CYBER READINESS
INSTITUTE

ЧАВО об облаке:
улучшение кибербезопасности для удаленных сотрудников

Вследствие пандемии COVID-19 сотрудники большинства компаний перешли на удаленную работу. Удаленная работа создает новые риски кибербезопасности, особенно в связи с тем, что сотрудники получают доступ к информации новыми способами, в том числе через облако.

Настало время оценить, как ваша организация использует облако. Облако имеет множество возможностей, которые могут помочь сделать удаленную работу более практичной, эффективной и безопасной. Этот материал предназначен для того, чтобы помочь высшему руководству малых и средних предприятий (МСП) ознакомиться с терминологией облачных технологий и понять основы того, как облако может повысить кибербезопасность удаленных сотрудников.

Я много слышал об «облаке», но какие основные сведения мне нужно знать?

«Облако» — это группа компьютеров (известных под общим названием «серверы»), которыми владеет и управляет компания (обычно именуемая «поставщик облачных услуг» или «CSP»), предоставляющая вам ПО или хранилище. Клиент или компания лицензируют использование ПО и/или хранилища, как правило, ежемесячно, при этом затраты меняются в зависимости от использования, аналогично ежемесячным расходам на коммунальные услуги.

CSP отвечает за эксплуатацию, техническое обслуживание и модернизацию компьютерного оборудования (например, хранилища, серверы), которое физически расположено в центре обработки данных, а не на территории клиента. Как клиент вы платите за использование их услуг.

guide@cyberreadinessinstitute.com

Какие общие термины я услышу, когда буду говорить с людьми об облаке?

ДАТА-ЦЕНТРЫ

Представьте себе большие склады, заполненные компьютерами, подключенными к Интернету и известными под общим названием «серверы». Когда вы как клиент используете службу (например, Outlook), вы, по сути, арендуете как пространство (хранилище), так и услуги (электронную почту) для написания, чтения и отправки электронных писем.

СЕРВЕРЫ

Набор компьютеров и оборудования, подключенных к Интернету, которые предоставляют какие-либо услуги, хранилища или другие функции.

ПОСТАВЩИКИ ОБЛАЧНЫХ УСЛУГ (CSPs)

Компании, которые предоставляют услуги вам как клиенту. Некоторыми хорошо известными примерами являются Microsoft, Google или Amazon Web Services (AWS).

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК УСЛУГА (SAAS) (произносится как «сэсс»)

CSP размещает на своих серверах программное обеспечение, доступ к которому ваша компания получает через Интернет. Компании обычно лицензируют использование многих видов ПО таких, как электронная почта (Google Mail), обработка текстов (Microsoft Word), электронные таблицы (Google Таблицы), бухгалтерский учет (QuickBooks) и управление продажами (Salesforce). Это наиболее распространенный способ использования облака для малого бизнеса, который требует минимального обслуживания со стороны клиента.

ПЛАТФОРМА КАК УСЛУГА (PAAS) (произносится «паз»)

CSP предоставляет инфраструктуру (например, операционную систему такую, как Windows) и программное обеспечение, которое позволяет вам разрабатывать, управлять и использовать настраиваемые приложения (например, приложения для управления запасами или мобильные заказы клиентов).

ИНФРАСТРУКТУРА КАК УСЛУГА (IAAS) (произносится как «ай-эз»).

Поставщик облачных услуг физически размещает компоненты, которые традиционно находились в «локальном» центре обработки данных, включая серверы, хранилище, сетевое оборудование и серверное ПО.

Каковы общие преимущества переноса операций и информации в облако с точки зрения безопасности?

CSP рассматривают безопасность как основную бизнес-функцию и признают, что доверие является фундаментальной частью их бизнес-модели. Они уделяют особое внимание постоянному обновлению предоставляемых услуг и инфраструктуры, чтобы гарантировать безопасные решения для своих клиентов. Их опыт и постоянное внимание к безопасности позволят вам извлечь пользу.

Физическая инфраструктура (напр. серверы, маршрутизаторы, сетевые устройства) размещается в дата-центрах, которыми владеет и обслуживает CSP. Как правило, это а) снижает затраты, связанные с содержанием, включая плату за создание и техническое обслуживание, а также б) предоставляет специальные ресурсы для защиты места от проблем с физической безопасностью.

CSP обеспечивают экономию за счет масштаба, предоставляя вам доступ к ресурсам и услугам, превосходящие возможности, которые может задействовать любой отдельный пользователь. Например, CSP объединяют ресурсы, чтобы лучше понимать последние кибератаки, которые используют хакеры, и применять решения для защиты своих услуг и ваших данных.

Большинство авторитетных облачных провайдеров четко определяют, какие меры безопасности они применяют и каковы ваши обязанности, когда дело касается использования их услуг. Если они этого не делают или если эта информация не поступает от интересующего вас поставщика облачных услуг, вы можете рассмотреть другого поставщика.

При использовании облака каковы текущие обязанности моей организации в области кибербезопасности?

Ваша основная ответственность заключается в поведении ваших сотрудников. Вы несете ответственность за их обучение тому, как предотвращать проблемы и что делать в случае их возникновения. Вы должны убедиться, что они понимают, что киберготовность является приоритетом для вашей компании.

Существуют основные принципы, которые необходимо понимать, когда речь заходит об ответственности вашей организации за безопасность при использовании CSP:

- Во-первых, аутсорсинг услуг, функций или инфраструктуры CSP не означает, что вы передаете на аутсорсинг свою ответственность за безопасность. Простой пример, который применим практически ко всем, — осведомленность и доступ сотрудников. Знают ли они, как обнаруживать подозрительные электронные письма? Ограничивает ли ваша организация доступ сотрудников к программному обеспечению (например, бухгалтерским приложениям) в зависимости от потребностей и их обязанностей?
- Во-вторых, злоумышленники сосредотачивают свои усилия на том, чтобы обмануть людей (известно как «фишинг»), получить несанкционированный доступ. Более 90% удавшихся взломов начинаются с того, что кто-то нажимает на подозрительную ссылку в электронной почте. Обучение сотрудников кибербезопасности имеет большое значение, включая соблюдение правил «кибергигиены», например, не переходить по ссылкам от неизвестных отправителей или проверять электронные письма менеджеров, которые запрашивают конфиденциальную информацию.
- В-третьих, ответственность за то, что происходит с данными, почти всегда лежит на клиенте. Например, ответственность за утечку плохо защищенных конфиденциальных финансовых данных клиентов (например, информации о кредитных картах), которые загружаются в CSP, лежит на клиенте, а не на CSP. Репутационные, юридические, финансовые последствия и влияние на соблюдение нормативных требований, среди прочего, также являются ответственностью клиента.

Как переход в облако повышает нашу киберготовность, связанную с управлением идентификацией пользователей (например, паролями и аутентификацией)?

Многие поставщики облачных услуг имеют команды, занимающиеся кибербезопасностью, и могут реагировать на инциденты в режиме реального времени, определяя, когда возникают проблемы, и предпринимать шаги для сокращения ущерба. Один крупный поставщик облачных услуг получает более 200 миллионов попыток входа в систему в день. Он может быстро узнать, когда ваши пароли находятся под угрозой новой атаки, и принять меры, чтобы предотвратить ее влияние на вас или ваших пользователей.

Как переход в облако повышает киберготовность, связанную с поддержанием актуальности программного обеспечения?

Поддержание ПО в актуальном состоянии является огромным преимуществом для клиентов и часто является ключевым преимуществом для поставщиков облачных услуг, особенно при развертывании решения SaaS или PaaS. Когда вы переходите на облачный сервис, поставщик несет ответственность за поддержание текущих обновлений ПО без необходимости предпринимать какие-либо действия.

Однако у этой функции может быть обратная сторона, поскольку пользователи могут быть не готовы адаптироваться к новым функциям так же быстро, как их внедряют облачные компании. Если это относится к вашей компании, вы должны спросить, есть ли возможность отложенного обновления для вашей лицензии на облачное программное обеспечение. Помните, что сотрудники могут по-прежнему нести ответственность за обновление ПО на своем компьютере, планшете или телефоне.

Как переход в облако повышает нашу киберготовность, связанную с предотвращением фишинговых сообщений электронной почты?

С фишингом трудно бороться, поскольку он использует обман социальной инженерии (иногда специально адаптированный для отдельных лиц, называемый адресным фишингом) для входа в приложение или доступа к чувствительным данным (например, к информации о логине и пароле).

Тем не менее, поставщики облачной электронной почты могут быстро узнавать о фишинговых атаках и реагировать на них, как только о них становится известно. Поставщики облачной электронной почты могут предоставлять услуги, помогающие сообщать об известных фишинговых сообщениях и предотвращать их получение вашими сотрудниками. В конечном счете, лучшая линия защиты — это хорошо обученный пользователь, который знает, как выглядят фишинговые электронные письма и что делать (и не делать!), когда он их видит.

Использование поставщика облачных услуг повышает киберготовность вашей компании в управлении

Как переход в облако повышает киберготовность, связанную с использованием USB-накопителей и съемных носителей?

Переход в облако представляет собой значительное улучшение, поскольку для использования облачного ПО не требуются съемные носители. Все, что нужно для облака, — это пользователь с логином, браузером и подключением к Интернету. USB-накопители и съемные носители становятся в значительной степени неактуальными, пока вы обучаете своих пользователей тому, как использовать облако для хранения, передачи и доступа к необходимой им информации.

Вы по-прежнему будете нести ответственность за обеспечение безопасности на физических устройствах, которые поддерживают съемные носители и могут помешать клиенту получить доступ к услугам. Преимущество, однако, заключается в том, что хотя отдельное устройство (например, настольный компьютер) может быть скомпрометировано USB-атакой, сервисы «живут» в облаке и доступны с незараженного устройства. Это мощная облачная функция, которая помогает обеспечить непрерывность вашего бизнеса.

Как поможет облако , если у вас произойдет киберинцидент?

Поставщики облачных услуг тратят много времени и денег на то, чтобы их услуги не были отключены в результате киберинцидентов. CSP предлагают программные инструменты, которые могут помочь вам изолировать основную причину (например, службы регистрации событий, подозрительную активность) инцидента, чтобы уменьшить вероятность его повторения. Дата-центры CSP также имеют надежные средства физической безопасности, защиты электропитания и предотвращения возгорания, поэтому вы можете быть уверены, что реальная физическая ИТ-инфраструктура надежно защищена.

Наши сотрудники используют свои смартфоны для работы. Каким образом использование облачных сервисов помогает снизить связанный с этим риск кибербезопасности?

Вы должны создать политику безопасности для мобильных устройств, которая будет применяться ко всем пользователям независимо от того, какое устройство они используют. Облако обеспечивает одинаковые общие преимущества безопасности для сотрудников независимо от того, используют ли они свой смартфон или другое устройство. Важно помнить, что смартфоны представляют собой наибольшее количество видов угроз, и каждая компания должна быть требовательной в отношении в своей политики безопасности мобильных устройств.

Об Институте киберготовности

Институт киберготовности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов с целью обмена ресурсами и знаниями, которые используются для разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Самостоятельная онлайн-программа киберготовности доступна на китайском, английском, французском, испанском, португальском, арабском и японском языках. Если у вас есть вопросы, комментарии, или вы хотите поделиться историей успеха, свяжитесь с нами (guides@cyberreadinessinstitute.org).

Как расставить приоритеты в вопросе о том, что переместить в облако?

Нет универсального ответа на все вопросы. В большинстве организаций существует так называемая «гибридная» среда, в которой используется сочетание облачных сервисов с самоуправляемыми локальными решениями (например, компания может использовать свою сетевую настройку для небольшого офиса и службу электронной почты, предоставляемую CSP). Вот некоторые соображения:

- Подключены ли ПО или служба напрямую к Интернету? Многие компании переносят свою электронную почту и приложения для управления взаимоотношениями с клиентами (CRM) в облако, поскольку это критически важные приложения, серверы которых традиционно требуют постоянного обслуживания и содержания. Большинство компаний сегодня также получает свое базовое программное обеспечение для бизнеса (т. е. обработку текстов, электронные таблицы, бухгалтерский учет) по подписке SaaS.
- Насколько это будет сложно или вызовет нарушения? Некоторые функции намного проще перенести, чем другие. Например, перенести электронную почту или файловое хранилище в облако несложно. Однако перенос систем таких, как расчет заработной платы или бухгалтерский учет, которые включают в себя большое количество исторических данных, может быть гораздо сложнее.
- Каковы относительные затраты? Сравнивая затраты на использование облака и самостоятельное выполнение, не забудьте также учесть время и затраты на локальное выполнение. Это не просто стоимость оборудования и ПО — это время для настройки, обновления, обслуживания и устранения неполадок вашей системы.
- Оцените аспекты укрепления безопасности при использовании облака. Подумайте о возможных сбоях в работе вашего бизнеса, а также о потере вашей информации, особенно самых ценных данных.

Как переход в облако повлияет на наш текущий рабочий процесс, и что должны делать наши сотрудники?

Ответ на этот вопрос будет зависеть от того, что вы перемещаете в облако. Перенос электронной почты в облако обычно приводит к очень небольшим изменениям, в то время как перенос вашего программного обеспечения для бухгалтерского учета в облако может привести к серьезным нарушениям, требующим управления изменениями для ваших пользователей и организации.

Каково влияние использования облака на то, как я взаимодействую со своими поставщиками и клиентами?

Простым ответом будет: «в зависимости от обстоятельств». Компании используют облако для достижения разных целей в самых разных проектах. Однако переход в облако часто экономит время и деньги, которые вы бы потратили на ИТ-ресурсы (серверы, сети и т. д.). В большинстве случаев использование облака упростит и сделает более безопасным передачу или совместное использование информации с вашими клиентами и поставщиками.