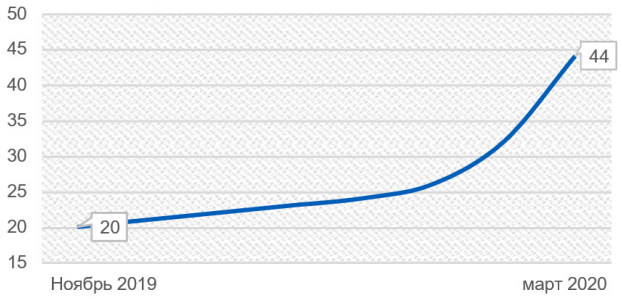
Обеспечение организации совместной работы и видеоконференций

16 апреля 2020

В результате текущего кризиса многие компании оказались в ситуации, когда сотрудникам компаний приходится работать удаленно, а самим компаниям применять новые методы работы. Инструменты совместной работы могут стать действенным способом объединения членов команды и эффективного взаимодействия. Однако их применение повышает подверженность компаний новым киберрискам.

Несмотря на то, что использование инструментов для проведения видеоконференций уже было на подъеме, режим самоизоляции, введенный по всему миру, придал ускорение развитию данной тенденции. В 2019 году компания Gartner представила прогноз, согласно которому к 2024 году около 75 % рабочих совещаний будут проходить в режиме онлайн, хотя в нынешней ситуации мы должны признать, что данная цифра уже превышена. Например, число ежедневных активных пользователей программы Microsoft Teams удвоилось - с 20 миллионов в ноябре 2019 до 44 миллионов в марте 2020 года.

Число ежедневных активных пользователей программы Microsoft Teams (в миллионах)



Для компаний это может создать ряд проблем не только в плане способов организации работы, но также в плане защиты данных. Мы видим, что компании прилагают все усилия, чтобы удовлетворить потребности своих работников, часто очень срочные, в использовании решений для удаленной работы, при этом обеспечивая безопасность применения таких ИТ-решений.

Наиболее значимые риски

— **Риск утечки данных**: Утечка данных — это инцидент в системе информационной безопасности, который происходит в результате случайного или преднамеренного раскрытия информации посторонним лицам. В инструментах совместной работы такое может произойти при неэффективном управлении доступом к рабочим «зонам», или когда общими файлами легко обмениваться или загружать без всяких ограничений. Это также может случиться, если включена функция «демонстрации экрана» и на нем отображаются конфиденциальные документы.
Утечка данных может привести к раскрытию критически важной для компании информации, или даже к штрафу за нарушение норм GDPR в случае утечки персональных данных. Кроме того, легкость организации онлайн-совещаний влечет за собой дополнительные риски. Если виртуальное пространство для проведения рабочих встреч не было должным образом сконфигурировано, то посторонние лица могут получить доступ к такой онлайн-встрече. Данный риск особенно важен для совещаний с большим количеством участников, поскольку в этом случае существует возможность для посторонних лиц остаться незамеченными.

— **Перегруженность сети**: С увеличением числа совещаний, проводимых в режиме видеоконференции, дополнительные технические требования предъявляются к пропускной способности сети. Это особенно касается тех случаев, когда большое количество сотрудников подключается к видеоконференции через серверы или сеть VPN компании. Это может привести к недоступности файлов или к сбоям в сети во время совещания.

Выход из тени – управление теневыми ИТ

Облачные сервисы, включая инструменты совместной работы, можно относительно легко приспособить для работы, не получив одобрения отделов ИТ, безопасности или закупок, или не поставив их в известность. Работники способны создавать (платные) аккаунты, не проинформировав свою организацию, с возможностью обмениваться конфиденциальной информацией за пределами организации. Это может привести к ситуации, когда конфиденциальные документы хранятся в облачной среде без ведома организации, и при этом отсутствует надлежащий уровень безопасности и контроля. Такое применение информационных технологий часто именуется как «теневые информационные технологии».

Большинство работников, особенно во времена неопределенности, стремятся продолжать работать максимально эффективно. При отсутствии четких указаний или реальной альтернативы работники могут взять вопрос выбора решения в свои руки.

Кроме того, многие риски не только никуда не исчезают, они еще и увеличиваются по причине отсутствия должного контроля.

Практические рекомендации по обеспечению безопасности совместной работы при удаленном режиме

Наряду с общими рисками, существуют и общие принципы обеспечения безопасного применения инструментов совместной работы. Далее представлены некоторые из выбранных нами примеров передовой практики применения наиболее популярных инструментов организации совещаний и конференций, как в целом, так и в конкретных случаях, с обеспечением безопасности совместной работы.

Общие рекомендации

В то время как некоторые настройки и практические рекомендации могут относиться только к конкретным инструментам, существуют и такие, которые носят общий характер. Например:

- убедитесь в том, что программа по организации видео- конференций обеспечивает шифрование данных, направляемых (передаваемых) в сети, и, предпочтительно, сквозное шифрование;
- обеспечьте включение и применение VPN для незашифрованного сетевого трафика;
- постоянно обновляйте вашу программу по организации видео-конференций;
- рассмотрите возможность снижения качества видео-картинки (например, 240p/360p/480p) для предотвращения перегрузки сети;
- обеспечьте проведение многофакторной проверки подлинности во всех устройствах и приложениях.

Microsoft Teams

Microsoft Teams включает набор стандартных конфигураций безопасности для защиты конечных потребителей и данных, которые они хранят и пересылают. Тем не менее, не будет лишним проверить, включены ли эти настройки безопасности. Ниже представлена информация относительно комплексных конфигураций безопасности, которые можно проверить/запустить:

- Современная проверка подлинности (Modern Authentication -MA): метод управления идентификацией пользователей, обеспечивающий более безопасный способ проверки подлинности и предоставления доступа пользователям. Данная функция запускается по умолчанию.
- Многофакторная проверка подлинности (Multi-Factor Authentication - MFA): метод проверки подлинности, при котором пользователю предоставляется доступ только после успешного прохождения двух или более проверок подлинности, к которым относятся одноразовый пароль (OTP), токены, коды SMS и т.д.
- Единый вход (Single-Sign-On - SSO): единый вход обеспечивает безопасность и удобство при входе пользователей в приложения. Для того чтобы у пользователей была возможность использовать данную функцию, они должны быть зарегистрированы либо в Azure Active Directory (Azure AD), либо в Hybrid Azure AD.

Принимая во внимание тот факт, что сервис Teams - это не просто инструмент для проведения видеоконференций, большое значение придается обучению сотрудников тому, каким образом необходимо обмениваться файлами на базе этой платформы. Например:

- не обмениваться конфиденциальной информацией посредством каналов, предусматривающих гостевой доступ, и использовать приложение Microsoft Azure Information Protection (с DLP) для обеспечения большего уровня безопасности и контроля;
- обеспечить отсутствие скрытого доступа к файлам через основной сайт SharePoint;
- использовать виртуальный зал собраний для встреч с внешними пользователями.

Cisco WebEx

Cisco WebEx обладает большим количеством настроек безопасности, которые необходимо установить. Несмотря на то, что некоторые настройки установлены по умолчанию, желательно просмотреть их все, чтобы обеспечить оптимальный уровень безопасности для ваших сотрудников. Опираясь на передовой опыт Cisco, мы рекомендуем активировать следующие функции:

- Использование графических файлов, которые прошли процедуру аутентификации.
- Шифрование данных при передаче и хранении.
- Безопасная разработка программного обеспечения с использованием приложения Cisco «Development Lifecycle (CSDL)».
- Контролируемое включение настроек безопасности на базе продукта Cisco «Product Security Baselines (PSB)».
- Авторизация пользователя с использованием OAuth2.
- Обеспечение настроек безопасности и соответствия требованиям, установленным в администраторе Webex Control Hub и Webex Teams.

Проведение собраний на базе онлайн-платформы Zoom

Большое количество настроек параметров для программного обеспечения влечет потенциальные ошибки в обеспечении безопасности. Ниже приведен список рекомендаций, основанных на передовых практиках работы:

- вводить пароли для участия во всех виртуальных собраниях;
- активировать функцию «waiting room» для предотвращения подключения неизвестных участников;
- активировать функцию «wait for host to join» для того, чтобы убедиться в подключении к совещанию только приглашенных участников;
- закрыть виртуальный зал после того, как все участники собрались;
- обеспечить допуск к совещаниям только зарегистрированных пользователей или пользователей проверенных доменов;
- не использовать идентификатор личных конференций для общих собраний.

Не так давно Zoom столкнулась с проблемами, связанными с обеспечением безопасности и конфиденциальности данных клиентов. Поэтому, прежде чем начать использование платформы следует обратить внимание на результаты расследования и дальнейшие изменения.

Управление теневыми ИТ

Важно отметить, что все это практические рекомендации для обеспечения безопасной работы с использованием инструмента, санкционированного организацией. Как было указано выше, использование работниками теневых ИТ-ресурсов в организации может по-прежнему представлять угрозу. Одной из наиболее важных мер, предпринимаемых в этом отношении, является использование приложения «Брокер безопасного доступа в облако» (Cloud App Security Broker (CASB)). С помощью CASB можно обнаружить использование несанкционированных программ для проведения видеоконференций и предусмотреть упреждающие меры безопасности.

При использовании CASB в первую очередь важно понять, почему работники используют те или иные программы. Хотя блокирование программы может представляться самым простым решением, это может привести к тому, что всплывет другой теневой ИТ-ресурс. Мы бы рекомендовали:

— конфигурировать CASB для определения наиболее часто используемых программ;
— обсудить с работниками причины, по которым они используют эти инструменты;
— определить дальнейших действий на основе полученных результатов.

Действия могут варьироваться от проведения обучения тому, какие возможности предоставляют санкционированные программы, введения дополнительных функциональных возможностей в программы компании до полного блокирования теневых ИТ-программ. Результатом таких действий также могло бы стать выявление недостатков программ, дополнительных функциональных требований для организации эффективной работы в удаленном режиме.

Перспективы на будущее

Хотя для многих внедрение инструмента организации совместной работы было экстренной мерой, скорее всего, такие формы работы станут нормой. Поэтому важно выбрать для применения инструмент с перспективой на долгосрочный успех, и мыслить категориями не только недель или месяцев, но и лет. Что случится с данными, если вы решите сменить инструменты? Как работники должны обрабатывать данные? Какие инструменты мы могли бы внедрить для повышения эффективности?

Опыт KPMG, а также мировые передовые практики помогут вам ответить на все вопросы, связанные с безопасностью совместной работы дистанционных сотрудников.

Контакты:

Константин Аушев
Директор группы консультирования
в области ИТ и кибербезопасности
KPMG в Казахстане и Центральной Азии
T: +7 (776) 215 16 73
E: kaushev@kpmg.kz

www.kpmg.kz