как гарантировать безопасность ваших облачных сервисов

если все делать правильно, то облака ничуть не уступают в надежности традиционным системам

По прогнозам, в ближайшие два года популярность облачных сервисов вырастет в два раза. Ваша компания, скорее всего, уже использует облака — и активнее, чем вы думаете. Поэтому важно как следует защитить ваши данные.

«Защищать облачную инфраструктуру намного сложнее, чем обеспечивать безопасность обычных ИТ-систем. Раньше было достаточно физической защиты устройств, на которых хранились данные», — предупреждает компания 451 Research в своем докладе «Проблемы перехода на облачные решения», заказанном Orange Business Services.

Угроза кибератак абсолютно реальна. Согласно последнему отчету PwC «О проблемах информационной безопасности в современном мире», за последний год 69% британских компаний стали жертвами кибератак, и некоторые из них обернулись потерей денег.

В стремлении взломать корпоративные ИТ-системы злоумышленники проявляют чудеса изобретательности. Существует три главных вида угроз:

- *Внешние угрозы*: атаки киберпреступников, нацеленные на ваши системы или системы ваших главных партнеров, через незащищенные и не контролируемые вами точки доступа.
- *Внутренние угрозы*: **предательство сотрудников**, ненадежные системы безопасности, хранение информации на общедоступных облачных сервисах и пр.
- *Операционные угрозы*: потеря данных при переходе от одного провайдера к другому или при переносе информации с устаревшей системы на новую.

Руководствуйтесь тремя главными факторами: конфиденциальность, сохранность, доступность. Если вы не располагаете достаточными ресурсами, **сконцентрируйте усилия на самых ценных, конфиденциальных или критически важных для бизнеса данных**. Это будет не только полезно, но и ускорит возврат инвестиций.

Очень важно также, где хранятся ваши данные и через какие страны передаются: то есть **законы какой страны их охраняют**? Как эти законы могут повлиять на ваш бизнес?

советы по обеспечению безопасности

Матрица средств контроля за облаками, разработанная Альянсом по безопасности облаков (Cloud Security Alliance), поможет вам выбрать подходящего провайдера. Самое меньшее, что нужно сделать, — **обязательно** убедиться, что ваш провайдер отвечает стандартам безопасности ISO 27001 или Сертификату STAR Альянса по безопасности облаков. Это означает, что информация будет надежно хранится на серверах провайдера, и он обеспечит защиту от атак.

Не менее важно убедиться, что все системы облачной инфраструктуры и звенья логистической цепочки, в том числе системы партнеров вашего провайдера, надежно защищены. Обязательно **следите за всем**, что представляет хоть малейшую угрозу вашим частным, публичным или гибридным облакам.

Где бы ни хранились ваши файлы и через какие бы страны ни передавались, вы можете еще больше усилить их защиту, **зашифровав все данные**, в том числе хранящиеся на серверах. Используйте токены — это дополнительный уровень защиты. Тогда, даже если киберпреступники сумеют перехватить данные где-то на полпути между вашим компьютером и сервером, им будет непросто в них разобраться.

разработайте стратегию безопасности

Вы можете обезопасить себя от внутренних уязвимостей, разработав протоколы, регламентирующие доступ к информации: кто может использовать данные, когда, откуда и как.

Если сотрудники используют для работы личные устройства, то вы можете создать такие протоколы с помощью систем управления мобильными устройствами (MDM). Не забывайте и о традиционном оборудовании — компьютерах, серверах и т. п.

В обязательном порядке своевременно обновляйте программы на всех системах, подключенных к облачным сервисам — да, и на том маленьком сервере в углу тоже. Вы ведь не хотите, чтобы он стал дырой, через которую злоумышленники проникнут в вашу систему?

Безопасность вашей сети следует **обеспечивать круглосуточно**. Выполняйте мониторинг данных в реальном времени, оценивайте все свои приложения в упреждающем режиме, чтобы быстро обнаруживать угрозы безопасности и оперативно устранять их.

Ограничьте использование данных для сотрудников: новички не должны сразу же получить доступ ко всей критически важной информации. Если кто-то из сотрудников попытается взломать систему изнутри, это поможет вам ограничить круг подозреваемых.

думайте на шаг вперед

И самое главное — **думайте на шаг вперед**. При наличии четкого плана действий на случай катастрофы вы сможете быстро и эффективно решить любую проблему. Лучше заранее продумать план, чем в панике обзванивать всех подряд — тем более что вы рискуете так ни до кого и не дозвониться.

Самое слабое место любой облачной системы безопасности — пользователи. Даже если вы разработаете отличную стратегию, это не значит, что люди будут ей следовать. Пользователи не любят подчиняться правилам, которых они не понимают. Поэтому имеет смысл **обучить** ваших сотрудников. Расскажите им о рисках и попросите соблюдать простейшие меры предосторожности, например:

- не открывать важные документы через публичные точки Wi-Fi
- никогда не использовать один пароль дважды

Итак, при переходе в облако не забывайте о правилах безопасности, и тогда облачная инфраструктура не будет уступать в надежности любыми другим ИТ-решениям.

Джон Эванс (Jon Evans)