирмы на COVID-19?
- Предупреждали ли вы персонал о повышенном риске фишинговых атак с использованием COVID-19 в качестве прикрытия?
- Если вы зависите от альтернативных систем или решений, в том числекупаемых в качестве облачных сервисов, кто будет решать инциденты по безопасности, связанным с этими системами?
- Нужно ли вам изменить подход к операциям безопасности во время пандемии, включая меры по мониторингу событий безопасности?

Что произойдет, если произойдет ИТ-инцидент?

Несмотря на то, что COVID-19 доминирует в новостях, вы все равно должны знать о возможности сбоя ИТ-систем с учетом меняющихся требований к вашей инфраструктуре или возможности кибератаки.

- Сможете ли вы дистанционно координировать инциденты, и есть ли у вас необходимые конференц-залы и доступ к процессам и руководствам по управлению инцидентами?
- Есть ли у вас виртуальная боевая машина на случай, если физический доступ ограничен?

- Зависите ли вы от ключевых лиц в реагировании на инциденты? Если да, что можно сделать, чтобы уменьшить эту зависимость?
- Как меняется структура управления кризисными ситуациями / реагированием на инциденты, если менеджеры по ключевым инцидентам / ответственные сотрудники по восстановлению недоступны?
- Уверены ли вы, что ваши резервные копии актуальны, и что в худшем случае вы сможете восстановить важные данные и системы?
- Как бы вы справились с частыми инцидентами, когда большая часть вашей команды работает дома?

Насколько эффективно вы используете свои ресурсы?

Вам придется работать с ограниченным числом сотрудников - необходимо понимать приоритетные задачи для вашей команды.

- Определили ли вы приоритеты деятельности своей команды, есть ли задачи, которые вы можете отложить и освободить сотрудников для планирования действий при ЧС?
- Есть ли у вас возможность доступа к денежным средствам на случай ЧС, если вам нужно быстро найти оборудование или дополнительного подрядчика / специалиста?
- Если на вас оказывают давление с целью сокращения операционных расходов, ясно ли вам, какие расходы должны быть сохранены?

Подаете ли вы пример?

Вы по-прежнему остаетесь Руководителем, и ваша команда будет обращаться к вам за руководством и поддержкой.

- Удалось ли вам убедиться, что ваша команда внедряет необходимые меры предосторожности, в том числе предлагает своим сотрудникам возможность дистанционной работы?
- Есть ли у вас актуальные контактные данные всей вашей команды? Знает ли ваша команда, к кому обращаться в чрезвычайной ситуации?
- Моделируете ли вы поведение, которое вы ожидаете от своей команды, и что произойдет, если вы станете недееспособным? Кто заменит вас?

Не бойтесь и удачи.

Если у вас есть какие-либо вопросы или вы хотите получить дополнительную консультацию, свяжитесь с нами.

Контакты

Константин Аушев

Директор

Группа консультирования в области ИТ и кибербезопасности

T: +7 727 298 08 98

E: kaushev@kpmg.kz

kpmg.kz



Информация, содержащаяся в настоящем документе, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации. Хотя мы неизменно стремимся представлять своевременную и точную информацию, мы не можем гарантировать того, что данная информация окажется столь же точной на момент получения или будет оставаться столь же точной в будущем. Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и тщательного анализа конкретной ситуации.

© 2020 «КПМГ Такс энд Эдвайзори», компания, зарегистрированная в соответствии с законодательством Республики Казахстан, член сети независимых фирм KPMG, входящих в ассоциацию KPMG International Cooperative ("KPMG International"), зарегистрированную по законодательству Швейцарии. Все права защищены.

Наименование KPMG и логотип KPMG являются зарегистрированными товарными знаками или торговыми марками ассоциации KPMG International.

Переведено с разрешения KPMG International.